SENATO DELLA REPUBBLICA

XVIII LEGISLATURA

Doc. **CXXXVI**
n. **4**

RELAZIONE

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

(ANNO 2021)

(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 l'8 luglio 2022

PAGINA BIANCA

25 1997-2022 GPDP

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

UMANESIMO DIGITALE E PROTEZIONE DEI DATI

RELAZIONE DEL PRESIDENTE PASQUALE STANZIONE 2021

PAGINA BIANCA

1. Il "rumore della storia"

Signora Presidente del Senato,
Autorità,
Signore e Signori,

questa Relazione si inserisce in una congiuntura del tutto particolare, che con le parole del Papa potremmo definire più un cambiamento d'epoca che un'epoca di cambiamenti. Tanto profonde, sono, infatti, le innovazioni che caratterizzano l'ora presente, da aver determinato un vero e proprio mutamento di paradigma generale nel rapporto tra l'uomo e il mondo.

In questo più ampio contesto si inscrive la riflessione di oggi, al crocevia tra due momenti importanti: la congiuntura socio-politica attuale, segnata dal passaggio dall'emergenza sanitaria a quella internazionale e le spinte riformatrici sul terreno del digitale di cui l'Europa si è resa protagonista indiscussa, sviluppando l'itinerario intrapreso

già sei anni fa con il quadro giuridico europeo in materia di protezione dei dati.

Ma il dramma che si agita sullo sfondo è una priorità logica e assiologica da cui non è possibile prescindere; il "rumore della Storia" e l'"immane concretezza" del reale impongono una considerazione preliminare.

La guerra irrompe, contro ogni tentativo di rimozione, alle porte dell'Europa da più di quattro mesi, lascia consumare vite e le armi tornano a sostituire, con una pericolosa regressione storica e simbolica, la competizione non solo tra Stati ma tra modelli politici, tra autoritarismi e democrazie. Poco più in là dai confini del vecchio continente, il nomos della Terra si riprende, prepotentemente, lo spazio sinora occupato dalla paziente tessitura del diritto e dalla costante mediazione della politica. E gli effetti drammatici di questa anacronistica "patologia del confine" dimostrano, ancora una volta, le irrinunciabili virtù della democrazia e dello Stato di diritto, per perfettibili che siano.

Lo aveva, del resto, reso evidente la pandemia,

nel raffronto tra le politiche di contenimento sanitario adottate in Europa e le ben diverse misure di biosorveglianza di alcuni sistemi asiatici. Proprio la protezione dei dati è stata uno dei pilastri del modello europeo di governo dell'emergenza, che in snodi importanti come le scelte sul *contact tracing* o sul *green pass* ha suggerito la direzione più conforme al personalismo sotteso alla costruzione europea.

Sul terreno dell'emergenza sanitaria si è infatti misurata, fino in fondo, la capacità tutta europea di coniugare libertà e solidarietà senza consentire prevaricazioni dell'una sull'altra. E in questo gioco di equilibri in continua ridefinizione, la privacy ha dimostrato di essere un diritto mai tiranno, duttile nelle soluzioni di volta in volta richieste ma rigoroso nei principi e nel significato ultimo: promuovere la sinergia tra innovazione e libertà, collocando sempre - come ci ha ricordato il Presidente della Repubblica e analogamente al preambolo della Carta di Nizza - la "persona al centro".

Questo straordinario diritto di libertà si

è rivelato determinante nel guidare la transizione digitale promossa, con accelerazione esponenziale, dalla pandemia, per impedire che il doveroso distanziamento sociale annientasse le relazioni e la vita collettiva, spostando il nostro quotidiano nella realtà virtuale senza, tuttavia, il rischio di divenire schiavi del sempre più invasivo occhio elettronico.

Ma lo sviluppo dirompente della digitalizzazione, favorito con progressione geometrica dalla pandemia, mostra oggi, nel contesto della prima guerra (anche) cibernetica, tutte le sue più profonde implicazioni per quella che lucidamente è stata definita "super-società", fatta di interdipendenze inestricabili, paradossalmente proprio nell'era della disintermediazione (M. Magatti).

Nel passaggio dal reale al virtuale, in quello che è stato un vero e proprio uploading della vita individuale e collettiva, la simmetria della trasposizione online non ha riguardato anche - o non come avrebbe dovuto e non solamente in Italia - i presidi a tutela della persona e degli Stati.

Secondo le stime del World Economic Forum,

nell'anno trascorso si sarebbe registrato un aumento del 151% degli attacchi ramsomware: cifra tutt'altro che marginale se si considera che ciascun incidente può determinare una perdita aziendale quantificabile addirittura, secondo il Ponemon Institute, in 4,24 milioni di dollari. Ecco, anche, perché la protezione dati rappresenta per le aziende non già un costo ma un fattore di competitività, oltre che una risorsa reputazionale importante.

La più accentuata esposizione on line delle nostre vite ha mutato, parallelamente, la stessa generale percezione della vulnerabilità informatica: secondo uno studio del Censis, il 56, 6% degli italiani teme, oggi, di subire violazioni della propria sicurezza informatica più del libero accesso alla rete da parte dei minori (34,7%), della dipendenza dal web (23,7%) e di essere vittima di hater (22%). E la vicenda milanese (operazione "Rear Window") delle organizzazioni criminali aduse a violare gli impianti di sorveglianza persino domestici, consentendo così di spingere un'insana curiosità sin nelle pieghe più intime delle "vite degli altri", è soltanto un esempio di quanto

la porosità del confine digitale possa pregiudicare i singoli e la collettività.

Talmente veloce e improvvisa è stata la traslazione *online* delle nostre attività che quella digitale è apparsa, progressivamente, come la frontiera più permeabile e agevolmente valicabile da parte della criminalità informatica e di chiunque intenda sfruttare dati e informazioni, anche personali, a fini illeciti. Proprio durante il *lock down* si è registrato un incremento significativo degli attacchi informatici ai danni (anche) di enti pubblici, di catene di approvvigionamento e di reti sanitarie, secondo una tendenza che si sarebbe, inevitabilmente, amplificata con il conflitto russo-ucraino.

Ma se la guerra convenzionale soggiace, quantomeno, alla logica territoriale del confine, la sua componente ibrida, cibernetica, ne prescinde mettendo in gioco, sia pur solo per *spillover*, anche i Paesi che non partecipano direttamente alle ostilità. L'Enisa ha calcolato che oltre un terzo dei trecento attacchi *cyber* verificatisi tra Russia, Ucraina e Bielorussia, dall'inizio delle ostilità, ha avuto

implicazioni nell'Unione europea: anche sotto questo profilo la guerra, dunque, ci riguarda e impone una strategia comune di difesa. La protezione della frontiera digitale - la cui componente centrale è proprio la protezione dei dati personali - assume, quindi, una funzione prioritaria nella tutela dei singoli e degli Stati.

Particolarmente lungimirante, in questo senso, è stata la scelta dell'UE di aggiornare, proprio a fine 2020, la propria strategia di *cybersecurity* proponendo anche una nuova direttiva (la NIS2) maggiormente calibrata sulle sfide attuali. Altrettanto opportuna è apparsa, in ambito nazionale, l'istituzione dell'Agenzia per la cybersicurezza nazionale, con cui il Garante ha sin dall'inizio instaurato - come previsto dalla stessa disciplina istitutiva - una proficua collaborazione, recentemente declinata in uno specifico protocollo d'intenti.

Ma la guerra alle porte dell'Europa non è "soltanto", anche, una *cyber-war*, ma è persino una social-war, combattuta con strategie di condizionamento del consenso realizzate soprattutto attraverso i social

network, sulle quali potrà peraltro incidere il recente Codice di condotta sulla disinformazione della Commissione europea.

Anche in questo caso, la pandemia aveva anticipato la tendenza futura all'infodemia che, con la guerra, ha mostrato di poter divenire persino autarchia informativa, realizzata mediante censura di contenuti ostili e promozione della narrazione dei fatti più utile alla propria parte.

Si tratta di implicazioni tutt'altro che trascurabili del processo di datificazione della vita individuale e collettiva, che ridisegna assetti di potere e strategie di gestione del consenso e che l'Unione europea mira a governare, concentrando proprio sul digitale la sua spinta riformatrice, per temperare la *rule of technology* con la *rule of law*.

2. La via europea al digitale

Particolarmente significativo, da questo punto di vista, è il *draft* di *Artificial Intelligence Act*, che introduce alcune misure indispensabili a prevenire

le implicazioni pregiudizievoli, per i singoli e la collettività, dell'intelligenza artificiale.

La proposta sottende una scelta importante, in termini non soltanto regolatori, ma anche e soprattutto politici e assiologici. Essa esprime l'esigenza di rimodulare il perimetro del tecnicamente possibile sulla base di ciò che si ritiene giuridicamente ed eticamente accettabile.

L'*Artificial Intelligence Act* è uno (forse persino il più rilevante) dei vari tasselli che compongono il mosaico, in costante evoluzione, della regolazione europea del digitale, nel cui ambito il Gdpr svolge un ruolo centrale, sotto il profilo del metodo e del merito. Esso, infatti, ha da un lato rappresentato un vero e proprio paradigma di tutela cui la legislazione europea successiva si sta conformando, valorizzandone ora la sinergia tra *principles* e *rules*, ora la neutralità tecnologica, ora il principio di responsabilizzazione e, in linea generale, la fonte regolamentare quale forma regolatoria elettiva per garantire livelli di garanzie uniformi (*one continent, one law*).

Per altro verso, il Gdpr ha espresso il primo, importante tentativo di introdurre, con obblighi di responsabilizzazione e trasparenza nel trattamento, un argine significativo al capitalismo delle piattaforme, la cui egemonia anche culturale (nell'accezione gramsciana) si fonda sullo sfruttamento di quei frammenti dell'io che sono i dati personali. Quest'istanza regolatoria è stata espressa tentando di coniugare le esigenze di circolazione dei dati-funzionali non solo a fini economici ma anche solidaristici - e diritto dei singoli al "governo" della propria sfera informazionale. E l'altro elemento del binomio su cui si fonda, sin dal titolo, il Gdpr ("la libera circolazione" dei dati) è l'oggetto delle due ulteriori proposte legislative (*Data Act* e *Data Governance Act*) che, pur con un testo certamente perfettibile (come chiarito anche dal Comitato europeo per la protezione dei dati e dal Garante europeo) concorrono al quadro delle riforme del settore. Nella stessa linea, la proposta normativa sullo Spazio europeo dei dati sanitari dovrà realizzare un congruo bilanciamento tra condivisione, anche

a fini di ricerca, di questo particolare tipo d'informazioni e la tutela rafforzata che esse meritano.

Particolarmente importanti sono, del resto, il *Digital Services Act* e il *Digital Markets Act*, presentati dalla Commissione con l'intento di introdurre una regolazione essenziale del potere privato delle piattaforme. A tal fine se ne rafforzano gli obblighi (di informazione, lealtà, correttezza ma più in generale responsabilizzazione) e, per converso, si riconosce all'utente una gamma di strumenti di intervento volti a promuoverne, anche in forma proattiva, la tutela ad ampio spettro.

Ma non meno significative sono anche le proposte normative sul targeting politico e sul lavoro su piattaforma, entrambe le quali affrontano, sia pure da punti di vista diversi, i rischi di involuzione sociale e democratica connessi a un abuso delle nuove tecnologie. La *gig economy*, con il rischio di un nuovo caporalato digitale, ma anche il *targeting* politico funzionale al condizionamento del consenso, sono, infatti, due emblemi significativi dell'esigenza di una *governance* del digitale che tenga conto delle

implicazioni, potenzialmente distorsive, delle nuove tecnologie sulle coordinate essenziali della democrazia.

Si tratta, dunque, di disciplinare le condizioni per un utilizzo sostenibile della potenza di calcolo che, con la sua capacità di "colonizzare il pensiero" (L. Violante), rischia di incidere su quella libertà cognitiva necessaria per la garanzia di ogni altro diritto fondamentale. Il capitalismo delle piattaforme non è, infatti, più soltanto cognitivo (fondato dunque sulla raccolta delle informazioni) ma addirittura, come suggerisce Eric Sadin, delle "affezioni", in quanto tale da condizionare comportamenti partendo dall'analisi delle reazioni ai contenuti diffusi. Anche per questo la privacy comportamentale è un presupposto essenziale di libertà a fronte del rischio di un costante pedinamento digitale: lo abbiamo ricordato, in particolare, con le Linee guida sui cookies, che contengono indicazioni importanti per un uso consapevole della rete.

Le implicazioni complessive delle riforme in discussione sono rilevanti. Esse contribuiscono infatti, ciascuna nel suo ambito, a una rimodulazione generale

dell'assetto dei poteri così scardinato dal digitale, in una direzione funzionale alla tutela della persona (e della stessa libertà di espressione), contrastando gli effetti distorsivi di una tecnica altrimenti anomica. E il dibattito statunitense di questi giorni, sulla rimozione dai *social* dei contenuti relativi a farmaci abortivi, dimostra quanto cruciale sia una regolazione delle piattaforme realmente conforme ai valori di una democrazia.

La protezione dei dati rappresenta un elemento costitutivo di questo disegno regolatorio europeo, anche in funzione di contenimento dei poteri privati. Esso, infatti, presuppone anzitutto, in capo alle piattaforme, obblighi di trasparenza e responsabilizzazione mutuati dalla disciplina privacy e con essa interrelati. Di qui anche l'estensione delle competenze delle Autorità di protezione dati (si pensi alla direttiva sul lavoro mediante piattaforme o al regolamento sul targeting politico), pur al di là di una loro attribuzione formale di specifici ruoli (come pure si è auspicato per l'*Artificial Intelligence Act* e il *Digital Services Act*).

Le Autorità di protezione dei dati s'inseriscono dunque, pienamente, nel disegno riformatore europeo, di cui sono anzi interpreti d'avanguardia. Esse sono state infatti chiamate ad applicare la prima effettiva, organicaregolazione del digitale, che non a caso viene assunta a modello in molti altri Paesi (effetto Bruxelles), tra i quali, da ultimo, la Cina o comunque esige un'uniformazione delle garanzie a livello globale, come dimostra la vicenda delle sentenze Schrems e dei successivi accordi con gli Usa. Un'eccessiva asimmetria nel livello di garanzie accordate dagli ordinamenti dei Paesi terzi nel trattamento dei dati personali determina, infatti, l'impossibilità di avvalersi di canali più agevoli per il trasferimento dei dati, con l'esigenza di bloccare i flussi informativi che non siano assistiti da misure di protezione adeguate. E' quanto si è dovuto ricordare, anche recentemente, con il provvedimento su Google Analytics, che affronta le implicazioni (anche in termini di sovranità digitale e indipendenza tecnologica) dell'asimmetria, e livello internazionale, nella regolazione dell'uso dei dati: infrastruttura

strategica per lo sviluppo dei Paesi, come ha sottolineato il Ministro del lavoro e delle politiche sociali.

Ecco anche perché la protezione dei dati assurge sempre più a fattore determinante della geopolitica, in un contesto in cui, se la Cina tende a far coincidere spazio fisico e virtuale, confini territoriali e risorse informative, per parte opposta anche negli Stati Uniti si discute di rideclinare in forme nuove l'idea di sovranità digitale.

3. Il dialogo istituzionale

La centralità della protezione dei dati nel contesto sociale attuale si riflette sul ruolo del Garante e sul suo coinvolgimento, sempre più rilevante, nella dinamica istituzionale. Nell'ultimo anno si è registrato, in particolare, un incremento rilevante (nell'ordine di circa il 50%) nel numero di pareri su (schemi di) atti legislativi o regolamentari, nonché di audizioni parlamentari, sia in sede di istruttoria legislativa sia nell'ambito di specifiche indagini conoscitive promosse anche da commissioni d'inchiesta

(come ad esempio è stato per quelle sul femminicidio o sulla tutela dei consumatori), anche di là, dunque, dalla sola consultazione obbligatoria.

Proprio la varietà dei contesti istituzionali in cui il contributo del Garante viene richiesto dimostra come si stia, progressivamente, diffondendo la consapevolezza dell'esigenza di progettare le riforme, in qualsiasi campo, secondo una prospettiva *privacy-oriented*, per promuovere innovazioni che siano realmente inclusive e non determinino, sia pur per mera preterintenzione, discriminazioni.

Il coinvolgimento del Garante, in varie forme e nelle diverse fasi del procedimento normativo (inclusa dunque quella attuativa) ha consentito, ad esempio, alla disciplina del *green pass* di delineare progressivamente, per approssimazioni successive, un equilibrio ragionevole tra esigenze di sanità pubblica, riservatezza individuale e autodeterminazione in ordine alle scelte sanitarie.

Attraverso l'audizione del Garante sui principali snodi dell'evoluzione normativa che ha caratterizzato la materia e la sua consultazione sui provvedimenti

attuativi, si sono infatti approntate le garanzie necessarie, tra le altro, per consentire la verifica della certificazione senza, però, renderne ostensibile il presupposto di rilascio. Si è potuto così impedire l'indebita conoscenza, da parte di terzi, della condizione sanitaria o, comunque, delle scelte vaccinali del soggetto, tranne per il solo aspetto, su cui il monito del Garante è rimasto inascoltato, della facoltà di consegna della certificazione al datore di lavoro nel periodo di vigenza del relativo obbligo di verifica. Si è, inoltre, conferita maggiore determinatezza tanto all'"architettura" quanto alle finalità del trattamento, di cui si è correttamente prescritta la previsione con legge statale, in ragione delle riserve legislative su cui incide la disciplina.

Costruttivo e determinante è stato il confronto tra Camere, Governo e Garante sul *telemarketing* illecito, che resta un fenomeno endemico, al punto di essere assurto a simbolo dell'invadenza del mercato nella vita privata. Nell'ultimo anno, in particolare, con un emendamento al d.l. 'capienze' che ha esteso

la riferibilità del registro delle opposizioni alle chiamate automatizzate, si è superato, nel senso auspicato dall'Autorità, uno stallo che ha impedito, per oltre due anni, la piena attuazione della l. n. 5 del 2018. Il che ha consentito anche l'approvazione del nuovo regolamento sul registro pubblico delle opposizioni, che ha recepito i rilievi espressi dal Garante con ben tre pareri e che determinerà, tra pochi giorni, il suo effettivo funzionamento con estensione alle utenze mobili (e riservate), nonché alle chiamate automatizzate.

Il radicamento, nelle dinamiche economiche, del fenomeno del *telemarketing* illegale esige tuttavia una strategia di contrasto multilivello, che alla forza della disciplina normativa affianchi l'efficacia delle regole di settore. Così, il Garante ha incoraggiato e sostiene attivamente - come già ho rappresentato in Parlamento - il progetto di redazione di un codice di condotta in materia che, promuovendo la responsabilizzazione dei titolari favorisca comportamenti virtuosi, persino forse più di quanto possa riuscirvi la deterrenza esercitata dal

quadro sanzionatorio, pur elevato e che anche quest'anno ha determinato l'irrogazione di sanzioni tra le più rilevanti per un Paese, quale il nostro, risultato al secondo posto per numero di sanzioni irrogate e quarto per ammontare complessivo (nell'ultimo anno pari a oltre 38 milioni di euro per il solo *telemarketing*).

Un altro contesto sul quale la consultazione del Garante è stata intensa è quello fiscale, interessato ora peraltro da una delega legislativa che, nel suo sviluppo, dovrà delineare quel congruo equilibrio tra esigenze di contrasto degli illeciti e riservatezza dei contribuenti, cui alludevamo in audizione sulle politiche fiscali. Le indicazioni del Garante volte a migliorare gli standard di esattezza e qualità dei dati trattati contribuiranno, peraltro, ad assicurare una più corretta rappresentazione della capacità contributiva degli interessati, migliorando complessivamente l'efficacia dell'analisi del rischio fiscale su cui si fonda buona parte delle politiche di contrasto in materia.

Nello sviluppo della delega si dovrà anche considerare che, (anche) in quest'ambito, sono necessari non tanto e non solo, genericamente, dati in maggiore

quantità, ma di migliore qualità, non eterogenei per struttura e dimensione né soggetti al rischio di disallineamento, perché aggiornati. Solo in tal modo l'interoperabilità potrà offrire un contributo effettivo alla semplificazione e all'efficienza dell'azione amministrativa, come si è del resto avuto modo di chiarire in relazione alla Piattaforma digitale nazionale dati ma anche alla complessiva materia della sanità digitale.

In quest'ultimo caso, poi, l'esigenza di qualità ed esattezza dei dati è ancor più rilevante, dal momento che un errore nel dato sanitario o un suo mancato aggiornamento può determinare, nel contesto clinico, rischi addirittura per la salute del paziente: tema ineludibile soprattutto per il fascicolo sanitario elettronico.

Proficua è stata l'interlocuzione anche rispetto a un tassello centrale, ancora mancante, della disciplina di protezione dati: il regolamento sui dati giudiziari ex art. 2-*octies* del Codice, necessario ai fini dell'individuazione dell'ambito legittimo di trattamento di questa particolare tipologia di dati, in particolare

nel settore privato. Proprio in ragione della funzionalità di questa disciplina allo svolgimento di molte, rilevanti attività (anche) economiche in condizioni di sicurezza e affidabilità, lo stallo nell'adozione del testo definitivo dev'essere necessariamente superato.

4. Per un'innovazione non regressiva

Ancor più rilevante è e continuerà ad essere il confronto tra Camere, Governo e Garante sui provvedimenti attuativi del PNRR, su alcuni dei quali (in particolare sull'innovazione della p.a. e la sanità digitale) l'Autorità si è già pronunciata. E' importante mantenere questo dialogo costante anche e soprattutto dopo la denormativizzazione operata dal decreto-capienze rispetto ai presupposti del trattamento dei dati personali (non giudiziari, come chiarito in un recente provvedimento) in ambito pubblico.

La perdita di centralità della fonte normativa a favore di atti amministrativi generali rischia

infatti, in assenza di una visione sinottica, di rendere disomogenei gli standard di tutela, laddove invece l'innovazione delle pubbliche amministrazioni dovrebbe promuovere non soltanto l'efficienza dell'azione amministrativa ma anche l'inclusione, la partecipazione e, in ultima analisi, il superamento delle diseguaglianze.

Il Garante è pronto a supportare le amministrazioni in questo passaggio così determinante, nella consapevolezza di come la protezione dati abbia rappresentato sinora un fattore unificante (perché impone uniformità di garanzie), a fronte della frammentazione che, spesso, ha caratterizzato il processo di digitalizzazione nel nostro Paese, eplicando se non addirittura accentuando la disomogeneità, su base territoriale, nel livello di prestazioni erogate.

Anche l'indagine conoscitiva avviata, dalle Autorità di protezione dati europee (tra cui il Garante), sul ricorso a sistemi *cloud* in ambito pubblico mira a indirizzare l'allocazione di asset informativi strategici in un percorso di piena sicurezza,

che garantisca effettivamente indipendenza tecnologica.

Per questo l'innovazione - quale obiettivo trasversale di riforma - va declinata in termini più complessi della mera delega al digitale di più o meno significative funzioni pubbliche e private. Essa va intesa come un progetto di sviluppo organico e lungimirante, in cui la tecnica sia posta al servizio dell'uomo e non viceversa e in cui il progresso sia, anzitutto, progresso nei diritti. Il richiamo alla "resilienza" all'interno dell'acronimo PNRR è, in questo senso, molto più che uno slogan. Indica, infatti, la capacità dell'Europa prima (e, per essa, dei singoli Stati) di adattamento a congiunture avverse, come quelle emergenziali, senza tuttavia mai indebolire la garanzia dei diritti.

E' quanto, del resto, traiamo dall'esperienza della pandemia, che l'Italia e l'Europa tutta hanno affrontato senza mai porre un *aut aut* tra sanità e diritti individuali, tra solidarietà e libertà, ma coniugando queste istanze in modo da realizzarne il miglior equilibrio. L'attuazione delle riforme deve anzitutto far tesoro del lascito dell'esperienza

di questi mesi difficili: la "lotta per il diritto" è anche e, soprattutto, lotta per l'affermazione del diritto nelle varie emergenze che si ripropongono, soprattutto in un ordinamento, come il nostro, che non prevede stati di eccezione.

Questa consapevolezza è il presupposto ineludibile per riforme che siano non soltanto e mera innovazione tecnica, ma che sanciscano invece un reale progresso in termini di libertà e di garanzie democratiche. E per far questo è indispensabile che la digitalizzazione proceda parallelamente alle garanzie di protezione dei dati, tra le quali soprattutto i principi di minimizzazione, di sicurezza, di trasparenza del trattamento, come abbiamo avuto modo di sottolineare rispetto ad alcuni provvedimenti espressivi di politiche, anche sociali, innovative (Carta europea della disabilità, Registro nazionale tumori, Carta dello studente, Anagrafe nazionale degli assistiti, App Io, raccolta on line di firme per referendum e iniziativa legislativa popolare, Spid minori, Anagrafi dell'istruzione). Va, infatti, assicurato che il percorso di transizione digitale dell'azione

amministrativa, in ogni campo, non avvenga rivelando dati, in particolare se soggetti a tutela rafforzata come quelli "sensibili", giudiziari o sui minori non strettamente indispensabili, non li esponga a rischi d'esfiltrazione e corrisponda sempre a quanto normativamente previsto e reso noto al cittadino. Il rischio, altrimenti, è quello di replicare, se non addirittura approfondire, le diseguaglianze esistenti, con un effetto paradossalmente regressivo in termini sociali. Le notevoli potenzialità in termini di efficienza ed efficacia delle politiche sociali, offerte dagli algoritmi devono dunque essere valorizzate minimizzando i rischi connessi a un uso poco attento delle neotecnologie, assicurandone un controllo costante sui possibili effetti distorsivi, non certo rinunciando ai benefici suscettibili di derivarne.

I rischi, in termini di discriminazione, potenzialmente connessi al *social scoring* (non a caso vietato, se basato sul monitoraggio individuale, dall'Artificial Intelligence Act) hanno indotto così, ad esempio, la nostra Autorità a disporre accertamenti sulle iniziative di alcuni enti territoriali volte a offrire

incentivi a fronte di comportamenti virtuosi dei cittadini, oggetto di monitoraggio o di una vera e propria profilazione.

Ecco, dunque, che il richiamo - frequente nel PNRR - all'innovazione, alla digitalizzazione, alla crescita non può mai essere disgiunto da una visione, di lungo periodo, più complessiva, che coniughi sviluppo e diritti.

La protezione dei dati assume dunque un ruolo baricentrico nel comporre queste istanze, tracciando la direzione intorno alla quale imprimere al Paese un'innovazione sostenibile anche in termini di diritti e libertà.

5. Libertà, giustizia, dignità

Particolarmente significativo è stato, in particolare in quest'anno, il confronto con il Governo sul tema dell'uso giudiziario dei tabulati, al centro di due importanti sentenze della Corte di giustizia europea.

Con la prima, del 2 marzo 2021, *H.K. c. Prokuratuur (C 746-18)* la Corte di giustizia ha

sottolineato l'esigenza di terzietà, rispetto al soggetto pubblico richiedente, dell'autorità titolare del potere di acquisizione dei tabulati. A seguito di tale pronuncia il Garante aveva rivolto, nel luglio scorso, una segnalazione al Parlamento e al Governo, volta a suggerire una riforma della disciplina modulata sulla piena giurisdizionalizzazione del procedimento acquisitivo e sulla revisione, in senso maggiormente conforme al canone di proporzionalità, di condizioni, limiti e termini di conservazione dei tabulati.

Sviluppando le indicazioni della Corte (e della stessa segnalazione), il Governo ha sottoposto al parere del Garante uno schema di decreto-legge di revisione della disciplina della *data retention* che, oltre ad attribuire al giudice la competenza autorizzatoria in materia, ha limitato la possibilità di acquisizione dei tabulati ai soli procedimenti per reati connotati da una determinata gravità, in presenza di sufficienti indizi e della rilevanza dell'acquisizione ai fini dell'accertamento dei fatti. Il testo definitivo del decreto-legge (n. 132 del 2021), già in linea con la segnalazione, ha anche recepito

le indicazioni del Garante sull'esercizio, da parte degli interessati, dei propri diritti in relazione ai dati contenuti nei tabulati.

Si è così realizzato un rilevante (ancorché non del tutto risolutivo) avanzamento nelle garanzie correlate all'acquisizione dei tabulati, in virtù della convergenza tra terzietà nella fase autorizzatoria e limitazione oggettiva dei casi di ammissibilità. Ma anche quest'assetto sembra destinato ad essere superato dai rilievi più dirimenti espressi con la sentenza C-140/20 del 5 aprile scorso, con la quale la Corte di giustizia Ue ha chiarito come la conservazione dei tabulati a fini di giustizia non possa essere generalizzata e indifferenziata, ma soltanto "mirata" sulla base di criteri soggettivi, geografici o di altra natura (purché oggettivi e non discriminatori) ovvero "rapida" (*quick freeze*). La Corte suggerisce, dunque, una vera e propria mutazione della natura di questo strumento investigativo, che esigerà un'ampia riforma della disciplina interna. Essa, infatti, - pur a fronte di una differenziazione per titolo di reato in fase acquisitiva - presuppone, comunque,

la conservazione preventiva e generalizzata dei dati di traffico relativi alla generalità indistinta dei cittadini. Dovranno, dunque, essere disciplinati, non solamente la conservazione rapida e il relativo accesso, ma soprattutto i parametri (oggettivi e non discriminatorii) sulla base dei quali procedere alla conservazione mirata dei dati di traffico e relativi all'ubicazione, da utilizzare a fini di contrasto di reati gravi.

Il ricorso alle neotecnologie nell'ambito delle attività di contrasto può amplificarne, in assenza di un quadro organico di garanzie, i rischi tanto sul piano individuale quanto su quello collettivo. La congiunzione tra potere d'indagine e potenza della tecnica impone, infatti, la previsione di limiti tanto più stringenti quanto più avanzato sia il grado d'autonomia decisionale della macchina. In questo senso, l'utilizzo dell'intelligenza artificiale nel settore investigativo dev'essere circondato delle garanzie necessarie ad evitare la delega all'algoritmo di attività della massima delicatezza perché, tra l'altro, potenzialmente incidenti sulla libertà personale. Per questo, ad esempio, il Garante ha escluso

che il ricorso alle *body cam*, da parte delle autorità di pubblica sicurezza, potesse di per sé legittimare anche il riconoscimento facciale in ragione dei rischi, per la dignità e libertà individuali, ad esso connessi, su cui ci ammoniscono anche le recenti Linee guida del Comitato europeo per la protezione dei dati. Ed è significativo che, con un emendamento al d.l. 'capienze', si sia introdotta una generale moratoria nel ricorso al riconoscimento facciale, ammesso solo in ambito di polizia - previo parere avorevole del Garante - o giudiziario. I rischi di un monitoraggio su base biometrica dei cittadini, realizzato peraltro da soggetti privati "rastrellando" dati dalla rete (*web scraping*) è, del resto, alla base del provvedimento inibitorio e sanzionatorio (dell'entità di venti milioni di euro) adottato nei confronti di Clearview.

Il rapporto tra esercizio della funzione giurisdizionale, informazione e privacy - tra i più complessi del nostro sistema giuridico- è stato, peraltro, oggetto di recenti modifiche normative di rilievo. Da un lato, infatti, la riforma del processo

penale ha previsto (quale criterio direttivo per l'esercizio della delega legislativa) che le pronunce giurisdizionali favorevoli costituiscano titolo per un provvedimento di deindicizzazione che, nel rispetto della normativa in materia di protezione dei dati personali, garantisca il diritto all'oblio dell'interessato. La pronuncia favorevole assurge, dunque, a presupposto normativo per una specifica tutela della privacy (già, peraltro, accordata in questi termini da una consolidata prassi del Garante), che coniuga esigenze informative e riservatezza individuale.

Particolarmente rilevante è anche il d.lgs. 188 del 2021, che ha introdotto un articolato sistema di tutele del diritto dell'indagato o dell'imputato a non essere indicato "pubblicamente come colpevole" finché non ne sia definitivamente accertata la responsabilità penale, unitamente a nuove modalità di gestione del rapporto tra giustizia e informazione.

Parallelamente a queste garanzie extraprocessuali della presunzione d'innocenza, si introducono poi ulteriori garanzie specificamente intraprocessuali,

rilevanti (anche) quali parametri di redazione degli atti. Si rimodula, dunque, il rapporto tra comunicazione sulla giustizia e dignità personale, nella condivisibile direzione di una loro effettiva sinergia.

6. Vecchie e nuove vulnerabilità

Tra le direttrici dell'attività del Garante che più si stanno accentuando vi è quella incentrata sulla tutela della persona che versi, per qualità soggettiva o per contesto oggettivo, in condizioni di particolare vulnerabilità. Se, infatti, protezione dei dati personali è, sempre, diritto al libero sviluppo della propria personalità, in condizioni di autodeterminazione informativa, nel caso dei soggetti più vulnerabili essa è anche di più. E' tutela della persona (della sua identità, dignità, finanche libertà) da discriminazioni vecchie e nuove, spesso amplificate dalla potenza della rete o accentuate dalla (solo pretesa) neutralità dell'algoritmo.

Quest'obiettivo di tutela - indicato già un anno fa come prioritario per il nostro mandato - è sotteso

a pressoché tutta l'attività del Garante; ne qualifica anzi l'identità come Autorità per la tutela delle (di tutte le) persone (neppure soltanto dei cittadini).

Ma, nell'anno trascorso, alcune specifiche esigenze di tutela sono emerse, in modo particolare, nel contesto dell'informazione e nel rapporto di lavoro. Per quanto riguarda il giornalismo, si è avuto modo, in particolare, di sottolineare come l'esigenza informativa vada soddisfatta nel rispetto del criterio di essenzialità (come ad esempio si è ribadito per il caso del liceo Montale di Roma), ma soprattutto senza indulgere a forme di spettacolarizzazione del dolore o sensazionalismo, suscettibili di pregiudicare ulteriormente la condizione delle vittime e dei loro familiari.

Il giornalismo vive del costante equilibrio tra diritto di (e all') informazione e dignità della persona, che mai va strumentalizzata a fini di cronaca; soprattutto se versi in condizioni di particolare vulnerabilità: minori, malati detenuti, arrestati.

Ecco la ragione per cui, anche a proposito della guerra, abbiamo ribadito l'esigenza di evitare,

pur nel prezioso esercizio della libertà di stampa, la spettacolarizzazione del dolore, espresso dalla forza drammatica dei corpi straziati, soprattutto dei bambini. La narrazione della guerra - cui non dobbiamo mai assuefarci come a uno spettacolo da osservare quasi anestetizzati, da comoda distanza - non ha bisogno di sacrificare la dignità della persona per soddisfare le pur legittime esigenze informative.

Nel corso dell'anno sono stati diversi i casi nei quali il Garante ha rappresentato l'esigenza di non indulgere sulla "personalizzazione del dramma", sull'imprimere alle tragedie (che pur vanno raccontate) necessariamente il volto straziato, martoriato, offeso delle vittime e i dettagli della loro vita privata non essenziali alla descrizione dei fatti. Lo si è sottolineato, ad esempio, rispetto al bambino ucciso a Vetralla e alla bimba morta a Cisliano, a fronte di un eccesso informativo incompatibile con la tutela rafforzata della riservatezza accordata ai minori (non solo in vita) dall'ordinamento.

Analogamente, meritano una tutela specifica

i soggetti sottoposti a misure limitative della libertà personale che- come è stato necessario ricordare anche quest'anno - non devono essere ripresi, in chiaro, in tali condizioni e vanno protetti - come afferma, per le traduzioni, la legge sull'ordinamento penitenziario - dalla mera "curiosità del pubblico".

L'esigenza di tutela rafforzata delle persone (non soltanto minori) che versino in condizioni di fragilità va, peraltro, osservata anche al di fuori del contesto giornalistico in senso stretto ed anche laddove la pubblicazione sia sostenuta da fini di "denuncia" anche politica, come si è avuto modo di sottolineare rispetto alla diffusione, via *social*, di video e foto di ragazzi disabili o in situazioni di disagio socio-economico.

Analogamente, è stata sanzionata la diffusione sul web, da parte di una pubblica amministrazione, dei dati personali degli studenti percettori di sussidi economici riservati a nuclei familiari con reddito inferiore a una determinata soglia, così rivelandone la condizione di disagio socio-economico che la disciplina sulla trasparenza amministrativa vuole,

correttamente, sottratta a pubblicità.

Anche in tal caso, il fine sotteso al divieto di diffusione è quello di evitare discriminazioni e stigmatizzazioni riferite alle condizioni di vulnerabilità del soggetto, che per questo merita invece una tutela rafforzata e specifica, tale da rappresentare anche un limite interno agli obblighi di pubblicità.

Analoga tutela specifica s'impone per quella peculiare condizione di debolezza propria del lavoratore, dovuta alla sua posizione all'interno di un rapporto strutturalmente asimmetrico, quale quello di lavoro, non a caso destinatario, con la l. 300 del 1970, delle prime norme dell'ordinamento a tutela dell'autodeterminazione informativa. Tra queste, in particolare, il divieto di controllo a distanza dell'attività lavorativa, funzionale a evitare ingerenze datoriali indebite nella sfera di riservatezza dei lavoratori.

Così, si è precisato che anche i sistemi di *customer care* dai quali derivi, sia pur indirettamente, un controllo sull'attività lavorativa necessitano delle garanzie (concertazione sindacale o autorizzazione amministrativa) previste dallo Statuto dei lavoratori,

pena un'indebita elusione di tale forma di tutela. Analoga elusione è stata stigmatizzata rispetto al monitoraggio indiscriminato e preventivo della navigazione in internet dei lavoratori, inammissibile in quanto tale, appunto, da annullare quelle garanzie essenziali di autodeterminazione riconosciute come indispensabili sin dal 1970.

Per altro verso, in sede consultiva, si sono suggerite alcune integrazioni volte a ulteriormente perfezionare un già condivisibile disegno di legge governativo per l'introduzione di alcune garanzie essenziali nel contesto del lavoro mediante piattaforma.

Si è, in particolare, condivisa la scelta - già sottesa alla corrispondente direttiva europea - di disciplinare condizioni e tutele specifiche, anche in termini di equità e trasparenza, per il ricorso a processi decisionali automatizzati con effetti sul rapporto di lavoro.

7. Una tutela inclusiva

Se la tutela della persona in condizioni di particolari vulnerabilità è una componente

(sempre più) rilevante della protezione dei dati personali, lo è non certo per mera contingenza ma per un'intima, originaria, vocazione di questo diritto al riequilibrio dei rapporti sociali e alla ridefinizione degli assetti di potere.

Questa vocazione viene oggi valorizzata dal legislatore, che proprio in quest'anno ha attribuito all'Autorità funzioni rilevanti sul terreno della tutela dei soggetti più vulnerabili, secondo il paradigma, risultato particolarmente efficace, del cyberbullismo. Il "decreto-capienze" ha, infatti, esteso tale modello di tutela al *revenge porn*, legittimando (anche gli ultraquattordicenni) a presentare istanza, al Garante, di blocco del caricamento di contenuti intimi riguardanti il richiedente, in presenza di specifici presupposti. I primi provvedimenti, approvati sulla base di tale disciplina, si sono dimostrati particolarmente efficaci nel prevenire la diffusione di contenuti suscettibili di arrecare pregiudizi, anche gravissimi - come insegna la tragedia di Tiziana Cantone - alla dignità della persona.

Questi nuovi strumenti risulteranno

particolarmente utili a tutelare soprattutto i minori, che sembrano purtroppo assurgere a vittime elettive dell'accelerazione del processo di digitalizzazione innescato dalla pandemia, come si evince dall'incremento del 295% dei casi di abusi su minori trattati dalla Polizia postale e delle comunicazioni, rispetto ai dati prepandemici del 2019, con un significativo aumento delle vittime di età compresa tra i dieci e i tredici anni, per quanto concerne la pedopornografia. Anche tenendo conto di questi elementi, nell'ambito del Tavolo per la tutela dei minori on line istituito presso il Ministero della giustizia si è condivisa, in particolare, l'opportunità di rafforzare le garanzie di *age verification* promuovendo il ricorso alla certificazione dell'identità da parte di terzi; introdurre norme a tutela dei *baby influencer*, verificandone i profitti generati online; estendere al fenomeno dello *sharenting* (diffusione d'immagini di minori da parte di adulti di riferimento) la tutela remediale, accordata al minore, sul terreno del cyberbullismo.

Anche per quanto riguarda un uso consapevole della rete da parte dei minori, risulterà rilevante il ruolo attribuito, sul terreno della pedagogia digitale, al Garante, che può ora prescrivere (o, comunque, valutare ai fini della commisurazione sanzionatoria) l'effettuazione, da parte del titolare del trattamento, di campagne di comunicazione istituzionale volte alla promozione della consapevolezza del diritto alla protezione dei dati personali.

Promuovere la "cultura" della protezione dei dati è certamente una delle soluzioni più importanti per favorire comportamenti virtuosi sia da parte dei titolari del trattamento che degli stessi interessati, spesso ignari dell'importanza di proteggere, con i propri dati, la propria libertà, con il rischio di divenire schiavi della "dittatura della presenza" (M. Serra).

Profetiche le parole di Umberto Eco, secondo cui il compito più significativo delle autorità di garanzia della privacy sarebbe stato non tanto e non solo "di assicurarla a coloro che la sollecitano (…) bensì di farla considerare un bene prezioso a coloro che vi hanno entusiasticamente rinunciato", pur di

liberarsi, con la micro-celebrità che assicurano le neotecnologie, di uno "spaventoso e insopportabile anonimato".

E' stato peraltro approvato, in prima lettura, un progetto di legge che condivisibilmente attribuisce al Garante la competenza a decidere le istanze - presentate anche da minori, se ultra quattordicenni - di rimozione di contenuti istigativi al suicidio.

Anche in tal caso, si intende contenere gli effetti pregiudizievoli della diffusione virale di comunicazioni suscettibili di condizionare, talora anche fatalmente, il comportamento degli utenti, soprattutto se minorenni.

Ecco perché il Garante sta divenendo progressivamente, sempre più, Autorità a tutela non già della persona digitale ma della persona, complessivamente intesa, (anche e soprattutto) nel digitale. Alcuni emendamenti e progetti di legge hanno colto, correttamente, lo spirito di quest'evoluzione, proponendo di designare il Garante quale Autorità per i diritti fondamentali.

Di là dalla soluzione legislativa, queste proposte

sottendono una consapevolezza nuova e significativa, che è emersa con sempre maggiore nettezza nel corso dei venticinque anni dall'istituzione del Garante, in un processo di progressiva "democratizzazione" di un diritto, la cui vocazione liberale e garantista affonda le sue radici proprio in quel *"penumbral right"* della sentenza Roe v. Wade.

Oggi quel diritto - arricchitosi di implicazioni e contenuti nuovi - riafferma e valorizza, ulteriormente, la sua caratterizzazione democratica.

In un contesto in cui i dati, anche e soprattutto personali, rappresentano le principali e più rilevanti risorse per l'economia, per la ricerca, per la crescita sociale, per l'attività politico-istituzionale, l'autodeterminazione informativa assurge, infatti, a presupposto ineludibile di altri diritti e libertà fondamentali, per la promozione dell'umanesimo digitale.

Ed ecco perché la protezione dei dati personali costituisce, sempre più, una componente centrale delle democrazie liberali, allorché garantisce che l'innovazione, l'iniziativa economica, l'attività

pubblica in ogni campo non violino - con un indebito sfruttamento dei dati e contraddicendo la stessa natura dello Stato di diritto - la dignità della persona. Soprattutto la dignità di soggetti quali minori, migranti, malati, detenuti, vittime o appartenenti a minoranze comunque individuate; di tutti coloro, cioè, la cui fragilità - per natura o per circostanza - rischia di renderli davvero "nudi" di fronte al potere: dello Stato, del mercato, della tecnica.

E proprio il potere della tecnica determina non solo nuove vulnerabilità ma addirittura nuove soggettività che esigono tutela: tra tutti, il "gemello digitale" di ciascuno di noi in quella dimensione sempre più "iperreale"- nell'accezione di Baudrillard - che appare il Metaverso. Anche per queste nuove istanze sociali la protezione dei dati può rappresentare uno strumento importante di tutela inclusiva, perché una tecnica sempre più ingiuntiva (demiurgica, predittiva e quindi performativa) non degeneri in egemonia distopica dell'algoritmo, in "gabbia di durissimo acciaio" di weberiana memoria.

L'obiettivo da perseguire è promuovere una vera e propria civiltà digitale, in cui la direzione dell'innovazione sia ancora agita e non subita dall'uomo, a partire dalla definizione delle coordinate assiologiche in cui inscrivere uno sviluppo tecnologico inclusivo, concependo il confine (anche con l'altro-da-sé) non solo come *limes*, frontiera rigida, ma sempre anche come *limen*, cioè soglia, contatto" (M. Magatti).

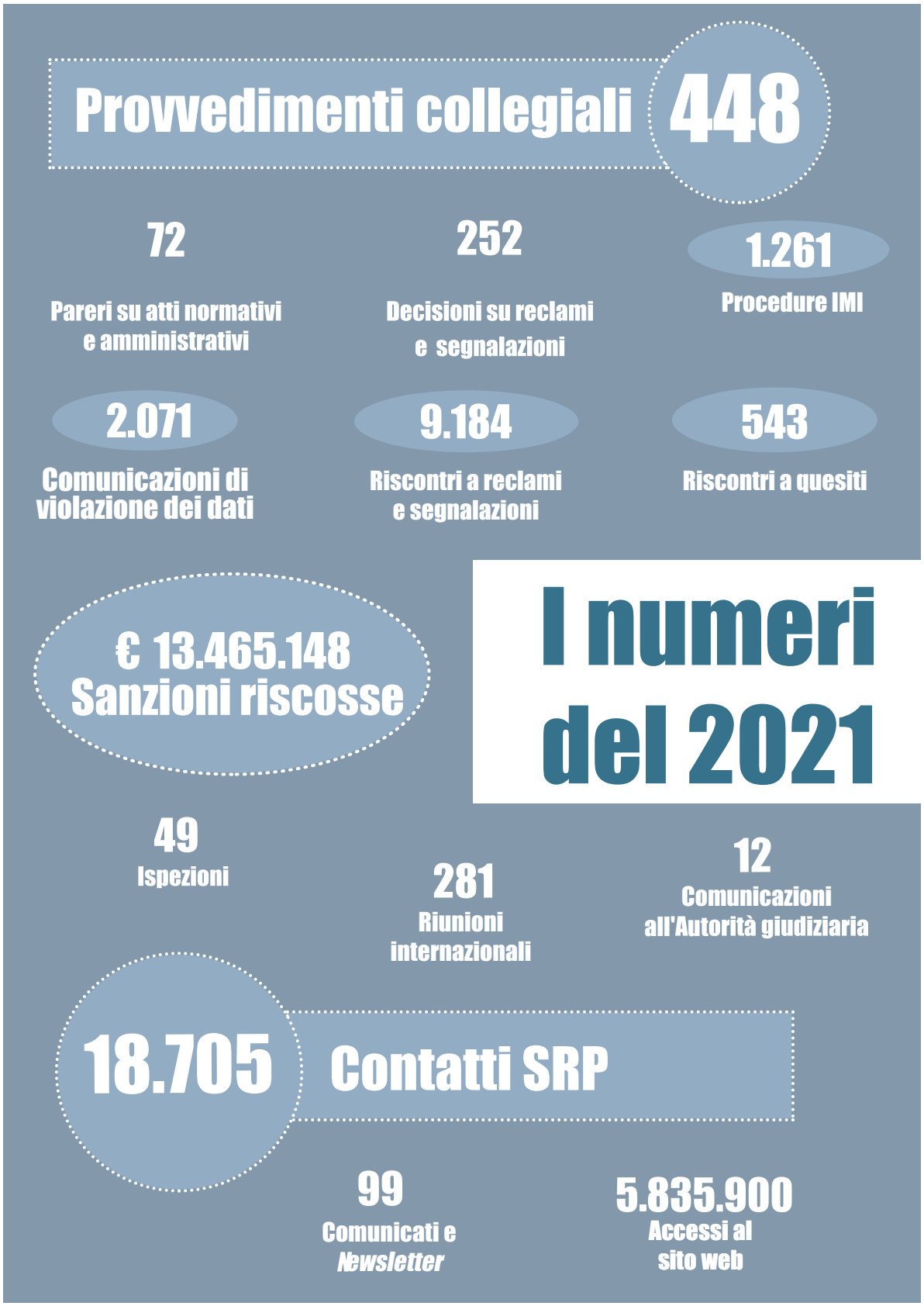
Il Garante accoglie questa sfida con senso di responsabilità e di consapevolezza dell'importanza dell'obiettivo, da perseguire grazie al lavoro costante e attento del personale tutto, che voglio qui, unitamente al Collegio e al Segretario generale, sinceramente ringraziare. E ringrazio anche le Autorità che hanno inteso offrirci, in vario modo, sostegno, nonché il corpo della Guardia di Finanza, per la ormai consueta collaborazione.

Con l'auspicio di sapere sempre, come da venticinque anni, "guardare negli occhi il destino del proprio tempo" (Max Weber).

Relazione Annuale 2021

www.gpdp.it

PAGINA BIANCA


Provvedimenti collegiali 448
72
Pareri su atti normativi e amministrativi
252
Decisioni su reclami e segnalazioni
1.261
Procedure IMI
2.071
Comunicazioni di violazione dei dati
9.184
Riscontri a reclami e segnalazioni
543
Riscontri a quesiti
€ 13.465.148
Sanzioni riscosse
I numeri del 2021
49
Ispezioni
281
Riunioni internazionali
12
Comunicazioni all'Autorità giudiziaria
18.705
Contatti SRP
99
Comunicati e Newsletter
5.835.900
Accessi al sito web

PAGINA BIANCA

Indice

Indice

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

II- L'ATTIVITÀ SVOLTA DAL GARANTE

Indice

Indice

Indice

Indice

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	*Binding corporate rules*
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
DAD	didattica a distanza
DDI	didattica digitale integrata
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
Dsu	dichiarazione sostitutiva unica
es.	esempio

FAQ	*Frequently Asked Questions*
Fse	Fascicolo sanitario elettronico
Gepd	Garante europeo per la protezione dei dati
Gruppo Art. 29	Gruppo dei garanti europei istituto 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	*Internal Market Information System*
Ivass	Istituto per la vigilanza sulle assicurazioni
IWGDPT	*International Working Group on Data Protection in Telecommunications*
l.	legge
LED	*law enforcement directive*
lett.	lettera
Mef	Ministero dell'economia e delle finanze
Mise	Ministero dello sviluppo economico
n.	numero
p.	pagina
p.a.	pubblica amministrazione/pubbliche amministrazioni
par.	paragrafo
Pec	posta elettronica certificata
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
TULPS	Testo unico delle leggi di pubblica sicurezza
UE	Unione europea
Url	*Uniform resource locator*
v.	vedi

25 1997-2022

GPDP

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

Relazione annuale 2021

PAGINA BIANCA

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

1 Introduzione

Nel quadro di un notevole incremento complessivo del volume di atti pervenuti all'Autorità (segnalazioni/reclami, quesiti, richieste di parere, di accesso agli atti) e da questa formati (sez. IV, tab. 1) – il protrarsi per il secondo anno dello stato di emergenza sanitaria dà solo in parte conto dell'attività del Garante. Per quanto riguarda, in particolare, i dati relativi alla salute, così delicati per il singolo e rilevanti per la collettività, è stata costante l'attenzione a coniugare la protezione dei dati stessi e dei diritti fondamentali degli interessati, strettamente interconnessi nella vita quotidiana e nel disegno normativo (art. 9 del RGPD), con le esigenze che ne rendono necessario il trattamento. In un contesto caratterizzato da una importante successione di norme primarie e di disposizioni attuative, l'Autorità è stata coinvolta sulle grandi linee del trattamento dei dati nell'ambito della campagna vaccinale e delle relative certificazioni verdi, in continuo raffronto con le competenti amministrazioni, per evitare il trattamento di dati non necessari, delimitarne l'ambito di circolazione dei dati in funzione delle previsioni normative ed assicurare il rispetto delle esigenze di sicurezza dei sistemi di trattamento (par. 5.1). Parallelamente sono stati esaminati centinaia di reclami e segnalazioni rela-

1 Executive Summary

Against the backdrop of a considerable increase in the total number of cases handled by the Italian Garante – complaints, alerts, queries, requests for opinions and access to documents, see Section IV, Table 1 – the continuation of the health emergency for the second year in a row cannot account as such for the workload falling within the Authority's remit. In particular, care has been taken throughout in reconciling the need to process health data – which are valued considerably by individuals in their daily lives as well as being of great significance for society as a whole – with the protection of those data and of fundamental human rights, which are closely connected both in daily life and in the European regulatory framework (see Article 9 GDPR). In Italy, major primary law instruments regarding health data were enacted last year along with the respective implementing regulations; the Garante was involved in laying out the processing architecture in connection with the vaccination campaign and the relevant green certificates. To that end, a dialogue was kept up with the competent ministries to prevent unnecessary data from being processed, channel data flows in line with the law, and ensure the security of processing systems (para. 5.1). At the same time, hundreds of complaints

1

tivi al trattamento dei dati sulla salute nel contesto emergenziale, riguardanti in misura considerevole il mondo della scuola (par. 4.3) e del lavoro privato e pubblico (parr. 14.1. e 14.6), sfociati in taluni casi in provvedimenti prescrittivi e sanzionatori.

Di questo quadro fa parte l'attivo contributo del Garante in seno al Cepd (cfr. art. 68 e segg. del RGPD), che insieme al Gepd, in particolare con un parere sulle proposte di regolamento UE (par. 23.1) ha evidenziato che l'uso del certificato verde digitale non può in alcun modo dar luogo a discriminazioni dirette o indirette nei confronti delle persone e deve essere pienamente in linea con i principi fondamentali di necessità, proporzionalità ed efficacia.

Occorre al riguardo considerare che la dimensione europea della protezione dati comporta per l'Autorità un'impegnativa partecipazione all'attività del Comitato, per quanto riguarda sia le decisioni su casi singoli, sia i pareri sulla normativa della Commissione e del Consiglio in via di elaborazione – di ampio rilievo quelli relativi alla proposta di regolamento UE sulla *governance* dei dati e alla proposta di regolamento UE sull'intelligenza artificiale (n. 5/2021) – sia le linee guida elaborate dal Comitato stesso per l'attuazione uniforme del RGPD – tra le quali vanno qui menzionate quelle sulla nozione di titolare e responsabile del trattamento, e quelle sulla composizione delle controversie ex art. 65, par. 1, lett. *a*), del RGPD, nel quadro dell'attività di interpretazione delle norme concernenti i meccanismi di cooperazione tra le autorità di protezione dati previsti dal Capo VII del Regolamento (par. 23.1).

Di grande impatto, anche in relazione all'esigenza di assicurare un adeguato livello di protezione nei Paesi terzi in cui i dati siano esportati, il parere congiunto 2/2021, espresso dal Comitato e dal Cepd, sulla decisione di esecuzione della Commissione 2021/914, relativa alle clausole contrattuali tipo per il tra-

and alerts were evaluated concerning the processing of health data in connection with the COVID-19 emergency; a substantial portion of those complaints and alerts concerned schools (para. 4.3) and private and public employers (paras. 14.1 and 14.6) and led in some cases to the taking of corrective measures and the imposition of fines.

The Garante contributed actively to the work carried on by the EDPB in this area (see Article 68 et seq. GDPR); reference should be made in this respect to the joint EDPB-EDPS opinion on the draft EU regulation concerning green certificates (para. 23.1), where it was recalled that use of the digital green certificate may in no case result into direct or indirect discrimination of individuals and must be fully in line with the fundamental principles of necessity, proportionality and effectiveness.

It should be pointed out in this regard that the European dimension of data protection requires the Garante to participate in the multifarious activities of the EDPB, which range from issuing decisions on individual cases to giving opinions on draft EU legislation – including in particular the EU draft Data Governance Act and the draft AI regulation (5/2021) – up to drafting guidance to ensure the consistent application of the GDPR. As for the latter, reference should be made here to the guidelines on the concepts of controller and processor in the GDPR and to the guidelines on dispute resolution proceedings under Article 65(1)(a) GDPR; in turn, they are part of a broader set of documents that were issued to provide interpretive guidance on cooperation mechanisms under Chapter VII of the Regulation (para. 23.1).

Of great import was also the joint EDPB-EDPS Opinion 2/2021 on the Commission's implementing decision 2021/914, concerning standard contractual clauses for the transfer of personal data to third countries under the GDPR, partly in light of the need to

sferimento di dati personali verso Paesi terzi a norma del Regolamento (quanto all'esigenza di adeguate garanzie con riferimento al trasferimento di dati personali verso Paesi terzi, v. Corte di giustizia, Grande Sezione, 16 luglio 2020, C-311/18, *Data Protection Commissioner* c. Facebook Ireland Ltd, Maximillian Schrems, cd. Schrems II).

L'adeguatezza della protezione offerta è da accertare anche ai sensi della direttiva 680/2016, cd. *law enforcement directive* (LED), che regola il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, per quanto riguarda il trasferimento di dati nell'ambito della cooperazione relativa ad attività di polizia e giustizia (art. 36 LED). Il Gruppo ha rilasciato un parere positivo sull'adeguatezza del Regno Unito.

Sempre con riferimento alla direttiva 680, richiede menzione il parere sfavorevole del Garante sull'utilizzo del sistema Sari *Real Time* da parte del Ministero dell'interno, per la mancanza di una base normativa che legittimi il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza (par. 8.3), in sintonia con le valutazioni al riguardo espresse, tra l'altro, in seno al Consiglio d'Europa (par. 23.1) e poi dal Comitato nel citato parere 5/2021.

Nel rinviare al seguito della trattazione per più dettagliati elementi, preme qui sottolineare il raccordo tra la quotidiana trattazione di segnalazioni e reclami e la consulenza normativa da un lato e, dall'altro, la partecipazione alle diverse articolazioni del Comitato, nelle quali l'adozione di atti di carattere generale porta a sintesi le variegate esperienze proprie delle autorità dei Paesi membri.

Da questo punto di vista si può osservare come la trasversalità tra i diversi temi, segnatamente il carattere interdisciplinare di molte decisioni, frutto in particolare di un'istruttoria relativa a

ensure an adequate level of protection in the third countries where the data are exported to. As for the adequate safeguards that must be in place to transfer personal data to third countries, account should be taken of the judgment by the CJEU, Grand Chamber, of 16 July 2020 – Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (so called Schrems-II judgment).

The adequacy of the level of protection is to be established also within the meaning of directive 2016/680, i.e., the so-called LED (Law Enforcement Directive), which regulates the processing of personal data by law enforcement authorities, insofar as personal data are transferred for the purposes of law enforcement cooperation (see Article 36 LED). The EDPB issued a favourable opinion on the adequacy of the UK law enforcement framework in this respect.

Still regarding the LED, reference should be made to the unfavourable opinion given by the Garante on use of the SARI Real Time system by the Italian Ministry of the Interior; this was due to the lack of a legal basis legitimising the automated processing of biometric data for facial recognition purposes in a security context (para. 8.3) and was in line with the assessment made in this connection both by the Council of Europe (para. 23.1) and by the EDPB via the aforementioned Opinion 5/2021.

Additional details can be found in the relevant sections of this Annual Report; suffice it to say here that there is a close link between the daily handling of complaints and alerts and the provision of expert opinions, on the one hand, and the participation in the different forums of the EDPB, on the other hand, where the multifarious experiences of Member States' supervisory authorities are pooled into acts of a general nature that are ultimately adopted by those forums.

From this perspective, one should observe that standing features of the Garante's activities do consist in the over-

1

profili giuridici e di tecnologie dell'informazione, e l'intersecarsi dei diversi piani di lavoro, interno ed europeo, istituzionale e rivolto alla trattazione del singolo caso, costituiscano una chiave di lettura dell'attività del Garante.

Ed in questa prospettiva le decisioni nei singoli casi delle diverse autorità di supervisione hanno carattere non solo nazionale ma, funzionalmente, anche europeo, perché il sistema dell'autorità capofila (*Lead Authority*) – che per i trattamenti collegati con più ordinamenti viene individuata in relazione allo stabilimento principale del titolare del trattamento – è volto sia ad acquisire al procedimento le valutazioni delle diverse autorità interessate (v. art. 60 del RGPD) – sia ad assicurare che tutte riconoscano la competenza di quella che nel caso concreto adotta la decisione. Il meccanismo è complesso, e per precisare i rapporti tra le autorità di controllo, anche per quanto riguarda il loro potere di agire in giudizio in situazioni di urgenza è intervenuta la Corte di Giustizia, 15 giugno 2021, C-645/19 sottolineando che "La ripartizione delle competenze e delle responsabilità tra le autorità di controllo, … si basa necessariamente sulla premessa di una cooperazione leale ed efficace tra tali autorità".

In tal senso si vedano i provvedimenti (par. 14.2) relativi a due società, parte di gruppi societari, operanti nel settore del *food delivery,* in relazione ad accertamenti nel corso dei quali sono emersi possibili trattamenti transfrontalieri ai sensi dell'art. 4(23) del RGPD. In relazione ad entrambi i casi oggetto di accertamento è stata riconosciuta la competenza del Garante a procedere per i trattamenti aventi impatto solo locale ai sensi dell'art. 56, par. 2, del RGPD, mentre in uno dei due casi il Garante partecipa alla procedura di cooperazione avviata dall'autorità capofila nei confronti della società capogruppo, in vista dell'adozione di una decisione concordata e vincolante (v. art. 60, par. 6, del RGPD).

arching nature of the issues addressed and, in particular, in the cross-sectoral nature of many decisions - which result from investigations into both legal and IT matters - as well as in the interactions between the individual dimensions of the SA's work which is at the same time domestic and European, high-level and case-driven.

Indeed, the decisions taken by supervisory authorities in the individual cases are not only domestic in nature, as they are actually and inherently European decisions. This is so because the lead authority mechanism, whereby the location of the controller's main establishment determines the authority that is competent for processing activities across several jurisdictions, is meant both to enable obtaining the views of the individual supervisory authorities concerned (CSAs) in the given proceeding (see Article 60 GDPR) and to ensure that all CSAs acknowledge the competence of the SA adopting the final decision in the specific case. This is a complex mechanism, and the Court of Justice of the EU provided guidance to clarify the relationships between SAs as also related to their power to seek urgent legal remedies (case C-645/19, judgment of 15 June 2021) by pointing out that 'The sharing of competences and responsibilities among the supervisory authorities is of necessity underpinned by the existence of sincere and effective cooperation.'

This is the context in which the decisions concerning two companies should be placed (para. 14.2); such companies were members of corporate groups in the food delivery sector and the investigations by the Garante brought to light possible cross-border processing activities within the meaning of Article 4(23) GDPR. In both cases the Garante's competence to handle the processing activities having only local impact was acknowledged under Article 56(2) GDPR, whilst the Garante is currently participating in the cooperation proce-

In un altro caso la decisione finale del Garante irlandese nei confronti di Whatsapp per violazione del principio di trasparenza e degli obblighi informativi di cui agli artt. 12, 13 e 14 del RGPD, con una sanzione amministrativa pari a 225 milioni, è stata adottata sulla base di una decisione vincolante del Comitato, alla cui stesura il Garante ha attivamente partecipato (par. 13.6); la procedura di risoluzione delle controversie innanzi al Comitato stesso era stata avviata dalla *Lead Authority* irlandese poiché si era rivelato infruttuoso il confronto sulle obiezioni "motivate e pertinenti" di diverse autorità, tra cui quella italiana, al primo progetto di decisione (v. Relazione 2020 p. 223).

In tutti questi casi in sede istruttoria sono stati esaminati profili non solo giuridici ma anche tecnologici.

Questi ultimi hanno un grande rilievo nei provvedimenti in materia di *data breach,* in relazione ai quali l'Autorità esamina le misure del titolare volte a porre rimedio alla violazione dei dati personali o ad attenuarne i possibili effetti negativi, se del caso rappresentando la necessità di dare agli interessati comunicazione della violazione, fornendo loro indicazioni specifiche sulle misure per proteggersi da eventuali conseguenze pregiudizievoli (cap. 18), in particolare nel caso di reti sociali che raccolgono milioni di utenti (par. 13.4), esposti al possibile utilizzo illecito dei dati (numeri di telefono, contatti, ma anche immagini idonee ad agevolare furti di identità) provenienti dalle violazioni.

Le raccolte massive di dati ad opera dei grandi operatori economici, in particolare nel settore delle Tlc, sono costantemente oggetto di attenzione, per le informazioni che i dati stessi possono fornire sulla vita privata delle persone, per la lesione del diritto alla tranquillità individuale degli interessati raggiunti da telefonate indesiderate e da altre attività di *marketing* non consentite, ma in termini di sistema anche per la capacità dell'intero fenomeno di creare un indure that was initiated in one of such cases by the lead supervisory authority against the holding company in order to jointly adopt a binding decision within the meaning of Article 60(6) GDPR.

In yet another case, the Irish SA adopted its final decision against WhatsApp – having found infringements of the transparency principle and the information obligations under Articles 12-14 GDPR – by imposing an EUR 225 million administrative fine following the binding decision that was issued by the EDPB also on the basis of the active contribution provided by the Garante (para. 13.6). The dispute resolution procedure before the EDPB had been initiated by the Irish SA since no agreement could be found on the relevant and reasoned objections raised against the initial draft decision by several SAs including the Garante (see 2020 Annual Report, p. 223).

In all the above cases the fact-finding activities focused not only on legal issues, but also on technological ones.

Technology plays a key role in the Garante's decisions concerning data breaches since the controller's measures are assessed insofar as they are intended to remedy the personal data breach or at least to mitigate its negative effects; where appropriate, the need to communicate the breach to data subjects is flagged so as to provide the latter with specific guidance on the measures to fend off possible negative consequences (Chapter 18) with particular regard to social networks (para. 13.4). Indeed, social networks collect data on millions of users who are exposed to the risk that their data – phone numbers, contacts, also images that can facilitate identity thefts – are used unlawfully following a data breach.

Massive data collections by major business operators, in particular telecom operators, are always in the spotlight. This is due to the information the data can provide on individuals' private lives as well as to the breach of data subjects'

1

dotto di illiceità che investe numerose fasi del trattamento, quali la formazione delle banche dati, la comunicazione dei dati, i criteri di acquisizione del consenso, l'esercizio dei diritti degli interessati, la sicurezza nelle comunicazioni elettroniche. Alle decisioni volte ad interdire i trattamenti illeciti si aggiungono i procedimenti diretti a controllare l'attuazione degli adempimenti prescritti in occasione di provvedimenti precedenti, in una complessa attività di accertamento anch'essa relativa sia ai profili giuridici sia a quelli inerenti le tecnologie dell'informazione (par.13.3).

Non meno complessa la supervisione dei dati trattati nel settore pubblico, in particolare da parte dell'Agenzia delle entrate (par. 4.1), per i quali particolare significato acquistano il principio di minimizzazione dei dati (art. 5, par. 1, lett. *c*), del RGPD) e la trasparenza dei trattamenti di dati, segnatamente quelli presenti nei *dataset* di analisi e di controllo, soprattutto in relazione all'attività di profilazione, in considerazione dei potenziali rischi e delle interferenze che tale attività pone per i diritti degli interessati, i quali devono essere informati sulla logica sottostante al processo decisionale fondato su trattamenti automatizzati. Di pari rilievo la concreta attuazione del principio di esattezza dei dati, per prevenire, in particolare, erronee rappresentazioni della capacità contributiva, correggendo potenziali errori o distorsioni che potrebbero verificarsi nel processo decisionale fondato su tali trattamenti.

Qui emerge la centralità istituzionale del ruolo del Garante, che pur essendo estraneo rispetto ai trattamenti di volta in volta oggetto delle sue determinazioni, ne verifica la congruenza e la rispondenza ai principi di protezione dei dati personali, in termini idonei a tutelare le situazioni giuridiche soggettive degli interessati coinvolte nel trattamento. Si tratta non solo di una sorta di razionalizzazione dei trattamenti – nell'interesse dello stesso titolare, sia per quanto ripeace caused by unsolicited phone calls and other unauthorised marketing activities. From a broader perspective, one should also consider that this phenomenon gives rise to a sequence of infringements affecting several processing phases - from the setting up of databases to the mechanisms underpinning data disclosure, the criteria for obtaining consent, the exercise of data subjects' rights, up to the security of electronic communications. Along with the decisions banning unlawful processing, other proceedings were initiated to verify implementation of the measures that had been ordered via previous decisions; this entailed complex fact-finding exercises that spanned, once again, both legal and IT issues (para. 13.3).

No less complex are the supervision activities concerning processing by public bodies, with particular regard to the National Revenue Agency (para. 4.1). Here special importance should be attached to compliance with the data minimisation principle (Art. 5(1)(c) GDPR) and to transparency of processing activities – in particular concerning analytical and control datasets mainly in connection with profiling. Account should be taken in this context of the potential risks for and interference with data subjects' rights caused by profiling, so that information on the logic underlying the decision-making based on automated processing must be provided in all cases. Effective implementation of the data accuracy principle is also paramount in order to prevent, in particular, the misrepresentation of taxable assets by rectifying errors or biases that might arise in the fully automated decision-making process.

All of this shows the pivotal role played by the Garante: though not involved in the processing activities addressed from time to time as part of its tasks, it is called upon to verify whether such processing is proportionate and compliant with personal data protection principles so as to safeguard the data

guarda il migliore svolgimento delle funzioni per le quali il trattamento dei dati è richiesto, sia per quanto attiene alla sua responsabilità nei confronti dei soggetti ai quali i dati si riferiscono – ma, in termini più generali, di garantire l'effettiva protezione dei diritti delle persone nella società dell'informazione, per consentirne il libero svolgimento della personalità degli interessati, ossia per assicurare che le interferenze con i loro diritti fondamentali siano quelle necessarie in una società democratica (cfr. art. 8 CEDU e artt. 7 e 8 CDFUE). Nei confronti degli atti di soggetti pubblici, rileva, da un punto di vista che solo in apparenza può dirsi formale, il fondamento giuridico che consente l'interferenza nella vita dell'interessato ed il trattamento dei suoi dati. Tale fondamento ora, con importante ampliamento rispetto alle precedenti disposizioni, può essere costituito non solo da norme di legge o regolamento ma anche da atti amministrativi generali, nonché dalla necessità di adempiere un compito di pubblico interesse o dall'esercizio del pubblico potere (d.l. n. 139/2021, cd. decreto capienze convertito, con modificazioni, dalla l. n. 205/2021, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali; *infra* par. 2.1). Resta fermo peraltro, ne potrebbe essere altrimenti, il rispetto dei principi del RGPD, e quindi permane l'esigenza di un corretto bilanciamento tra i diritti compresenti e, in particolare, del rispetto dei principi di pertinenza, esattezza e non eccedenza dei dati trattati. Ciò consente di cogliere appieno l'esigenza di reale indipendenza dell'Autorità, che oltre alla non sottoposizione del Garante al potere governativo di indirizzo politico, richiede la disponibilità di risorse finanziarie ed umane idonee a consentire l'effettivo svolgimento delle funzioni istituzionali, ulteriori rispetto a quelle conferite dall'art. 9, d.l. n. 139, citato.

subjects' rights as set out in the relevant legal framework. On the one hand, this can be said to translate into streamlining data processing activities in the controllers' own interest both as regards improving the performance of those functions for which the processing is intended and as for the controller's accountability to data subjects; on the other hand, the ultimate purpose is ensuring the actual protection of the rights of individuals in the information society so as to allow the free development of their personalities – i.e., ensuring that any interference with their fundamental rights is necessary in a democratic society (see Art. 8 ECHR and Articles 7 and 8 TFEU). As regards public bodies, special importance should be attached to the legal basis allowing for such interference with the data subject's life and therefore for the processing of his or her data – which is only apparently a formal issue. The scope of the legal basis in question was expanded significantly by recent amendments to the domestic legislation so that it now includes not only primary or secondary legislation, but also so-called administrative instruments of a general nature along with the necessity of the processing to perform a task in the public interest or in the exercise of official authority (see decree-law No 139/2021 as enacted and amended by Law No 205/2021 – para. 2.1). Respect for the principles set out in the GDPR is left unprejudiced, indeed it could not be otherwise; accordingly, there remains the need to strike the appropriate balance between the rights at issue with particular regard to compliance with the requirements that data shall be relevant, accurate and non-excessive. Against this backdrop one can readily perceive the need for the Garante to be truly independent. As well as being free from the political influence exerted by government, the Garante must be equipped with such financial and human resources as can allow it to fully discharge its official tasks on top of those laid down in Section 9 of the said decree No 139/2021.

1

L'esigenza di correttezza nel trattamento dei dati personali e di bilanciamento tra i diritti del titolare e quelli delle persone cui i dati si riferiscono emerge con plastica evidenza nelle decisioni che toccano i profili legati alla libertà di manifestazione del pensiero e alla ricerca di un punto di equilibrio tra la libertà di informazione e il diritto ad essere informati, da un lato, e la protezione dei dati personali e il rispetto dell'identità personale, dall'altro (par. 9.2). È costante non solo in questo settore, ma forse qui più evidente per l'essenzialità del rapporto tra i diversi valori in gioco, il dialogo con la magistratura, i cui criteri di giudizio sono tenuti presenti nella trattazione dei diversi casi, ed alla quale spetta in ultima analisi valutare la correttezza delle soluzioni adottate dall'Autorità. (Sia consentito al riguardo osservare, incidentalmente, che in questo, come negli altri ambiti, le decisioni dell'Autorità non sono soltanto quelle adottate dal Collegio e pubblicate nel sito istituzionale, ma anche le archiviazioni disposte dai diversi Dipartimenti, che quando non riguardano segnalazioni o esposti palesemente infondati comportano sempre un attento esame di quanto prospettato, ed una motivazione, sindacabile in giudizio, idonea a dar conto della scelta di non procedere con una decisione dell'organo di vertice).

Le decisioni in materia, che riguardano non solo la stampa, ma anche, in misura considerevole i motori di ricerca e i *social network* – nei quali si trovano ad essere particolarmente esposti i minori – sono di grande delicatezza da un lato perché applicano norme con fattispecie relativamente vaghe, ossia con clausole generali in relazione alle quali vanno spesso soppesate tutte le caratteristiche dei singoli casi per giungere ad una decisione persuasiva, dall'altro per le loro ripercussioni concrete sulle vite degli interessati e sull'attività degli operatori titolari del trattamento, in sintesi per quanto contribuiscono al rafforzamento di una società libera e rispettosa della

The need for personal data to be processed fairly and for the controller's rights to be reconciled with those of data subjects is exemplified most powerfully in the decisions addressing freedom of expression and the required balance between freedom to receive and impart information, on the one hand, and the protection of personal data and personal identity, on the other hand (para. 9.2). An unceasing dialogue with judicial authorities is one of the key features of the Garante's activity in this area, perhaps to a greater extent than is the case with other subject matters because of the fundamental nature of the balancing at issue. The parameters set out by case law are taken into account in handling the cases, indeed it is ultimately a judicial authority who is required to assess how sound the solutions devised by the Garante are. It should be pointed out incidentally that the decisions by the Garante do not only include those adopted by the commissioners' panel and published on the official website; in fact, cases may also be dismissed by the individual departments which carefully assess the individual claims – unless they are clearly unsubstantiated – and provide reasons for such dismissals, which can be challenged in court and must be in any case such as to account for the choice to not defer the decision to the commissioners' panel.

The decisions issued by the Garante in this sector relate not only to press media, but also – to a considerable degree – to search engines and social networks, where children are especially exposed to risks. Deciding such cases is a daunting task because the applicable provisions are quite high-level in nature, i.e., they contain general clauses that have to be adapted carefully to the specifics of the individual cases in order to attain a convincing decision; on the other hand, these decisions have factual repercussions on data subjects' lives as well as on controllers' activities – in short, they are expected to contribute to enhancing individual freedom and respect of individ-

persona. Lo indica, in particolare, per quanto riguarda l'interesse a conoscere i dettagli di un fatto risalente, l'accoglimento di un reclamo che lamentava la pubblicazione di dati idonei ad identificare l'interessata all'interno di un articolo che ripercorreva i momenti principali di una vicenda in cui la stessa era stata coinvolta molti anni prima come autrice di un reato grave. L'Autorità ha ritenuto che la rinnovata pubblicazione di notizie relative a vicende risalenti nel tempo, non determinata da ragioni di attualità, costituisca invero esplicazione di un'attività storiografica che non richiede la divulgazione dei dati identificativi dei protagonisti, a meno che i fatti non riguardino personaggi che rivestano o abbiano rivestito un ruolo pubblico ovvero non implichino il richiamo necessario ai nomi dei protagonisti stessi (par. 9.2.3).

In questo quadro si colloca la novità normativa che, similmente alle disposizioni sul cyberbullismo (l. n. 71/2017), ha attribuito al Garante la tutela, con apposita procedura di urgenza, nei confronti di atti di *revenge porn* (d.l. n. 139/2021, convertito, con modificazioni, dalla l. n. 205/2021 - par. 2.1, cap. 11). Si tratta con ogni evidenza, della conferita possibilità di intervenire tempestivamente a protezione degli interessati, per ridurre, se non azzerare, i danni che possono derivare dalla diffusione e dalla persistenza in rete di immagini e situazioni intime. Anche qui emerge con chiarezza l'intreccio tra i profili giuridici e tecnologici che spesso caratterizza l'oggetto dell'attività del Garante ma anche la dimensione nella quale questo agisce, in relazione ai trattamenti di dati tramite tecnologie che, per la loro continua evoluzione, sarebbe improprio definire di ultima generazione. Queste, anche ma non solo in relazione al trattamento dei dati biometrici, ai quali si è fatto cenno, nella dimensione dell'intelligenza artificiale pongono al Garante, per la ricchezza, la molteplicità ma anche la pervasività delle possibili applicazioni, sul piano culturale, prima ancora che

uals' rights in our society. As regards in particular the interest in knowing details of past events, reference can be made to a decision that granted a complaint against the publication of data making the complainant identifiable in a news article; the latter summarised a case in which the complainant – who had committed a serious criminal offence – had been involved several years before. The Garante found that the publication of information relating to facts dating back to the remote past and devoid of any topicality was actually an instance of processing for historical purposes and did not require disclosing data such as to make the individuals involved identifiable – unless the facts at issue concerned individuals who were or had been public figures or entailed, by necessity, referring to the names of those individuals (para. 9.2.3).

Mention should be made in this context of the legislation that recently empowered the Garante to take urgent measures via an ad-hoc procedure against revenge porn (decree No 139/2021 as enacted and amended by Law No 205/2021 – see para. 2.1 and Chapter 11). Similar measures had been envisaged by the legislation enacted against cyberbullying (Law No 71/2017). The legislation in question basically empowers the Garante to step in promptly in order to protect data subjects so as to mitigate – or do away with – the harm that can be caused by the dissemination and permanence on the Internet of highly private images and situations. The interplay of legal and technical issues that often underpins the activities by the Garante is clearly a feature also in this sector; however, this also goes to show what is the dimension of the Garante's action as related to processing by way of technologies that can hardly be labelled as last-generation given their unrelenting evolution. Indeed, those technologies raise issues to be addressed and challenges to be coped with by the Garante – more from a cultural than from a merely

praticamente, questioni da affrontare e sfide da risolvere (sui diversi interventi dell'Autorità e dei componenti il Collegio volti a favorire la conoscenza e la riflessione sulle tematiche di interesse v. par. 25.5). La rilevanza dei diritti degli interessati a fronte di trattamenti elaborati con tecnologie complesse è ben esemplificata dalla Suprema Corte (ord. 25 maggio 2021, n. 14381), che ha chiarito come "In tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato; ne consegue che nel caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire punteggi di affidabilità, il requisito della consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati" (*infra* par. 22.3).

***

Il testo di seguito dà conto diffusamente di ciò che in questa sommaria sintesi si è tratteggiato cercando soprattutto di indicare la prospettiva dalla quale muove l'Autorità. Giova aggiungere che, come indicano alcuni cenni in questa introduzione, ma meglio chiarisce la Relazione nei vari approfondimenti, il RGPD responsabilizza da un lato i titolari dei diversi trattamenti ma dall'altro, in linea con la previgente normativa, gli interessati, la cui attiva partecipazione è essenziale per giungere al livello di protezione adeguato alle complessità con le quali costantemente si misura la società ed in essa il Garante.

practical perspective – in terms of the wide-ranging gamut, multifariousness, and pervasiveness of their applications including, but without being limited to, the processing of biometric data (as mentioned above) by way of AI techniques. (Details on the various activities by the Garante and the individual commissioners aimed to raise awareness of and spark a public debate on these issues can be found in para. 25.5). The importance to be attached to data subjects' rights in the presence of processing activities that rely on complex technologies was aptly recalled by the judgment of the Court of Cassation No 14381 of 25 May 2021, which clarified that 'When personal data are processed, consent is only valid if it is given freely and with specific regard to a processing activity that is identified unambiguously. Therefore, the requirement of informed consent cannot be said to be met in the case of a web-based platform (and the relevant IT database) that is intended to work out reputational profiles of natural and legal persons by way of a computing mechanism based on a reliability scoring algorithm, if the data subjects are left in the dark about or are unable to know the implementing logic and the components of such algorithm.' (see para. 22.3).

***

The Annual Report will provide further insights into the topics that were touched upon in this executive summary, which is meant above all to shed light on the rationale of the approach followed by the Garante. It should only be added that – as briefly recalled in the foregoing paragraphs and better explained in the individual sections of the Report – the GDPR focuses on the accountability of controllers whilst leveraging, on the other hand, the active role to be played by data subjects, which is fundamental in order to achieve a level of safeguards that is adequate to the complex challenges faced by society at large and as a consequence also by the Garante.

2 Il quadro normativo in materia di protezione dei dati personali

Nel 2021 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. *I decreti-legge*

Il cd. decreto capienze

Il decreto-legge n. 139/2021, convertito, con modificazioni, dalla legge n. 205/2021, ha introdotto modifiche significative alla disciplina di protezione dei dati personali, con novelle incidenti tanto sul Codice quanto sulla normativa complementare.

Il disegno di legge di conversione, peraltro, ha apportato rilevanti modifiche al testo originario del decreto-legge, estendendone il contenuto in gran parte anche sulla base delle indicazioni fornite dal Garante in sede di audizione dinanzi alla 1ª Commissione del Senato.

Si illustrano, di seguito, le disposizioni più rilevanti in termini di protezione dei dati:

a) Trattamento di dati personali a fini di pubblico interesse.

L'articolo 9, comma 1, lett. *a*), ha novellato l'art. 2-*ter* del Codice prevedendo, in particolare, che la base giuridica del trattamento dei dati comuni nei casi previsti dall'art. 6, par. 3, lettera *b*), del RGPD (ovvero i trattamenti necessari per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di funzioni e poteri pubblici), possa consistere, oltre che nella legge e nel regolamento (con soppressione del vincolo della necessaria predeterminazione legislativa dei casi di delega regolamentare), anche in atti amministrativi generali.

Tuttavia, pur senza derogare a questa previsione, il comma 1-*bis* inserito nel corpo dell'art. 2-*ter* ammette anche, quale presupposto di liceità dei trattamenti di dati comuni svolti da p.a. (ivi incluse le autorità amministrative indipendenti), da società a controllo pubblico statale o gestori di servizio pubblico locale ad eccezione delle attività svolte in regime di libero mercato, la necessità dell'adempimento del compito di pubblico interesse o dell'esercizio del pubblico potere. Una apposita clausola fa salvo ogni altro obbligo previsto dal RGPD e dal Codice, ed è esplicitamente previsto il rispetto dell'art. 6 del RGPD. Il medesimo autonomo presupposto di liceità riguarda anche la comunicazione di dati comuni fra titolari sempre in ambito pubblico (è soppressa la previsione dell'interpello del Garante ai fini dell'autorizzazione, anche con silenzio-assenso, di ipotesi di comunicazione di dati tra soggetti pubblici, non normativamente previste).

La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità, può invece avvenire solo dopo il decorso del termine di dieci giorni dalla comunicazione che le amministrazioni sono tenute ad effettuare al Garante.

La disposizione transitoria prevede che il nuovo regime di trattamento dei dati,

2

con estensione delle basi giuridiche agli atti amministrativi generali, si applichi anche alle vigenti disposizioni legislative che a tali fini rinviino ad atti regolamentari.

Analoga ricomprensione degli atti amministrativi generali nella categoria dei presupposti di liceità del trattamento si opera con riguardo ai trattamenti di dati per fini di sicurezza nazionale e difesa (pur con necessaria previsione regolamentare delle disposizioni attuative: art. 58 del Codice), nonché ai trattamenti di dati non appartenenti a categorie particolari, per fini di polizia e giustizia penale, le cui previsioni generali saranno contenute rispettivamente in un decreto ministeriale (dell'interno e della giustizia), anziché in un decreto del Presidente della Repubblica unitario (art. 5, d.lgs. n. 51/2018). Anche in tal caso opera la disposizione transitoria su descritta.

b) Trattamento di dati appartenenti a categorie particolari per motivi di interesse pubblico rilevante.

Analogamente alla novella dell'art. 2-*ter* del Codice, anche in questo caso si prevede che la base giuridica del trattamento possa essere costituita, oltre che dalla legge e dal regolamento (con soppressione del vincolo della necessaria predeterminazione legislativa dei casi di delega regolamentare), anche da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. La disposizione transitoria prevede che il nuovo regime di trattamento dei dati, con estensione delle basi giuridiche agli atti amministrativi generali, si applichi anche alle vigenti disposizioni legislative che a tali fini rinviino ad atti regolamentari.

Con il comma 1-*bis* inserito nell'articolo si è previsto che i dati personali relativi alla salute, privi di elementi identificativi diretti e sempre nel rispetto delle finalità istituzionali di ciascuna amministrazione, possano essere trattati dal Ministero della salute, dall'Istituto superiore di sanità, dall'Agenzia nazionale per i servizi sanitari regionali, dall'Agenzia italiana del farmaco, dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà e, relativamente ai propri assistiti, dalle regioni, anche mediante l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Ssn, ivi incluso il Fse, rinviando, per quanto concerne le modalità di interconnessione e l'indicazione delle finalità del trattamento, a un decreto del Ministro della salute da adottarsi previo parere del Garante, nel rispetto di quanto previsto dal RGPD, dal Codice, dal Cad e dalle linee guida dell'AgID in materia di interoperabilità delle basi dati.

La disposizione transitoria prevede che il nuovo regime di trattamento dei dati, con estensione delle basi giuridiche agli atti amministrativi generali, si applichi anche alle vigenti disposizioni legislative che a tali fini rinviino ad atti regolamentari.

c) Provvedimenti prescrittivi di carattere generale e *data retention.*

Il decreto-legge, già nel suo testo originario, ha abrogato l'art. 2-*quinquiesdecies* del Codice, relativo al potere prescrittivo del Garante – da esercitarsi anche mediante provvedimenti di carattere generale – in ordine a trattamenti svolti per l'esecuzione di un compito d'interesse pubblico, suscettibili di presentare rischi elevati. A fronte di tale abrogazione, l'art. 9, comma 1, lett. *e*), del d.l., come convertito dalla l. n. 205/2021, ha attribuito al Garante un potere prescrittivo generale con riferimento alla *data retention*. Novellando il comma 5 dell'art. 132 del Codice si è, in particolare, previsto che il Garante disciplini, con un provvedimento di carattere generale, le modalità con le quali i fornitori di servizi telefonici sono tenuti a trattare i dati relativi al traffico telefonico e al traffico telematico per le finalità di accertamento e repressione di reati previste dall'articolo medesimo (cfr. par. 13.2).

d) *Revenge porn.*

Inserendo nel corpo del Codice l'art.144-*bis,* in materia di *revenge porn,* il decreto-legge ha attribuito al Garante – sul paradigma di quanto già disposto dalla l. n. 71/2017 in materia di cyberbullismo – la specifica competenza di accordare una peculiare tutela preventiva avverso condotte riconducibili a tale fenomeno. In particolare, si prevede che chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso, possa segnalarne il pericolo al Garante (senza che l'invio di documentazione a sostegno integri il delitto di cui all'art. 612-*ter* c.p.). L'Autorità, nelle quarantotto ore dal ricevimento della richiesta, decide sull'istanza (che nel caso di minori è avanzata dai genitori o dagli esercenti la responsabilità genitoriale o la tutela, in via alternativa rispetto all'interessato solo per ultraquattordicenni). Si prevede inoltre che i gestori delle piattaforme destinatari dei provvedimenti dell'Autorità conservino il materiale oggetto della segnalazione, a soli fini probatori e con misure, indicate dal Garante, idonee a impedire la diretta identificabilità degli interessati, per dodici mesi. La norma legittima inoltre il Garante a disciplinare, con proprio provvedimento, specifiche modalità di svolgimento dei procedimenti di decisione sulle istanze in questione. Al fine di garantire l'effettività della tutela introdotta dalla norma, si impone ai fornitori di servizi di condivisione di contenuti audiovisivi, ovunque stabiliti, eroganti servizi accessibili in Italia, d'indicare senza ritardo al Garante o pubblicare sul proprio sito internet (con rilevanza amministrativa della condotta omissiva), un recapito da utilizzare per la comunicazione dei provvedimenti relativi alle istanze. La disposizione transitoria prevede che tale obbligo sia, in sede di prima attuazione, adempiuto nel termine di sei mesi dall'entrata in vigore della norma stessa.

Il coordinamento con l'attività dell'Autorità giudiziaria è assicurato dalla previsione secondo cui l'eventuale acquisizione, da parte del Garante, nell'ambito dell'esame delle segnalazioni in questione, di notizia della consumazione (o del tentativo) del reato di cui all'art. 612-*ter* nei casi di procedibilità d'ufficio, lo obbliga a trasmettere al pubblico ministero la segnalazione ricevuta e la documentazione acquisita.

e) Delitto d'inosservanza dei provvedimenti del Garante.

Il delitto di cui all'art. 170 del Codice e all'art. 45, d.lgs. n. 51/2018 viene trasformato da reato di mera inosservanza, di pericolo astratto e con bene giuridico primario riferibile all'effettività dei provvedimenti del Garante, in reato contro la persona, di evento (di danno) costituito dal concreto nocumento arrecato a uno o più soggetti interessati, procedibile a querela della persona offesa.

La modifica valorizza anche le specificità della condotta rispetto a quella integrante gli estremi del corrispondente illecito amministrativo.

f) Procedimentalizzazione del parere del Garante.

Con alcune modifiche all'art. 154 del Codice, si prevede che il parere del Garante su atti normativi primari debba essere espresso nei soli casi in cui la legge o la norma regolamentare in corso di adozione disciplini in modo espresso il trattamento dei dati personali, descrivendo una o più operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Si prevede che il parere venga reso anche nei casi in cui la legge in corso di

2

adozione autorizzi espressamente un trattamento di dati personali da parte di soggetti privati, senza tuttavia rinviare la disciplina delle modalità del trattamento a fonti sotto ordinate. Tale ultima previsione è finalizzata a consentire l'intervento del Garante anche nei casi in cui l'assenza di provvedimenti attuativi della norma legislativa determinerebbe, di fatto, l'impossibilità di pronuncia del Garante.

In ordine alle modalità con le quali viene sentito il Garante, analogamente a quanto disposto dall'art. 2, comma 5, d.lgs. n. 281/1997 in materia di Conferenza permanente tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano, nei casi di consultazione della Conferenza permanente Stato-Regioni, si prevede, con riguardo agli atti di iniziativa governativa, che il parere sui decreti-legge o nei casi in cui sussistano ragioni d'urgenza dichiarate dal Presidente del Consiglio dei ministri, venga reso in sede di esame parlamentare dei disegni di legge o delle leggi di conversione dei decreti-legge o in sede di esame definitivo degli schemi di decreto legislativo sottoposti al parere delle commissioni parlamentari (ciò, in particolare, positivizza la prassi consolidatasi a partire dall'entrata in vigore del d.lgs. n. 101/2018).

g) Irrogazione di sanzioni in assenza di previa contestazione.

Il potere di irrogazione di sanzioni amministrative in assenza di previa contestazione per incompatibilità con la natura e il fine del provvedimento, viene limitato – relativamente agli illeciti ascritti a p.a., società a controllo pubblico statale o gestori di servizio pubblico locale ad eccezione delle attività svolte in regime di libero mercato, titolari di trattamenti svolti per fini di sicurezza nazionale e pubblica, difesa, accertamento e prevenzione dei reati – ai casi nei quali sussista un pregiudizio attuale, effettivo e concreto derivante dalla violazione, che deve essere esplicitato in motivazione (art. 166, comma 5, del Codice).

h) Sanzioni accessorie e promozione della cultura della protezione dati.

Con una novella all'art. 166, comma 7, del Codice, si introduce una specifica sanzione accessoria, suscettibile di irrogazione da parte del Garante, consistente nell'obbligo di realizzare campagne di comunicazione istituzionale volte alla promozione della consapevolezza del diritto alla protezione dei dati personali, sulla base di progetti previamente approvati dal Garante e che tengano conto della gravità della violazione.

Inoltre, tra i parametri di commisurazione infraedittale della sanzione ai sensi dell'art. 83, par. 2, del RGPD, si introduce, quale criterio a favore del trasgressore, anche la realizzazione di campagne di comunicazione istituzionale volte alla promozione della consapevolezza del diritto alla protezione dei dati personali, realizzate anteriormente alla commissione della violazione.

i) Metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione.

L'articolo 9, comma 4, del decreto-legge ha introdotto una specifica novella all'art. 7, d.l. 19 maggio 2020, n. 34 convertito, con modificazioni, dalla l. 17 luglio 2020, n. 77, che autorizza il Ministero della salute al trattamento di dati relativi alla salute dei cittadini al fine di sviluppare metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione.

La norma prevedeva già che il Ministero della salute, nell'ambito dei compiti di cui all'art. 47-*ter,* d.lgs. 30 luglio 1999, n. 300 e, in particolare, delle funzioni relative a indirizzi generali e di coordinamento in materia di prevenzione, diagnosi, cura e riabilitazione delle malattie, nonché di programmazione tecnico sanitaria di rilievo nazionale e indirizzo, coordinamento, monitoraggio dell'attività tecnico sanitaria regionale, potesse trattare dati personali, anche relativi alla salute degli assistiti, raccolti nei sistemi informativi del Ssn, per lo sviluppo di metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione, secondo le modalità di cui al decreto del Ministro della salute 7 dicembre 2016, n. 262.

2

La novella consente il trattamento, da parte del Ministero della salute, anche di dati ulteriori e diversi da quelli sanitari, laddove comunque necessari a garantire l'effettivo perseguimento delle finalità di cui all'art. 7 e, dunque, lo sviluppo del sistema predittivo dell'evoluzione del fabbisogno di salute della popolazione, oggetto di uno dei progetti della missione 6 del Piano nazionale di ripresa e resilienza (Pnnr) approvato con la decisione di esecuzione del Consiglio del 13 luglio 2021. Si introduce comunque una clausola di salvaguardia rispetto a quanto previsto dall'art. 105 del Codice, che vieta l'utilizzo di dati trattati per finalità di ricerca o per fini statistici in vista dell'adozione di provvedimenti che riguardano singoli interessati o per scopi di altra natura.

Parallelamente alle modifiche apportate all'art. 2-*sexies* del Codice, si prevede inoltre, che le modalità del trattamento siano disciplinate dal Ministro della salute con provvedimento di natura non regolamentare, da adottarsi previo parere del Garante.

Si autorizza, infine, l'interconnessione dei sistemi informativi su base individuale del Ssn, ivi incluso il Fse, con i sistemi informativi gestiti da altre p.a. che raccolgono i dati non relativi alla salute specificamente individuati dal decreto di cui sopra, con modalità tali da garantire che l'interessato non sia direttamente identificabile.

i) *Telemarketing*.

Con una modifica alla legge n. 5/2018 si è esteso, alle chiamate automatizzate, l'effetto revocatorio dei consensi precedenti, derivante dall'iscrizione nel Registro pubblico delle opposizioni.

Questo risultato viene conseguito senza alterare – come richiesto dal Garante più volte – il doppio regime (*opt-out* per le chiamate con operatore e *opt-in* per le chiamate automatizzate) previsto dal Codice. Ne deriva una maggiore tutela per gli utenti, pur nell'invarianza delle garanzie offerte dal regime di *opt-in*, che resta applicabile alle chiamate automatizzate.

La modifica è stata poi seguita dall'approvazione definitiva del regolamento attuativo della legge n. 5/2018, che ha potuto recepire l'innovazione introdotta a livello legislativo.

j) Riconoscimento facciale.

L'articolo 9, comma 9, del decreto-legge – riproponendo nelle linee generali la proposta di legge dell'On. Sensi AC 3009 – ha disposto una moratoria, fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023, dell'installazione e dell'utilizzazione di sistemi di riconoscimento facciale con rilevazione biometrica, in luoghi pubblici o aperti al pubblico. Sono sottratte alla moratoria l'installazione e l'utilizzazione di tali sistemi da parte dell'Autorità giudiziaria o, in presenza di parere favorevole del Garante in sede di consultazione preventiva, delle autorità di polizia.

k) Norme organizzative.

L'articolo 9, comma 1, lett. *l*), del decreto-legge ha, infine, introdotto alcune modifiche di natura organizzativa rilevanti per l'Autorità, in relazione alla pianta organica e al trattamento economico del personale e dei componenti il Collegio.

Data retention

L'articolo 1, del decreto-legge n. 132/2021, convertito, con modificazioni, dalla legge n. 178/2021, ha introdotto un'innovazione importante della disciplina dell'acquisizione – ai fini dell'utilizzo in procedimenti penali – dei tabulati telefonici e telematici.

A tale novella (che incide direttamente sul testo dell'art. 132 del Codice) era sottesa l'esigenza di adeguare la normativa in materia ai principi sanciti dalla sentenza CGUE 2 marzo 2021, C-746/18, con cui si è ribadito che l'acquisibilità processuale dei dati di traffico va da un lato limitata ai soli procedimenti per gravi reati o per

2

gravi minacce per la sicurezza pubblica e, dall'altro, va subordinata all'autorizzazione di un'autorità terza rispetto all'autorità pubblica richiedente. A tali principi non pareva conforme la disciplina italiana (art. 132 del Codice), nelle parti in cui, per un verso, assegnava alla gravità dei reati la sola funzione di regolare la distanza cronologica dell'acquisizione e non la sua ammissibilità e, per altro verso, attribuiva al pubblico ministero la competenza all'acquisizione dei tabulati, in assenza del vaglio del giudice.

Condividendo l'esigenza di un intervento legislativo, con segnalazione 22 luglio 2021 il Garante invitava pertanto il legislatore a "differenziare condizioni, limiti e termini di conservazione dei dati di traffico telefonico e telematico in ragione della particolare gravità del reato per cui si proceda, comunque entro periodi massimi compatibili con il su richiamato principio di proporzionalità", subordinandone l'acquisizione "all'autorizzazione del giudice, ferma restando, nei casi d'urgenza, la possibilità per il pubblico ministero di provvedervi con proprio decreto, soggetto a convalida solo in fase successiva, sul modello dell'articolo 267, comma 2, c.p.p." Analoghe indicazioni erano state espresse anche dall'o.d.g. 9/2670-A/10 a prima firma dell'On. Costa, accolto dal Governo, nella seduta del primo aprile dell'assemblea della Camera in sede di esame del disegno di legge europea 2019-2020.

In linea con tali indicazioni, il decreto-legge ha disposto, all'art. 1, la piena giurisdizionalizzazione della procedura di acquisizione e la delimitazione dell'ambito oggettivo di applicazione della procedura stessa, esperibile solo nell'ambito dei procedimenti per reati connotati da una determinata gravità, in presenza di sufficienti indizi e della rilevanza dell'acquisizione ai fini dell'accertamento dei fatti.

Ai fini della definizione della gravità dei reati per i quali si ammette l'acquisizione dei tabulati, rileva la previsione della comminatoria edittale massima di tre anni, combinata con i parametri, da apprezzare in concreto, della sufficienza indiziaria e della rilevanza investigativa del dato da acquisire, con la previsione *ad hoc* dei reati di minaccia e molestie telefoniche.

Anche la disciplina della procedura d'urgenza salvaguarda, pur nella peculiarità che ne caratterizza l'oggetto, l'esigenza della giurisdizionalizzazione piena della procedura acquisitiva e della sua limitazione ai soli reati connotati da sufficiente gravità.

Il decreto-legge replica inoltre la previsione (prima presente al comma 3 dell'art. 132) dell'applicabilità della disciplina di cui all'art. 2-*undecies,* comma 3, periodi da terzo a quinto del Codice, nei casi di esercizio dei diritti di cui agli artt. da 12 a 22 del RGPD; esercizio in questi particolari casi demandato al Garante in vece dell'interessato in presenza di esigenze (anche) pubblicistiche prevalenti.

In sede di conversione è stata, inoltre, espressamente prevista l'inutilizzabilità dei dati acquisiti in violazione delle regole di acquisizione (ordinaria e d'urgenza) su descritte. Sempre con l'esame parlamentare è stata, peraltro, introdotta una disciplina transitoria che condiziona l'utilizzabilità processuale, a carico dell'imputato, dei tabulati già acquisiti prima della data di entrata in vigore della novella, alla concorrenza di altri elementi di prova ed alla esclusiva finalizzazione all'accertamento dei reati per i quali, secondo la disciplina "a regime", l'acquisizione è ammessa.

Inoltre, con una novella di valenza più generale, relativa al contenuto del decreto del giudice che autorizza le intercettazioni mediante captatore informatico (cd. *trojan*), si è previsto che le ragioni, da indicare nel decreto stesso, quali presupposti che rendono necessaria tale modalità per lo svolgimento delle indagini, debbano essere "specifiche".

Le certificazioni verdi in materia di Covid-19

La disciplina delle certificazioni verdi – costruitasi per stratificazioni successive, con estensioni e modifiche progressive – ha avuto riflessi importanti sulla protezione dati e, anzi, ha potuto registrare, anche grazie al costante dialogo con l'Autorità, una

complessiva evoluzione verso soluzioni ispirate a un più corretto bilanciamento tra sanità pubblica e *privacy*.

La normativa in materia è stata arricchita in base a disposizioni susseguitesi in pochi mesi, modulate sull'andamento epidemico e fondate tutte sulla comune matrice impressa dalla disciplina europea, con il regolamento (UE) 2021/953.

Le certificazioni verdi – che nella loro versione base attestano una condizione di guarigione, negatività al tampone o avvenuta vaccinazione – sono state prima concepite quale requisito per gli spostamenti tra regioni di "colore" diverso (d.l. n. 52/2021, convertito con modificazioni dalla l. n. 87/2021), poi per la fruizione di servizi o lo svolgimento di attività ritenute a rischio epidemico particolare (d.l. n. 105, convertito con modificazioni dalla l. n. 126/2021), quindi per la scuola, i trasporti, il personale esterno anche delle rsa (dd.ll. nn. 111 e 122 convertito con modificazioni e, rispettivamente, abrogato dalla l. n. 133/2021) e, infine, per il lavoro in ambito pubblico e privato (d.l. n. 127, convertito con modificazioni dalla l. n. 165/2021). Con il d.l. n. 172/2021, convertito, con modificazioni, dalla l. n. 3/2022 si è introdotta una differenziazione, all'interno della comune categoria delle certificazioni verdi, tra quelle base e quelle rafforzate, derivanti da vaccino o guarigione, richieste in contesti ritenuti a maggior rischio epidemico.

Lungo il corso dell'evoluzione che ha caratterizzato la disciplina in materia, il sistema del *green pass* nazionale si è perfezionato sotto il profilo della protezione dati, anzitutto circoscrivendo in maniera più puntuale l'ambito oggettivo di applicazione della misura anche considerandone l'incidenza su materie coperte da riserva di legge statale: profilassi internazionale, autodeterminazione terapeutica – relativamente all'esigenza di evitare discriminazioni nei confronti di quanti non possano o non vogliano vaccinarsi – e, appunto, protezione dati. È significativa, in particolare, la previsione, aggiunta in sede di conversione del d.l. n. 105/2021, secondo cui "Ogni diverso o nuovo utilizzo delle certificazioni verdi Covid-19 è disposto esclusivamente con legge dello Stato" (art. 9, comma 10-*bis*, d.l. n. 52/2021).

Nel corso dell'esame parlamentare del decreto-legge n. 52 e, poi, dei dd.ll. successivi che hanno esteso l'ambito di applicazione delle certificazioni verdi, in particolare, si è conferita maggiore determinatezza alla disciplina anche sotto il profilo dell'"architettura" del trattamento. Si sono, in particolare, individuati i soggetti istituzionali cui compete la responsabilità della gestione della piattaforma nazionale *Digital Green Certificate* (DGC), in ottemperanza al principio di trasparenza che impone un'adeguata informazione degli interessati circa le caratteristiche essenziali del trattamento, rendendo così anche possibile l'esercizio dei diritti loro riconosciuti.

Inoltre, in virtù delle misure introdotte con il d.P.C.M. 17 giugno 2021, attuativo dell'art. 9, comma 10, si è potuto garantire che oggetto della verifica – mediante l'*app* ufficiale Covid-19 – sia (oltre al nome, al cognome e alla data di nascita) il solo QR *code* attestante il possesso di una certificazione in corso di validità, senza alcun riferimento al presupposto del certificato (vaccinazione, guarigione, tampone). Si evita, in tal modo, un'indebita conoscenza, da parte di terzi, della condizione sanitaria o, comunque, delle scelte vaccinali del soggetto. Al fine di minimizzare l'impatto del trattamento, si è poi espressamente esclusa la raccolta, da parte dei soggetti verificatori, dei dati dell'intestatario della certificazione (art. 13, comma 5, d.P.C.M. 17 giugno 2021). La circolare del Ministero dell'interno del 10 agosto 2021 ha poi chiarito che l'identificazione dell'intestatario della certificazione, mediante raffronto con il documento d'identità, ai sensi dell'art. 13, comma 4, d.P.C.M. 17 giugno, non deve intendersi come sistematica, ma va svolta su base discrezionale e, in particolare, nei casi di manifesta incongruenza con i dati anagrafici contenuti nella certificazione.

2

Uno snodo particolare nell'evoluzione della disciplina è stato segnato dai dd.ll. nn. 127 e 172/2021. Con il primo, infatti, il possesso della certificazione verde è assurto a requisito necessario per l'effettuazione della prestazione lavorativa, mentre con il secondo si è introdotta la distinzione già descritta tra certificazione-base e certificazione-rafforzata, in ragione del presupposto di rilascio della stessa. L'ambito di utilizzo del cd. super *green pass* è stato poi esteso per effetto delle disposizioni di cui al d.l. n. 229/2021, abrogato, pur con salvezza di effetti, dal d.l. n. 221/2021.

Una previsione non scevra da criticità, sotto il profilo della protezione dati, introdotta in sede di conversione del d.l. n. 127, è quella relativa alla possibilità di consegna, da parte dei lavoratori dei settori pubblico e privato, di copia della certificazione verde, al datore di lavoro, con la conseguente esenzione, dai controlli, per tutta la durata della validità del certificato. Per effetto del rinvio, all'art. 9-*quinquies*, comma 5, d.l. n. 52/2021, contenuto al comma 5 dell'art. 9-*sexies* del medesimo d.l., la stessa facoltà è prevista per i magistrati.

Come sottolineato nella segnalazione dell'11 novembre 2021, la prevista esenzione dai controlli – in costanza di validità della certificazione verde – rischia di determinare la sostanziale elusione delle finalità di sanità pubblica complessivamente sottese al sistema del *green pass*. Esso è, infatti, efficace a fini epidemiologici nella misura in cui il certificato sia soggetto a verifiche periodiche sulla sua persistente validità; ciò che è reso possibile dal costante aggiornamento, mediante la piattaforma nazionale DGC, dei certificati in base alle risultanze diagnostiche eventualmente sopravvenute.

L'assenza di verifiche durante il periodo di validità del certificato non consentirebbe, di contro, di rilevare l'eventuale condizione di positività sopravvenuta in capo all'intestatario del certificato, in contrasto, peraltro, con il principio di esattezza cui deve informarsi il trattamento dei dati personali (art. 5, par.1, lett. *d*), del RGPD). La nuova previsione, nella misura in cui rischia di precludere la piena realizzazione delle esigenze sanitarie sottese al sistema del *green pass,* rende quindi anche il trattamento dei relativi dati non del tutto proporzionato (perché non pienamente funzionale rispetto) alle finalità perseguite.

Inoltre, la prevista conservazione (di copia) delle certificazioni verdi contrasta con il cons. 48 del regolamento (UE) 2021/953 il quale, nel sancire un quadro di garanzie omogenee, anche sotto il profilo della protezione dati, per l'utilizzo delle certificazioni verdi in ambito europeo, dispone che "laddove il certificato venga utilizzato per scopi non medici, i dati personali ai quali viene effettuato l'accesso durante il processo di verifica non devono essere conservati, secondo le disposizioni del presente regolamento".

Tale divieto è funzionale, essenzialmente, a garantire la riservatezza non solo dei dati sulla condizione clinica del soggetto (in relazione alle certificazioni da avvenuta guarigione), ma anche delle scelte da ciascuno compiute in ordine alla profilassi vaccinale. Dal dato relativo alla scadenza della certificazione può, infatti, agevolmente evincersi anche il presupposto di rilascio della stessa, dal momento che ciascuno dei requisiti (tampone, guarigione, vaccinazione) determina un diverso periodo di validità del *green pass.* In tal modo, dunque, una scelta quale quella sulla vaccinazione – così fortemente legata alle intime convinzioni della persona – verrebbe privata delle necessarie garanzie di riservatezza, con effetti potenzialmente pregiudizievoli in ordine all'autodeterminazione individuale. Tale potenziale pregiudizio è, poi, aggravato dal contesto lavorativo in cui matura. La prevista ostensione (e consegna) del certificato verde a un soggetto, quale il datore di lavoro, al quale dovrebbe essere preclusa la conoscenza di condizioni soggettive peculiari dei lavoratori come la situazione clinica e convinzioni personali, pare infatti poco compatibile con le garanzie sancite sia dalla disciplina di protezione dati, sia dalla normativa giuslavoristica (artt. 88 del

RGPD; 113, d.lgs. n. 196/2003; 5 e 8, l. n. 300/1970 e 10, d.lgs. n. 276/2003).

Né, del resto, la prevista facoltà di conservazione del *green pass* può ritenersi legittima sulla base di un presunto consenso implicito del lavoratore che la consegni, ritenendo il diritto sotteso pienamente disponibile. Dal punto di vista della protezione dei dati personali (e, dunque, ai fini della legittimità del relativo trattamento), il consenso in ambito lavorativo non può, infatti, ritenersi un idoneo presupposto di liceità, in ragione dell'asimmetria che caratterizza il rapporto lavorativo stesso (cons. 43 RGPD).

Naturalmente, poi, la conservazione dei certificati imporrebbe l'adozione, da parte datoriale, di misure tecniche e organizzative adeguate al grado di rischio connesso al trattamento, con un non trascurabile incremento degli oneri (anche per la finanza pubblica, relativamente al settore pubblico).

Oblio e provvedimenti giudiziari favorevoli

L'articolo 1, comma 25, l. n. 134/2021 ha introdotto, quale ulteriore criterio direttivo per l'esercizio della delega in materia di riforma del processo penale, la previsione secondo cui il decreto di archiviazione e la sentenza di non luogo a procedere o di assoluzione costituiscano titolo per l'emissione di un provvedimento di deindicizzazione che, nel rispetto della normativa UE in materia di protezione dei dati personali, garantisca in modo effettivo il diritto all'oblio degli indagati o imputati.

La norma mira a garantire ad indagati o imputati, destinatari di provvedimenti favorevoli, una specifica tutela al diritto all'oblio, nella declinazione peculiare (ulteriore rispetto al diritto alla non ripubblicazione e al diritto alla rettifica e all'aggiornamento di notizie obsolete) del diritto al *delisting* o deindicizzazione (disassociazione del nominativo del singolo a specifici contenuti *online*).

Si introduce, dunque, un'ipotesi speciale di deindicizzazione di (dati personali contenuti in) provvedimenti giudiziali favorevoli, sancendo una presunzione di meritevolezza dell'istanza di *delisting,* in ragione della sussistenza di un decreto di archiviazione, di una sentenza di non luogo a procedere o di assoluzione emessi nei confronti dell'interessato.

La norma non definisce l'oggetto della deindicizzazione; non chiarisce cioè se esso riguardi i soli provvedimenti giurisdizionali citati in sé ovvero, più genericamente, i dati (giudiziari) relativi al coinvolgimento dell'interessato nel procedimento penale definito con i provvedimenti indicati.

La delega, al termine del periodo al quale si riferisce la presente relazione, non è stata ancora esercitata.

Proroga dello stato di emergenza

Il decreto-legge n. 221/2021, convertito, con modificazioni ha disposto, segnatamente, la proroga al 31 marzo 2022 dello stato di emergenza nazionale e delle misure per il contenimento dell'epidemia da Covid-19. Tra queste ultime è compresa anche la norma di cui all'art. 17-*bis,* d.l. n. 18/2020, che sin dai primi mesi dell'emergenza ha introdotto un peculiare regime di circolazione dei dati personali a fini di contrasto dell'emergenza.

La norma dispone in particolare che: a) i dati personali, comuni e particolari, possono essere trattati e avere una circolazione interna agli organi deputati al contrasto dell'emergenza, tra i quali rientrano oltre ai soggetti precedentemente indicati, anche "gli uffici del Ministero della salute e dell'Istituto superiore di sanità, le strutture pubbliche e private che operano nell'ambito del Ssn e i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi dell'art. 3, decreto-legge 23 febbraio 2020, n. 6"; b) i medesimi dati possono essere comunicati ad altri soggetti pubblici (si pensi in particolare agli enti territoriali o alle autorità di pubblica sicurezza) e privati (si pensi ai datori di lavoro), nonché diffusi (purché non si tratti dei dati particolari di cui agli artt. 9 e 10 del RGPD), qualora ciò risulti indispensabile al fine dello svolgimento delle attività connesse alla gestione della

emergenza in atto; c) al trattamento si applicano i principi di cui all'art. 5 del RGPD (liceità, correttezza, trasparenza, finalità, minimizzazione, etc.); d) il conferimento di incarichi di trattamento ai sensi dell'art. 2-*quaterdecies* del Codice in materia di protezione dei dati potrà avvenire con modalità semplificate, ed anche oralmente; e) nel quadro delle attività di cui sopra, le autorità sanitarie e gli altri soggetti autorizzati, qualora trattino dati raccolti presso l'interessato medesimo, possono omettere o rendere in forma semplificata l'informativa prescritta dall'art. 13 del RGPD.

Cybersicurezza

Il decreto-legge n. 82/2021, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, convertito con modificazioni, dalla legge n. 109/2021, ha introdotto innovazioni significative sul tema.

Particolare rilievo assume l'istituzione dell'Agenzia, di cui è espressamente prevista la collaborazione con il Garante (anche in relazione agli incidenti che comportino *data breach*), in particolare mediante specifici protocolli d'intesa, nonché la consultazione del secondo da parte della prima. Il decreto-legge precisa che i trattamenti per finalità di sicurezza nazionale, in applicazione del decreto-legge, sono svolti ai sensi dell'art. 58, commi 2 e 3, del Codice, mentre a tutti gli altri trattamenti (svolti dunque, pur dall'Agenzia, ma per fini diversi, ad es. amministrativi), si applica la disciplina generale.

***Governance* Pnrr e semplificazioni**

Il decreto-legge n. 77/2021 recante *governance* del Pnrr e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure, convertito, con modificazioni, dalla l. n. 108/2021, ha introdotto alcune disposizioni di peculiare interesse in termini di protezione dei dati personali.

Tra queste si segnalano, in particolare:

- l'art. 11-*bis,* che legittima l'Istat ad accedere ad archivi della p.a. "contenenti dati e informazioni utili ai fini della produzione delle basi di dati" e "alle informazioni individuali ivi contenute, con esclusione della banca dati detenuta dal Centro elaborazione dati di cui all'articolo 8 della legge 1° aprile 1981, n. 121, e della banca dati nazionale unica della documentazione antimafia, (…)", nel rispetto della disciplina di protezione dati e, nel caso di dati particolari, sulla base di provvedimenti direttoriali adottati con parere del Garante, con possibilità di comunicazione, in particolare in ambito Sistan, dei dati privi di riferimenti individuali alle unità statistiche;
- l'art.38, recante talune innovazioni in materia di notifica digitale degli atti della p.a. e domicilio digitale; introduzione del Sistema di gestione deleghe (Sgd), che consente a coloro che non possiedono una identità digitale di delegare ad un altro soggetto l'accesso per proprio conto a servizi *online;*
- l'art. 38-*bis,* recante misure per la digitalizzazione del procedimento elettorale preparatorio prevedendo in particolare che:
  a) l'atto di designazione dei rappresentanti della lista possa essere presentato anche mediante posta elettronica certificata;
  b) il certificato di iscrizione alle liste elettorali, necessario per la sottoscrizione a sostegno di liste di candidati per le elezioni politiche, europee ed amministrative, nonché di proposte di *referendum* e per iniziative legislative popolari possa essere richiesto in formato digitale tramite posta elettronica certificata;
  c) i rappresentanti legali dei partiti e dei movimenti politici e delle liste competitrici in elezioni amministrative in comuni con almeno 15.000 abitanti possano richiedere anche tramite posta elettronica certificata i certificati penali rilasciati dai casellari giudiziali per i propri candidati, ai fini dell'ottemperanza per i partiti dell'obbligo di pubblicare sul sito internet il *curri-*

culum vitae e il certificato del casellario giudiziale dei candidati;

d) si pubblichino tempestivamente sul sito internet istituzionale dell'ordine i nominativi degli avvocati iscritti all'albo disponibili ad eseguire le autenticazioni delle sottoscrizioni elettorali;

e) la sperimentazione del voto elettronico per gli elettori fuori sede prevista dalla legge di bilancio 2020 per le elezioni politiche ed europee e per i *referendum* è estesa anche alle elezioni regionali e amministrative;

- l'art. 38-*quater* recante una nuova disciplina per la sottoscrizione elettronica per i *referendum* e per le proposte di legge di iniziativa popolare, integrativa delle previsioni della legge di bilancio 2021 (art. 1, commi 341-343) che hanno disposto l'istituzione di una piattaforma per la raccolta delle firme digitali, la cui disciplina di dettaglio è demandata a un decreto non regolamentare da emanarsi previo parere del Garante;
- l'art. 39-*quater* sulla digitalizzazione delle comunicazioni funzionali all'esecuzione dei trattamenti sanitari obbligatori nei casi in cui essi possano incidere sulle condizioni per il possesso del porto d'armi;
- l'art. 39-*quinquies* recante istituzione dell'Anagrafe nazionale dell'istruzione (recante anche dati sul rendimento scolastico degli studenti, attraverso l'interoperabilità con il registro elettronico) e dell'Anagrafe nazionale dell'istruzione superiore, secondo modalità che saranno definite con provvedimenti attuativi sui quali si acquisirà il parere del Garante;
- l'art. 39-*sexies* che reca talune disposizioni per la realizzazione di un sistema informativo integrato per il supporto alle decisioni nel settore dell'istruzione scolastica, per la raccolta, la sistematizzazione e l'analisi multidimensionale dei relativi dati, per la previsione di lungo periodo della spesa per il personale scolastico, nonché per il supporto alla gestione giuridica ed economica del predetto personale prevedendo, tra l'altro, il ricorso a tecniche d'intelligenza artificiale.

Sorveglianza epidemiologica

Il decreto-legge 25 maggio 2021, n. 73, recante misure urgenti connesse all'emergenza da Covid-19, per le imprese, il lavoro, i giovani, la salute e i servizi territoriali (Sostegni *bis*) convertito, con modificazioni, dalla l. 23 luglio 2021, n. 106, ha introdotto alcune disposizioni d'interesse in termini di protezione dati.

Tra queste si segnala, in particolare, l'art. 34-*bis,* in materia di sorveglianza epidemiologica del Sars-CoV-2 e di monitoraggio delle risposte immunologiche al Covid-19 e ai vaccini.

La norma legittima l'acquisizione, da parte dell'Iss, dei dati sulle risposte immunologiche e disciplina le modalità di trasmissione dei dati relativi alla positività al test, al dipartimento di prevenzione dell'azienda sanitaria locale territorialmente competente e all'Iss. Gli enti territoriali, in particolare, trasmettono i dati relativi ai positivi all'Iss mediante la piattaforma per la sorveglianza integrata del Covid-19 istituita presso il medesimo Istituto ai sensi dell'ordinanza del Capo del Dipartimento della protezione civile 27 febbraio 2020, n. 640 (G.U. 28 febbraio 2020, n. 50).

Obbligo vaccinale

Tra le norme rilevanti, in termini di protezione dati, del decreto-legge 1° aprile 2021, n. 44, recante disposizioni sugli spostamenti di aprile, vaccinazioni, giustizia e concorsi pubblici, convertito, con modificazioni, dalla l. n. 76/2021 si richiama, in particolare, l'art. 4.

Tale disposizione ha introdotto l'obbligo vaccinale da Sars-CoV-2 – quale requisito essenziale per lo svolgimento della professione – per gli esercenti le professioni sanitarie e gli operatori di interesse sanitario che svolgono la loro attività nelle strutture sanitarie, sociosanitarie e socio-assistenziali, pubbliche e private, nelle farmacie, parafarmacie e negli studi professionali.

2

L'accertamento dell'osservanza dell'obbligo è demandato a un complesso flusso informativo che coinvolge ciascun ordine professionale territoriale competente, le regioni e le province autonome e, quindi, le aziende sanitarie locali. A queste ultime compete l'adozione dell'atto di accertamento della violazione, con la conseguente sospensione del diritto di svolgere prestazioni o mansioni che implichino contatti interpersonali o comportino, in qualsiasi altra forma, il rischio di diffusione del contagio da Sars-CoV-2.

A seguito della segnalazione del Garante con cui sono state evidenziate talune criticità della disciplina originaria, in sede di conversione si sono superate le maggiori incongruenze e colmate le lacune della normativa proposta, perfezionando anche la complessiva architettura del trattamento.

Protocollo di emendamento alla Convenzione sul trattamento automatizzato di dati

Tra le norme approvate nell'anno, rilevanti in termini di protezione dati, va annoverata la legge n. 60/2021, recante ratifica ed esecuzione del Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, fatto a Strasburgo il 10 ottobre 2018.

Il Protocollo d'emendamento della Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (strutturato in 40 articoli) è stato adottato il 18 maggio 2018 ed aperto alla firma il 10 ottobre 2018. L'adozione, da parte degli Stati firmatari, delle misure necessarie a consentirne l'entrata in vigore è stata prevista come ammissibile nei tre anni successivi all'apertura alla firma del Protocollo. Sulla base della decisione con cui è stato adottato il Protocollo, gli Stati membri sono stati altresì incaricati di effettuare una revisione semestrale dei progressi compiuti in materia di trattamento automatizzato di dati personali, conformemente al contenuto normativo del Protocollo stesso. L'Italia ha sottoscritto il Protocollo il 5 marzo 2019.

Il disegno di legge di ratifica ed esecuzione del Protocollo è stato assegnato alla 3ª Commissione del Senato il 23 luglio 2019 e definitivamente approvato il 14 aprile 2021.

2.2. *I decreti legislativi*

Tra i numerosi decreti legislativi adottati nel 2021 e rilevanti, in varia misura, in termini di protezione dei dati personali, si segnalano, in particolare, i seguenti:

Uso d'informazioni finanziarie a fini di contrasto dei reati

il decreto legislativo n. 186/2021, recante attuazione della direttiva (UE) 2019/1153, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati e che abroga la decisione 2000/642/GAI (sul cui schema il Garante ha reso parere) recepisce, nell'ordinamento interno, la direttiva in questione, volta ad agevolare l'accesso alle informazioni ed analisi finanziarie e sui conti bancari e il loro utilizzo a fini di prevenzione, accertamento o perseguimento di reati gravi specificamente individuati, nonché a favorire la cooperazione tra le unità di informazione finanziaria, consentendo loro l'accesso alle informazioni "in materia di contrasto" per lo svolgimento delle proprie attività. Per tali esigenze (individuate dallo schema di decreto, correttamente, in quelle del procedimento penale e per l'applicazione delle misure di prevenzione), le autorità designate come competenti dagli Stati membri devono essere abilitate ad accedere ai rispettivi "registri centralizzati dei conti bancari", già istituiti in virtù della direttiva (UE) 2015/849, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. Tra gli aspetti più rilevanti del provvedimento si richiamano, in particolare, quelli inerenti: la designazione delle autorità nazionali competenti, abilitate ad accedere al

registro nazionale centralizzato dei conti bancari (Ufficio nazionale per il recupero dei beni istituito presso il Ministero dell'interno, Autorità giudiziaria e ufficiali di polizia giudiziaria delegati dal pubblico ministero, servizi centrali e interprovinciali per il contrasto della criminalità organizzata, Ministro dell'interno, Capo della polizia-direttore generale della pubblica sicurezza, questori, direttore della Direzione investigativa antimafia); la designazione del Nucleo speciale di polizia valutaria della Guardia di finanza e della Direzione investigativa antimafia quali autorità nazionali competenti a richiedere e a ricevere informazioni finanziarie o analisi finanziarie dalla Uif (Unità di informazione finanziaria istituita presso Banca d'Italia), qualora necessario per lo svolgimento di un procedimento penale o nell'ambito di un procedimento per l'applicazione delle misure di prevenzione patrimoniali. Per quanto riguarda il trattamento dei dati personali, si subordinano i vari scambi informativi alle condizioni previste dalla disciplina di protezione dati: prevalentemente il d.lgs. n. 51/2018 in quanto attinente ai trattamenti svolti nel contesto di attività di contrasto, ma anche il RGPD e il Codice rispetto all'utilizzo a fini ulteriori (generalmente di polizia amministrativa) dei dati raccolti, nei casi ammessi dalla direttiva.

Il testo definitivamente approvato ha tenuto conto delle indicazioni rese dall'Autorità (parere 26 agosto 2021, n. 307, doc. web n. 9717779);

Open data

il decreto legislativo n. 200/2021, recante attuazione della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (sul cui schema il Garante ha reso parere) recepisce, nell'ordinamento interno, la direttiva in questione, volta ad agevolare l'utilizzo di dati aperti e il riutilizzo, a fini commerciali e non commerciali, delle informazioni detenute da p.a., organismi di diritto pubblico e, a determinate condizioni, anche imprese pubbliche, promuovendo la concorrenza e la trasparenza nel mercato dell'informazione.

Il decreto legislativo – secondo il principio di gratuità del riutilizzo dei dati pubblici – prevede, in particolare: l'incremento dell'offerta di dati pubblici a fini di riutilizzo, estesa anche ai dati della ricerca finanziata con fondi pubblici; la disponibilità di dati dinamici in tempo reale dopo la raccolta e di set di dati con un impatto economico particolarmente elevato, tramite interfacce di programmazione adeguate; la determinazione di tariffe, se necessarie, secondo specifici criteri di calcolo; misure di contenimento di nuove forme di accordi di esclusiva o disposizioni limitative della possibilità di riutilizzo dei dati pubblici.

Il testo definitivamente approvato ha tenuto conto di gran parte delle indicazioni rese dall'Autorità (parere 26 agosto 2021, n. 308, doc. web n. 9717493);

Presunzione d'innocenza

il decreto legislativo n. 188/2021, recante disposizioni per il compiuto adeguamento della normativa nazionale alle disposizioni della direttiva (UE) 2016/343 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali introduce talune disposizioni, anche di carattere processuale, volte a garantire l'effettività del diritto alla presunzione di innocenza e, con esso, anche la tutela della dignità personale.

Il decreto legislativo introduce, in primo luogo, un articolato sistema di tutele del diritto dell'indagato o dell'imputato a non essere indicato "pubblicamente come colpevole" finché non ne sia definitivamente accertata la responsabilità penale, nonché nuove modalità di gestione del rapporto tra giustizia e informazione.

Parallelamente a queste garanzie extraprocessuali della presunzione d'innocenza, si introducono poi ulteriori garanzie specificamente intraprocessuali, rilevanti (anche) quali parametri di redazione degli atti e regola di trattamento dell'indagato e dell'imputato, nella fase anteriore all'accertamento definitivo di responsabilità.

Ne deriva, complessivamente un rafforzamento della tutela della dignità dell'in-

dagato e dell'imputato, anche sotto il profilo della protezione dati e, segnatamente, del principio di esattezza;

Fornitura di contenuti digitali

il decreto legislativo n. 173/2021, recante attuazione della direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, ha introdotto alcune disposizioni d'interesse anche sotto il profilo della protezione dati.

In attuazione della direttiva, il decreto introduce nel codice del consumo un Capo specifico, volto a disciplinare alcuni aspetti dei contratti di fornitura di contenuto digitale o di servizi digitali conclusi tra consumatore e professionista, relativamente, dunque, ai contratti in cui il professionista fornisca un contenuto o servizio digitale verso il corrispettivo di un prezzo corrisposto dal consumatore, nonché a quelli in cui il consumatore, al posto del prezzo, fornisca al professionista dati personali. Si chiarisce in cosa consista l'esatto adempimento dell'obbligo di fornitura da parte del professionista e si individuano i requisiti soggettivi e oggettivi del contenuto o del servizio digitale ai fini della sua conformità al contratto; si definiscono gli obblighi del professionista e la condotta del consumatore, con particolare riferimento agli aggiornamenti, anche di sicurezza, necessari al fine di mantenere la conformità del contenuto o del servizio digitale; si disciplinano le conseguenze dell'eventuale difetto di conformità derivante da un'errata integrazione del contenuto o del servizio digitale nell'ambiente digitale del consumatore; si individuano i diritti a tutela dei terzi, in particolare sotto il profilo della proprietà intellettuale; si disciplinano la responsabilità del professionista e le tutele del consumatore in caso di omessa fornitura da parte del professionista del contenuto o servizio digitale o di difetto di conformità del bene; si sancisce la nullità di ogni patto volto ad escludere o limitare a danno del consumatore i diritti introdotti;

Servizi di *media* audiovisivi

il decreto legislativo n. 208/2021 ha disposto l'attuazione della direttiva (UE) 2018/1808 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di *media* audiovisivi, in considerazione dell'evoluzione delle realtà del mercato. La direttiva (UE) 2018/1808, oggetto del recepimento, ha in particolare novellato la direttiva 2010/13/UE, sui servizi di *media* audiovisivi, al fine di adeguarla alla recente evoluzione del mercato e al processo di trasformazione delle modalità di fruizione dei servizi di *media* audiovisivi, della radiofonia e dei servizi di piattaforma per la condivisione di video.

Il testo – su cui l'Autorità è stata consultata – sostituisce il d.lgs. 31 luglio 2005, n. 177, valorizzando, nell'esercizio della delega legislativa, alcuni principi di particolare rilievo sia per gli utenti che per il mercato audiovisivo. Tra questi ultimi, particolare rilievo assumono la garanzia della libertà e del pluralismo dei mezzi di comunicazione radiotelevisiva, nonché la tutela della dignità umana e dei minori riguardo all'impatto che possono su di loro avere determinati contenuti audiovisivi e, più in generale, il contrasto delle discriminazioni.

Il testo definitivamente approvato ha tenuto conto delle indicazioni fornite dall'Autorità, con particolare riguardo alle disposizioni suscettibili di incidere sulla disciplina di protezione dati (nota 20 luglio 2021);

Comunicazioni elettroniche

il decreto legislativo n. 207/2021 ha attuato la direttiva (UE) 2018/1972 che istituisce il codice europeo delle comunicazioni elettroniche (rifusione), novellando gran parte del d.lgs. n. 259/2003.

Nell'esercizio della delega legislativa, il decreto sancisce anzitutto, quali obiettivi della disciplina delle reti e servizi di comunicazione elettronica, da assicurare nel rispetto del principio della libera circolazione delle persone e delle cose, la salvaguardia

della libertà di comunicazione, della segretezza delle comunicazioni stesse – anche attraverso il mantenimento dell'integrità e della sicurezza delle reti di comunicazione elettronica e l'adozione di misure preventive delle interferenze – e della libertà di iniziativa economica nonché del suo esercizio in regime di concorrenza, garantendo un accesso al mercato delle reti e servizi di comunicazione elettronica secondo criteri di obiettività, trasparenza, non discriminazione e proporzionalità. Il decreto rimodula, segnatamente, l'assetto istituzionale e la *governance* in materia, le garanzie per i consumatori, il regime sanzionatorio.

Il testo definitivamente approvato ha tenuto conto delle indicazioni fornite dall'Autorità, con particolare riguardo alle disposizioni suscettibili di incidere sulla disciplina di protezione dati (nota 6 luglio 2021).

2.3. *Norme di rango secondario*

Tra i regolamenti di particolare rilievo per la protezione dei dati e sui quali, peraltro, è stato acquisito il parere del Garante si segnalano, tra gli altri, i seguenti:

a) decreto 29 ottobre 2021 del Ministro dell'interno, recante le modalità tecniche dei collegamenti attraverso i quali sono effettuate le comunicazioni dei dati identificativi riportati nei documenti di identità esibiti dai soggetti che richiedono il noleggio di autoveicoli e relative modalità di conservazione (parere 14 ottobre 2021, n. 366, doc. web n. 9717525) (cfr. par. 3.1.3);
b) 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* del Codice (parere 24 giugno 2021, n. 247, doc. web n. 9682603).

3 I rapporti con il Parlamento e le altre Istituzioni

3.1. *L'attività consultiva del Garante*

La previsione, introdotta dal nuovo quadro giuridico europeo, del parere obbligatorio dell'Autorità sugli atti normativi anche di rango primario, rilevanti in termini 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. n. 96, del RGPD; 28, par. 2, direttiva 2016/680; 24, comma 2, d.lgs. n. 51/2018).

E questo, anche per effetto della più rilevante attività legislativa connessa alla situazione pandemica e alle necessità di riforme funzionali all'attuazione del Pnrr.

Il dialogo tra Parlamento, Governo e Garante, consolidatosi anche per effetto della più frequente consultazione di quest'ultimo, ha così contribuito, in linea generale, all'individuazione del corretto bilanciamento sotteso alle varie e 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

Il coinvolgimento del Garante nell'ambito del procedimento legislativo o, comunque, dell'esercizio delle funzioni conoscitiva, di indirizzo e controllo delle Camere è risultato, nel 2021, alquanto significativo.

Numerosi sono stati i casi di consultazione del Garante su atti normativi primari, spesso anche in sede di conversione di decreti-legge, soprattutto in relazione alle misure adottate a fini di contrasto della pandemia. Per tali forme di consultazione dell'Autorità è sempre più frequente il ricorso 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. Le audizioni sono state talora richieste anche nell'ambito dell'esame, in fase ascendente, di atti normativi dell'Unione europea.

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

a) audizione dinanzi alla 1ª Commissione del Senato sui profili costituzionali dell'eventuale introduzione di un "passaporto vaccinale" per i cittadini cui è stato somministrato il vaccino anti Sars-CoV2 - 8 aprile 2021 (doc. web n. 9574242);
b) audizione dinanzi alle Commissioni riunite I, II e XII della Camera dei deputati, sulle tematiche relative alla certificazione verde Covid-19 - 6 maggio 2021 (doc. web n. 9583365);
c) audizione dinanzi alla IV Commissione della Camera dei deputati sulle "Modifiche agli articoli 1058 e 1462 del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, in materia di documentazione dei giudizi di idoneità all'avanzamento e di attribuzione del punteggio di merito nonché di conferimento di encomi ed elogi" - 28 maggio 2021 (doc. web n. 9591317);
d) audizione dinanzi alla IX Commissione della Camera dei deputati sulla

proposta di regolamento relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) (COM (2020) 825 *final*) e proposta di regolamento relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali) (COM (2020) 842 *final* - 23 giugno 2021 (doc. web n. 9673114);

e) audizione dinanzi al Copasir sul disegno di legge di conversione del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale - 1° luglio 2021;
f) contributo alla 1ª Commissione del Senato, nell'ambito dell'esame del disegno di legge di conversione del decreto-legge 21 settembre 2021, n. 127, recante misure urgenti per assicurare lo svolgimento in sicurezza del lavoro pubblico e privato mediante l'estensione dell'ambito applicativo della certificazione verde Covid-19 e il rafforzamento del sistema di *screening* - 5 ottobre 2021 (doc. web n. 9707961);
g) audizione dinanzi alla 1ª Commissione del Senato sul disegno di legge di conversione del decreto legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali - 2 novembre 2021 (doc. web n. 9755883);
h) audizione, dinanzi alla 1ª Commissione del Senato sul disegno di legge di conversione del decreto-legge 26 novembre 2021, n. 172 recante misure urgenti per il contenimento dell'epidemia da Covid-19 e per lo svolgimento in sicurezza delle attività economiche e sociali - 7 dicembre 2021 (doc. web n. 9725434);
i) audizione dinanzi alla XI Commissione della Camera nell'ambito dell'esame delle proposte di legge C. 1779 Paolo Russo e C. 1782 Molinari, recanti disposizioni in materia di controlli sul personale addetto ai servizi di trasporto - 16 dicembre 2021 (doc. web n. 9736014).

Non sono, tuttavia, mancate richieste di contributi anche nell'ambito dell'esercizio delle funzioni conoscitiva, di indirizzo e controllo delle Camere, che dimostrano 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 1ª Commissione del Senato nell'ambito dell'esame dei disegni di legge nn. AS 1900 e 1549, concernenti l'istituzione di una commissione d'inchiesta sulla diffusione di informazioni false - 12 gennaio 2021 (doc. web n. 9518110);
b) audizione dinanzi alle Commissioni riunite 7ª e 12ª del Senato sull'affare n. 621 in materia di impatto della didattica digitale integrata (DDI) sui processi di apprendimento e sul benessere psicofisico degli studenti - 27 aprile 2021 (doc. web n. 9581498);
c) audizione dinanzi alla Commissione parlamentare di vigilanza sull'Anagrafe tributaria, nell'ambito dell'indagine conoscitiva riguardante la digitalizzazione e interoperabilità delle banche dati fiscali - 7 luglio 2021 (doc. web n. 9678216);
d) audizione dinanzi alla Commissione straordinaria del Senato per il contrasto dei fenomeni di intolleranza, razzismo, antisemitismo e istigazione all'odio e alla violenza, nell'ambito dell'indagine conoscitiva sulla natura, cause e sviluppi recenti del fenomeno dei discorsi d'odio - 13 luglio 2021 (doc. web n. 9680938);
e) contributo alla Commissione parlamentare per l'infanzia e l'adolescenza nell'ambito dell'indagine conoscitiva sulla diffusione delle dipendenze patologiche tra i giovani – 19 agosto 2021 (doc. web n. 9756411).

3

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

Rilevante è stato anche il coinvolgimento del Garante, da parte del Governo, rispetto alla sua iniziativa legislativa ovvero agli atti con forza di legge di sua competenza.

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

a) parere 13 gennaio 2021, n. 1 (doc. web n. 9563463), su uno schema di norma recante la disciplina dei sistemi informativi funzionali all'implementazione del piano strategico dei vaccini per la prevenzione delle infezioni da Sars-CoV-2 (art. 3, d.l. 14 gennaio 2021, n. 2, convertito con modificazioni dalla l. 12 marzo 2021, n. 29). Tale disposizione prevedeva l'istituzione di una piattaforma informativa nazionale idonea ad agevolare, sulla base dei fabbisogni rilevati, le attività di distribuzione sul territorio nazionale delle dosi vaccinali, dei dispositivi e degli altri materiali di supporto alla somministrazione, nonché il relativo tracciamento. La norma affidava le operazioni di predisposizione e gestione della piattaforma nazionale al Commissario straordinario per l'attuazione e il coordinamento delle misure occorrenti per il contenimento e il contrasto dell'emergenza epidemiologica Covid-19. La norma poi approvata ha recepito le indicazioni rese nel corso di alcune interlocuzioni con rappresentanti del Dicastero della salute e della struttura commissariale, per conformarne il contenuto alle garanzie previste dalla normativa europea e nazionale in materia di di protezione dati;
b) parere 26 agosto 2021, n. 307 (doc. web n. 9717779), su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2019/1153, recante disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati e che abroga la decisione 2000/642/GAI (cfr. par. 2.2);
c) parere 26 agosto 2021, n. 308 (doc. web n. 9717493), su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico;
d) parere 10 settembre 2021, n. 310 (doc. web n. 970485), su uno schema di decreto-legge recante la riforma della disciplina dell'acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale. Il provvedimento, in linea anche con la segnalazione del Garante del 22 luglio 2021 (v. *infra*), ha adeguato la disciplina interna alle esigenze, sottolineate dalla CGUE, di attribuzione della competenza autorizzatoria sull'acquisibilità dei tabulati telefonici e telematici a un'autorità non soltanto indipendente, ma anche terza rispetto all'autorità pubblica richiedente. La riforma inoltre, coerentemente con la giurisprudenza europea, ha limitato l'accessibilità ai dati di traffico ai soli procedimenti per gravi reati. Nel parere reso, il Garante ha ritenuto complessivamente condivisibile la normativa proposta, rilevando anche che le differenze rispetto alla disciplina delle intercettazioni, pur mutuata nelle coordinate essenziali, fossero giustificate e ragionevoli in considerazione della minore invasività del mezzo rispetto a quello intercettativo. Si è tuttavia suggerito di valutare l'opportunità di ripensare il termine di conservazione di settantadue mesi previsto dalla disciplina vigente per la conservazione dei dati di traffico telefonico e telematico, riconducendolo entro margini maggiormente compatibili con il canone di proporzionalità, tenendo conto dei precedenti sui quali la CGUE ha avuto modo di pronunciarsi. Per altro verso, il parere ha rilevato come la norma proposta non chiarisse il regime di esperibilità dei rimedi sanciti dagli artt. da 12 a 22 del RGPD in favore dell'interessato, in

funzione strumentale alla garanzia dell'effettività del diritto alla protezione dei dati personali. Si è quindi suggerito di introdurre una clausola di salvaguardia in favore della disciplina di cui all'art. 2-*undecies,* comma 3, periodi da terzo a quinto, del Codice, nei casi di esercizio dei diritti. Questo rilievo è stato accolto dal Governo nel testo poi rifluito nel d.l. n. 132/2021.

3.1.3. I pareri sugli atti regolamentari e amministrativi generali

Nel quadro dell'attività consultiva concernente norme regolamentari ed atti amministrativi generali suscettibili di incidere sulla protezione dei dati personali, il Garante ha reso parere, tra l'altro, sui seguenti schemi di provvedimento:

a) schema di regolamento del Mef, di concerto con il Mise in materia di comunicazione, accesso e consultazione dei dati e delle informazioni relativi alla titolarità effettiva di imprese dotate di personalità giuridica, di persone giuridiche private, di *trust* produttivi di effetti giuridici rilevanti ai fini fiscali e di istituti giuridici affini al *trust* (parere 14 gennaio 2021, n. 2, doc. web n. 954101);
b) schema di regolamento del Ministero della giustizia concernente l'elenco pubblico dei soggetti legittimati a proporre una "azione di classe" (parere 14 gennaio 2021, n. 19, doc. web n. 9543119);
c) schema di regolamento del Mise recante criteri, modalità e requisiti per l'iscrizione, la permanenza e l'esclusione dall'elenco dei soggetti abilitati alla vendita di energia elettrica, adottato ai sensi dell'art. 1, commi da 80 e 82, legge 4 agosto 2017, n. 124 (parere 11 febbraio 2021, n. 41, doc. web n. 9556647);
d) schema di decreto del Presidente della Repubblica recante la disciplina del registro unico telematico e disposizioni di semplificazione in materia di cessazione dalla circolazione dei veicoli fuori uso (parere 13 maggio 2021, n. 188, doc. web n. 9674176);
e) schema di regolamento del Ministero della giustizia recante la disciplina del trattamento di dati personali relativi a condanne penali e reati (cd. dati giudiziari), ai sensi dell'art. 2-*octies* del Codice (parere 24 giugno 2021, n. 247, doc. web n. 9682603);
f) schema di regolamento del Ministero della giustizia recante l'individuazione delle modalità di iscrizione, di sospensione e cancellazione dall'albo dei soggetti destinati a svolgere, su incarico del tribunale, le funzioni di curatore, commissario giudiziale o liquidatore, istituito dall'art. 356, d.lgs. 12 gennaio 2019, n. 14 (parere 24 giugno 2021, n. 248, doc. web n. 9681973);
g) schema di regolamento del Ministero del turismo in materia di comunicazione alle autorità di pubblica sicurezza dell'arrivo delle persone alloggiate in strutture ricettive (parere 8 luglio 2021, n. 300, doc. web n. 9690786);
h) schema di regolamento del Ministero della cultura concernente le regole sull'attribuzione e l'utilizzo della Carta elettronica per i diciottenni (cd. *bonus* cultura o anche 18*app*) (parere 29 settembre 2021, n. 349, doc. web n. 9721580);
i) schema di regolamento del Ministro della salute recante l'istituzione del Registro nazionale degli impianti protesici mammari (parere 28 ottobre 2021, n. 381, doc. web n. 9721558);
j) schema di decreto del Presidente della Repubblica recante la disciplina relativa al funzionamento dello Sportello unico doganale e dei controlli (S.U.Do.Co) (parere 2 dicembre 2021, n. 427, doc. web n. 9733130).

Il Garante si è inoltre espresso sui seguenti decreti, non aventi natura regolamentare:

- schema di decreto interministeriale Mise di modifica dell'allegato tecnico al d.P.R. n. 160/2010, recante le modalità di comunicazione e trasferimento dei dati tra lo Sportello unico per le attività produttive (Suap) e i soggetti

coinvolti nei procedimenti amministrativi (parere 16 settembre 2021, n. 313, doc. web n. 9716338);
- schema di decreto del Ministro dell'interno, concernente le modalità tecniche dei collegamenti attraverso cui sono effettuate le comunicazioni dei dati identificativi riportati nei documenti di identità esibiti dai soggetti che richiedono il noleggio di autoveicoli e le relative modalità di conservazione (parere 14 ottobre 2021, n. 366, doc. web n. 9717525).

3.1.4. La consultazione del Garante sugli atti normativi degli enti territoriali

Al Garante è stato richiesto di esprimere il proprio parere su alcuni progetti di legge o schemi di regolamento degli enti territoriali.

Si segnalano, in tal senso, i seguenti:

1) parere su proposta di modifica dell'articolo 19.1 della legge della Provincia autonoma di Trento n. 23/1992, in materia di decisioni automatizzate nei confronti dei minori (parere 16 settembre 2021, n. 314, doc. web n. 9713993);
2) parere su proposta di modifica del regolamento della Provincia autonoma di Trento in materia di "medicina di iniziativa", a seguito della revisione dell'art. 4 della legge provinciale n. 16/2010 (l.p. 4 agosto 2021 n. 18) (parere 16 dicembre 2021, n. 431, doc web n. 9738538);
3) parere su proposta di legge della Provincia autonoma di Trento in tema di trattamento di dati anche appartenenti a categorie particolari nell'ambito dei procedimenti amministrativi connessi allo svolgimento delle funzioni catastali delegate dallo Stato (parere 16 dicembre 2021, n. 432, doc. web n. 9736978).

Per quanto concerne il rapporto tra normazione statale e regionale, merita in particolare richiamare la nota del Garante 21 giugno 2021, indirizzata alle Regioni e alla Conferenza delle Regioni e delle Province Autonome con riferimento all'emissione, al rilascio e alla verifica delle certificazioni verdi (doc. web n. 9681670).

La nota – successiva ad alcune iniziative regionali in materia ritenute incompatibili con la disciplina statale – ha sottolineato la necessità di soprassedere dall'adottare disposizioni che prevedessero:
- ulteriori fattispecie di esibizione necessaria di certificati verdi quale requisito per l'accesso a luoghi e locali o l'instaurazione di rapporti giuridici (in senso analogo a questo rilievo vedasi la previsione, aggiunta in sede di conversione del d.l. n. 105/2021 al comma 10-*bis* dell'art. 9, d.l. n. 52/2021, secondo cui "Ogni diverso o nuovo utilizzo delle certificazioni verdi Covid-19 è disposto esclusivamente con legge dello Stato");
- modalità di emissione, gestione e controllo delle certificazioni difformi da quelle sancite a livello statale.

3.2. *Le segnalazioni al Parlamento e al Governo*

Nel 2021 le segnalazioni rivolte dal Garante al Parlamento e al Governo hanno riguardato le seguenti tematiche:

a) riforma della disciplina della conservazione dei dati di traffico telefonico e telematico a fini di giustizia (22 luglio 2021, doc, web n. 9685978);
b) necessità di bilanciamento tra il diritto alla protezione dei dati personali, il diritto di autodeterminazione sulle scelte vaccinali, le esigenze di prevenzione di contagi e il diritto all'istruzione in relazione al d.l. 6 agosto 2021, n. 111 (11 agosto 2021);
c) attuazione delle disposizioni relative alle certificazioni verdi nel contesto lavo-

rativo e, in particolare, all'esibizione del *green pass* quale condizione necessaria per accedere alle mense aziendali (18 agosto 2021);

d) disegno di legge di conversione del d.l. n. 127/2021 (AS 2394), in relazione alla possibilità di consegna, da parte dei lavoratori di copia della certificazione verde, al datore di lavoro (11 novembre 2021, doc. web n. 9717878);
e) disciplina dell'utilizzo delle fatture elettroniche, con particolare riferimento all'esigenza di sottrazione all'accesso ex l. n. 241/1990 ai file a tal fine conservati (23 dicembre 2021).

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

Rilevanti, per quantità e qualità, sono stati i contributi richiesti al Garante dal Governo, ai fini della risposta da fornire ad atti di sindacato ispettivo rilevanti in termini di protezione dei dati personali.

Si segnalano, in particolare le interrogazioni relative all'utilizzo dei *social network* da parte dei minorenni e, in particolar modo quelle riguardanti TikTok e il fenomeno delle sfide *online* e del cd. *black-out challenge,* alla base peraltro di alcuni suicidi emulativi tra minori.

L'Autorità in tale contesto, ha fornito il 22 febbraio 2021 il proprio contributo per l'interpellanza urgente n. 2-01092, sottolineando i rischi per la protezione dei dati e per i diritti fondamentali delle persone sottesi all'utilizzo di TikTok, in assenza di misure efficaci di verifica dell'età dell'utente.

Il Garante ha inoltre ricordato di aver avviato una serie di attività istruttorie nei confronti della piattaforma, tradottesi poi nella contestazione di alcune violazioni, con particolare riguardo all'inefficacia delle misure per l'*age verification.* Nel medesimo riscontro il Garante ha, peraltro, fatto riferimento al provvedimento adottato dall'Autorità il 22 gennaio 2021 (n. 20, doc. web n. 9524194) – in seguito al decesso di una bambina vittima di tali sfide –, con il quale, attraverso una procedura d'urgenza, si è vietato alla piattaforma l'ulteriore trattamento dei dati degli utenti "che si trovano sul territorio italiano, per i quali non vi sia assoluta certezza dell'età e, conseguentemente, del rispetto delle disposizioni collegate al requisito anagrafico, con effetto immediato dalla data di ricezione del provvedimento". Con note al Ministero dell'interno del 15 marzo, 6 maggio e 15 dicembre 2021 il Garante ha poi fornito ulteriori contributi per la risposta alle interrogazioni n. 2-01120 e 4-08359, ribadendo l'importanza ascritta dall'Autorità al tema e confermando di procedere al costante monitoraggio del trattamento dei dati personali effettuato mediante la piattaforma TikTok, soprattutto riguardo all'adozione di idonee misure di verifica dell'età dell'utente.

Sono pervenute, inoltre, richieste di elementi ai fini della redazione della risposta del Governo all'interrogazione a risposta scritta n. 4-09051, avente ad oggetto l'attacco avvenuto ai danni del sistema informatico del Comune di Brescia.

Con nota 25 ottobre 2021 il Garante ha ritenuto condivisibile, in ragione della tempestività con la quale il Comune di Brescia aveva reagito all'attacco informatico e delle analisi tecniche svolte e comunicate all'Autorità, la valutazione del rischio effettuata dal Comune, non ravvisando violazioni in materia.

Con nota 22 settembre 2021, l'Autorità ha poi fornito elementi riguardo all'interpellanza urgente n. 2-01330, relativa all'utilizzo dei sistemi di videosorveglianza con riconoscimento facciale in ambito pubblico, rilevando come nei casi sottoposti al suo esame avesse riscontrato l'insussistenza di una previsione normativa idonea, ai sensi dell'art. 7, d.lgs. n. 51/2018, a legittimare tale trattamento dei dati biometrici da parte dei comuni.

3

Con nota 9 dicembre 2021, infine, l'Autorità ha fornito il proprio contributo ai fini della redazione, da parte del Governo, della risposta scritta all'interrogazione n. 4-10786, in materia di accesso illecito ai dati contenuti nei *green pass* tramite il *software* di condivisione *peer-to-peer* eMule.

In particolare, l'Autorità ha rappresentato di aver avviato – a seguito di segnalazioni e reclami in ordine alla notizia, divulgata anche dalla stampa, della avvenuta diffusione *online* di numerose certificazioni verdi Covid-19, tramite reti *peer-to-peer* – le conseguenti attività istruttorie, giungendo poi a verificare la presenza in rete di oltre mille certificazioni verdi emesse a seguito di avvenuta guarigione, vaccinazione e esito negativo di tampone molecolare o antigenico.

L'Autorità ha inoltre segnalato di aver riscontrato che le certificazioni diffuse sarebbero state acquisite attraverso la piattaforma nazionale DGC e non ottenute attraverso gli altri canali ammessi (farmacisti, medici di medicina generale, pediatri di libera scelta, *app* IO, *app* Immuni e Fse) e quindi sarebbero state (verosimilmente) acquisite da terzi, a seguito della condivisione delle stesse, da parte degli interessati, su reti *peer-to-peer.* Per tali ragioni il Garante – pur riservando alla vicenda la massima attenzione ed evidenziando la necessità di rafforzare le misure tecniche relative al tracciamento delle operazioni di accesso alle certificazioni, al fine di ricostruire con maggiore precisione e tempestività condotte analoghe suscettibili di ripetersi in futuro – ha ritenuto che la diffusione delle certificazioni non potesse imputarsi a carenze nelle misure tecniche e organizzative adottate dal Ministero della salute, con riferimento al trattamento dei dati effettuato attraverso la suddetta piattaforma o a un comportamento fraudolento ascrivibile ai richiamati soggetti intermediari, ai quali è possibile rivolgersi per l'acquisizione delle certificazioni.

25 1997-2022

GPDP

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

L'attività svolta dal Garante

Relazione annuale 2021

PAGINA BIANCA

II - L'attività svolta dal Garante

4 Il Garante e le amministrazioni pubbliche

4.1. *L'attività fiscale e tributaria*

4.1.1. La dichiarazione dei redditi precompilata

Come negli anni precedenti, in più occasioni il Garante si è pronunciato in relazione alla cd. dichiarazione dei redditi precompilata, sia su schemi di decreto del Mef, sia con riguardo a schemi di provvedimento dell'Agenzia delle entrate, adottati ai sensi dell'art. 3, commi 4 e 5, d.lgs. 21 novembre 2014, n. 175.

Raccolta di nuovi dati

Il Garante si è espresso favorevolmente sullo schema di decreto del Mef concernente la trasmissione telematica all'Agenzia delle entrate dei dati riguardanti le erogazioni liberali agli enti del terzo settore, ai fini dell'elaborazione della dichiarazione dei redditi precompilata (provv. 14 gennaio 2021, n. 3, doc. web n. 7772714). Conseguentemente ha espresso il parere sullo schema di provvedimento del Direttore dell'Agenzia delle entrate che ha disciplinato la comunicazione all'Anagrafe tributaria di tali dati (provv. 11 febbraio 2021, n. 42, doc. web n. 9556670), esaminando in particolare le modalità per l'esercizio del diritto di opposizione da parte dei contribuenti all'inserimento delle erogazioni liberali nella dichiarazione. In base al menzionato provvedimento i dati relativi ai soggetti che hanno esercitato l'opposizione devono essere tempestivamente e integralmente cancellati dall'archivio; i dati relativi ai soggetti che non hanno esercitato l'opposizione possono essere utilizzati unicamente ai fini dell'elaborazione della dichiarazione dei redditi precompilata e ai fini dell'attività di controllo delle dichiarazioni di cui all´art. 7, d.P.R. n. 605/73; i dati relativi ai soggetti che non hanno effettuato l'accesso alla dichiarazione precompilata, direttamente o tramite gli altri soggetti autorizzati, devono essere tempestivamente e integralmente cancellati entro la data in cui verrà messa a disposizione la dichiarazione precompilata dell'anno successivo.

L'Autorità ha espresso altresì parere favorevole su alcuni schemi di provvedimento del Direttore dell'Agenzia delle entrate concernenti la comunicazione all'Anagrafe tributaria dei dati relativi agli interventi di recupero del patrimonio edilizio e di riqualificazione energetica effettuati su parti comuni di edifici residenziali nonché di quelli relativi ai contratti assicurativi e ai rispettivi premi (provv. 27 gennaio 2021, n. 43, doc. web n. 9556687); è stato altresì valutato favorevolmente lo schema di decreto del Ministro dell'economia e delle finanze, sull'estensione della rilevazione delle spese sanitarie (da trasmettere al Sistema tessera sanitaria a fini di elaborazione della dichiarazione dei redditi precompilata) alle prestazioni erogate dagli iscritti agli elenchi speciali ad esaurimento istituiti ai sensi del decreto del Ministro della salute 9 agosto 2019 (provv. 10 giugno 2021, n. 232, doc. web n. 9681102); favorevole anche la valutazione sul collegato schema di provvedimento del Direttore

4

Accesso alla dichiarazione precompilata

dell'Agenzia delle entrate volto a disciplinare le modalità tecniche di utilizzo, ai fini della elaborazione della dichiarazione dei redditi precompilata, dei dati delle spese sanitarie, a decorrere dall'anno d'imposta 2021 (provv. 22 luglio 2021, n. 275, doc. web n. 9689732).

L'Autorità ha inoltre esaminato lo schema di provvedimento del Direttore dell'Agenzia delle entrate per l'accesso alla dichiarazione precompilata da parte del contribuente e degli altri soggetti autorizzati, a partire dall'anno di imposta 2020, autorizzando l'Agenzia delle entrate ad effettuare il conseguente trattamento dei dati personali (provv. 29 aprile 2021, n. 164, doc. web n. 9677963).

In particolare, l'Autorità ha espresso parere favorevole sugli esiti della sperimentazione avviata nel 2018, che ha consentito ad alcuni Caf di accedere in cooperazione applicativa alle dichiarazioni dei redditi precompilate dei contribuenti. Il Garante ha ritenuto necessario che l'Agenzia delle entrate prosegua la propria attività di controllo a campione sulla legittimità degli accessi alla dichiarazione precompilata effettuati dai Caf nel corso del 2020, verificando i casi di anomalia rilevati, entro il 15 giugno 2021. Il Garante ha, inoltre, ritenuto necessaria un'analoga attività di controllo sugli accessi effettuati, nel corso del 2021, dai Caf nell'ambito della sperimentazione, provvedendo a trasmettere gli esiti all'Autorità, entro il 31 gennaio 2022.

4.1.2. La fatturazione elettronica

Il Garante è stato chiamato nuovamente ad esprimersi sulla fatturazione elettronica in relazione all'attuazione dell'art. 14, d.l. 26 ottobre 2019, n. 124, convertito dalla legge 19 dicembre 2019, n. 157, che ha introdotto la memorizzazione dei *file* XML delle predette fatture (cfr. Relazione 2020, p. 45).

L'Agenzia delle entrate in esito a numerose interlocuzioni con l'Autorità ha sottoposto un nuovo schema di provvedimento in materia di fatturazione elettronica. Il Garante, in seguito a un'approfondita istruttoria, ha dato il via libera a tali trattamenti, condizionandoli tuttavia all'introduzione di una serie di garanzie a tutela dei diritti e delle libertà degli interessati. In particolare, è stato ritenuto necessario rendere inintelligibili i campi relativi alla descrizione dei beni ceduti e dei servizi prestati e agli eventuali allegati, dei *file* XML delle fatture elettroniche (relative ad alcune specifiche operazioni) emesse in ambito legale individuando modalità compatibili con la disciplina relativa all'inalterabilità di tali documenti.

È stato altresì ritenuto necessario che i controlli fiscali nei confronti del consumatore finale, fondati sulle informazioni presenti nei *file* XML delle fatture elettroniche, possano essere avviati esclusivamente a seguito di puntuali verifiche fiscali – poste in essere nei confronti di operatori economici nell'ambito del contrasto all'evasione dell'Iva – i cui beni ceduti o servizi prestati, oggetto della fattura elettronica, siano stati acquistati dalla predetta persona fisica e, contestualmente, gli elementi così rilevati dalla stessa fattura siano tali da far emergere un rischio di evasione fiscale.

Per rendere maggiormente efficaci le predette misure, è stato demandato all'Agenzia il compito di individuare, sentito il Garante, le misure di garanzia adeguate a escludere ulteriori trattamenti dei dati contenuti nei *file* XML delle fatture elettroniche relativi a determinate operazioni, anche adottando sistemi di controllo e monitoraggio che consentano all'Agenzia e al Garante la verifica della conformità ai predetti criteri delle attività di trattamento effettuate nei confronti delle persone fisiche.

Con il provvedimento, è stato altresì ritenuto necessario che analoghe garanzie siano assicurate anche in relazione alle attività di trattamento effettuate dalla Guardia di finanza ai sensi del citato art. 14, d.l. n. 124/2019, previa stipula di apposita

convenzione ai sensi art. 47, d.lgs. n. 51/2018 per l'accesso alle informazioni delle fatture, in conformità al parere del Garante.

Infine sono stati avvertiti i cedenti/prestatori che l'emissione di fatture elettroniche nei confronti del consumatore finale, in luogo di altri documenti commerciali, può violare il RGPD laddove ciò avvenga in assenza di un obbligo di legge, ovvero di una richiesta di quest'ultimo (provv. 22 dicembre 2021, n. 454, doc. web n. 9732234).

4.1.3. Limitazione dei diritti degli interessati in ambito fiscale

Il Garante ha espresso parere favorevole, richiedendo alcune modifiche, sullo schema di decreto del Mef volto ad individuare le categorie e le finalità dei trattamenti di dati, connessi alla lotta all'evasione fiscale, per i quali viene limitato l'esercizio dei diritti dei contribuenti, nonché la portata di tali limitazioni, in attuazione della legge di bilancio 2020 (art. 1, comma 683, l. n. 160/2019).

Il Garante ha ribadito che, in ossequio a quanto previsto dall'art. 23 del RGPD e dall'art. 2-*undecies* del Codice, le limitazioni possono ritenersi legittime solo nella misura in cui dall'esercizio dei diritti degli interessati possa derivare un pregiudizio effettivo e concreto agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale. Inoltre, il legame tra le restrizioni previste e l'obiettivo perseguito dovrebbe essere chiaramente stabilito e dimostrato nella misura legislativa o in documenti supplementari.

In particolare, è stata evidenziata la necessità di integrare lo schema di decreto al fine di garantire la trasparenza dei trattamenti di dati presenti nei *dataset* di analisi e di controllo, oggetto di limitazione, soprattutto in relazione all'attività di profilazione, in considerazione dei potenziali rischi e delle interferenze che tale attività pone in relazione ai diritti degli interessati, fornendo agli stessi un quadro sulla logica sottostante al processo decisionale fondato su trattamenti automatizzati.

Sono state, poi, richieste specifiche garanzie circa il regime applicabile ai diritti degli interessati (e, in particolare, al diritto di accesso) i cui dati dovessero essere presenti nel *dataset* di controllo ma che non dovessero risultare destinatari di inviti o provvedimenti dell'amministrazione finanziaria nei termini prescrizionali, senza comprimere ingiustificatamente il diritto di accesso dei contribuenti ai propri dati personali.

Con riguardo alla pseudonimizzazione dei dati che l'Agenzia dovrà assicurare nell'effettuare tali attività, il Garante ha, invece, sottolineato che occorre individuare tecniche efficaci rispetto all'ingente mole di informazioni presenti in Anagrafe tributaria e nelle altre banche dati, mascherando adeguatamente l'identità delle persone fisiche e riducendo effettivamente i rischi di reidentificazione degli interessati. Altre misure di protezione dei dati potrebbero rendersi necessarie per prevenire, in particolare, erronee rappresentazioni della capacità contributiva, correggendo potenziali errori o distorsioni che potrebbero verificarsi nel processo decisionale fondato su tali trattamenti.

Inoltre, tenendo conto anche di quanto indicato nelle linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del RGPD (adottate dal Gruppo Art. 29 il 3 ottobre 2017 e successivamente aggiornate il 6 febbraio 2018, WP 251 rev.01) l'Autorità ha in particolare evidenziato l'esigenza di adottare misure per assicurare la registrazione del grado di coinvolgimento umano nel processo decisionale e la comprensione, da parte degli operatori ai quali è affidato l'intervento umano, delle capacità e dei limiti del processo decisionale automatizzato, monitorandone debitamente il funzionamento, in modo che i segnali di anomalie, disfunzioni e prestazioni inattese possano essere individuati e affrontati quanto prima.

L'Autorità si è, comunque, riservata di esaminare l'adeguatezza del complesso delle misure adottate a tutela dei diritti e delle libertà degli interessati nell'ambito dell'esame delle valutazioni sulla protezione dei dati che saranno predisposte dall'Agenzia delle entrate e dalla Guardia di finanza, e del provvedimento che sarà predisposto dal Direttore dell'Agenzia (provv. 22 dicembre 2021, n. 453, doc. web n. 9738520).

4.1.4. La lotteria dei corrispettivi

L'Autorità si è espressa su alcuni schemi di provvedimento attuativi della cd. lotteria dei corrispettivi, in attuazione delle disposizioni di cui all'art. 1, comma 542, della legge 11 dicembre 2016, n. 232.

In primo luogo, il Garante ha adottato un parere favorevole sullo schema di provvedimento interdirettoriale di modifica della determinazione del Direttore dell'Agenzia delle dogane e dei monopoli, d'intesa con l'Agenzia delle entrate, del 5 marzo 2020 (su cui il Garante si era favorevolmente espresso con i provv.ti 13 febbraio 2020, n. 30, doc. web n. 9282901 e 1° ottobre 2020, n. 172, doc. web n. 9466165), disciplinante le modalità tecniche relative alle operazioni di estrazione, l'entità e il numero dei premi messi a disposizione, in ragione della modifica legislativa (cfr. art. 1, commi 1095 e 1096, l. n. 178/2020) che ha limitato la possibilità di partecipazione alla lotteria dei corrispettivi ad acquisti effettuati attraverso strumenti di pagamento elettronici.

Lo schema e le valutazioni di impatto predisposte dalle agenzie fiscali hanno tenuto conto delle indicazioni emerse nelle interlocuzioni con il Garante, con particolare riferimento alle misure individuate per assicurare che vengano raccolti e trattati esclusivamente i dati relativi ai corrispettivi per i quali è prevista la partecipazione alla lotteria, cancellando tempestivamente i dati non necessari (pagamenti in contanti o per importi inferiori a un euro) eventualmente trasmessi dagli esercenti (provv. 27 gennaio 2021, n. 33, doc. web n. 9544524).

Successivamente, l'Autorità si è espressa favorevolmente anche sullo schema di provvedimento del Direttore generale dell'Agenzia delle dogane e dei monopoli, formulato d'intesa con il Direttore dell'Agenzia delle entrate, che ha disciplinato l'invio di segnalazioni di mancata partecipazione alla lotteria dei corrispettivi, ovvero i casi in cui l'esercente, al momento dell'acquisto rifiuti di acquisire il codice lotteria. Tali segnalazioni possono essere utilizzate dall'Agenzia delle entrate e dalla Guardia di finanza nell'ambito delle attività di analisi del rischio di evasione (provv. 11 marzo 2021, n. 101, doc. web n. 9568271).

Nel parere, l'Autorità ha rilevato, in particolare, che l'identificazione del soggetto segnalante non risulta necessaria alle attività di analisi del rischio di evasione fiscale e che il sistema consente di evidenziare il motivo della segnalazione trasmessa dal contribuente, ai fini della valutazione del rischio di evasione fiscale, distinguendo le segnalazioni di mero rifiuto di far partecipare alla lotteria il cliente da quelle di mancata certificazione del corrispettivo, meglio indirizzando gli eventuali controlli fiscali nei confronti degli esercenti.

4.1.5. Archivio nazionale dei numeri civici e delle strade

Il Garante si è espresso sullo schema di provvedimento interdirigenziale predisposto dall'Agenzia delle entrate e da Istat per la definizione delle specifiche tecniche e delle modalità di accesso ai servizi erogati dall'Anncsu (Archivio nazionale dei numeri civici e delle strade) (provv. 28 ottobre 2021, n. 282, doc. web n. 9721273).

Si tratta di un archivio nazionale informatizzato, codificato e dinamicamente certificato dai comuni, che in conformità a quanto previsto dal regolamento anagrafico

(d.P.R. 223/1989) ed alla direttiva Inspire (2007/2/CE del 14 marzo 2007) in materia di indirizzi, contiene per ciascun comune, l'elenco delle aree di circolazione e dei relativi numeri civici, nonché le coordinate degli stessi, suddivise nelle sezioni "stradario", l'archivio contenente l'elenco completo degli odonimi utilizzati nel territorio comunale, ossia dei nomi delle aree di circolazione, che individuano ogni spazio del suolo pubblico o aperto al pubblico destinato alla viabilità, "indirizzario", estensione dello stradario comunale che include l'elenco completo dei numeri civici che individuano gli accessi esterni che, dall'area di circolazione, immettono, direttamente o indirettamente, alle unità ecografiche semplici, ossia alle abitazioni, esercizi commerciali, uffici e simili; e "interni", archivio contenente le informazioni relative agli accessi interni che da spazi privati o da scale immettono direttamente alle unità ecografiche semplici ovvero abitazioni, esercizi commerciali, uffici e simili.

Queste informazioni possono essere collegabili alle persone fisiche che – attraverso la mera consultazione di pubblici registri o la interconnessione prevista dal d.P.C.M. con altre banche dati di rilevanza nazionale e regionale – risultano intestatarie, proprietarie, residenti o comunque collegate ai luoghi individuati, comportando così un trattamento di dati personali. I servizi di consultazione individuati nello schema in esame devono perciò essere conformi alla specifica normativa in materia di protezione dati (artt. 25, par. 1, e 35 del RGPD) e individuare le necessarie garanzie. Lo schema di provvedimento ha tenuto conto delle indicazioni fornite dal Garante in sede di interlocuzioni e concernenti, in particolare, la definizione dei ruoli dei soggetti coinvolti nella realizzazione e nella gestione dell'Anncsu, l'individuazione delle informazioni presenti nell'archivio da rendere disponibili attraverso i diversi servizi offerti a soggetti pubblici e privati e le relative modalità di accesso, il tracciamento degli accessi degli utenti all'Anncsu e delle operazioni effettuate.

4.1.6. Altri provvedimenti in ambito fiscale

L'Autorità si è espressa anche sullo schema di decreto del Ministro dell'economia e delle finanze che disciplina le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale sono tenuti a comunicare la propria operatività sul territorio nazionale, nonché le relative forme di cooperazione tra il Mef e le Forze di polizia (provv. 28 ottobre 2021, n. 380, doc. web n. 9721489).

Lo schema esaminato ha tenuto conto delle indicazioni fornite dal Garante nell'ambito delle interlocuzioni informali, con particolare riferimento alla definizione di misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio, per le operazioni effettuate attraverso il portale, la trasmissione periodica dei dati relativi a clienti le transazioni da parte dei prestatori.

Infine, l'Autorità ha reso parere favorevole sullo schema di provvedimento del Mef di cui all'art. 1, comma 501, l. n. 145/2018, che ha disciplinato le modalità di verifica delle dichiarazioni relative al patrimonio mobiliare per la procedura di indennizzo forfettario del Fondo indennizzo risparmiatori (Fir), da adottarsi su proposta della Commissione tecnica del Fir, sentita l'Agenzia delle entrate (provv. 11 febbraio 2021, n. 44, doc. web n. 9556150). In particolare, il Garante ha rilevato che nello schema sono previste le modalità di riscontro da parte dell'Agenzia delle entrate in conformità al principio di minimizzazione, con l'invio dei dati di dettaglio solo in caso di superamento del previsto limite del patrimonio mobiliare. Sono state, inoltre, previste misure tecniche e organizzative adeguate ad assicurare l'integrità e la riservatezza dei dati trasmessi e ricevuti dall'Agenzia, anche nella fase di formazione dell'elenco dei richiedenti oggetto di verifica (firma digitale e cifratura dei *file* oggetto di scambio con l'Agenzia delle entrate).

4

4.2. *Previdenza, assistenza sociale e altri benefici economici*

4.2.1. Erogazione di benefici

Nel corso del 2021, il Garante si è espresso in diverse occasioni in relazione a trattamenti di dati personali necessari per l'erogazione di benefici economici, o comunque di agevolazioni, di varia natura.

Buono veicoli sicuri

Il Ministero delle infrastrutture e della mobilità sostenibili ha sottoposto all'Autorità lo schema di decreto in merito al riconoscimento di un contributo ai sensi dell'art. 1, comma 706, l. n. 178/2020 (cd. buono veicoli sicuri), consistente in un rimborso *una tantum* in favore dei proprietari di veicoli a motore che, dal 1° novembre 2021 e per i successivi tre anni, sottopongono il proprio veicolo alle operazioni di revisione.

Tenuto conto che la piattaforma utilizzata per l'erogazione del buono applica le misure tecniche ed organizzative e le modalità di attuazione utilizzate per altre applicazioni web già vagliate dal Garante, è stato pronunciato parere favorevole, pur con l'osservazione volta a precisare che Sogei spa e Consap spa, responsabili del trattamento, siano dichiarati competenti anche in merito ai relativi controlli (provv. 22 luglio 2021, n. 274, doc. web n. 9689706).

Carta giovani nazionale

Il Garante ha rilasciato parere positivo sullo schema di provvedimento del Capo del Dipartimento per le politiche giovanili e il servizio civile universale della Presidenza del Consiglio dei ministri e, a seguire, sulla valutazione d'impatto sulla protezione dei dati, relativamente alla Carta giovani nazionale, un servizio digitale che permette ai giovani tra i 18 e i 35 anni residenti in Italia di ottenere sconti su manifestazioni culturali, sportive, attività di orientamento professionale, e di accedere all'*European Youth Card.*

In particolare, nel primo parere, il Garante ha rilevato che lo schema di provvedimento in questione costituisce il necessario completamento della base giuridica su cui si fonda il trattamento effettuato, tenuto conto delle lacune presenti nel quadro normativo di riferimento con riguardo alla disciplina sulla protezione dei dati personali (art. 1, commi 413 e 414, l. n. 160/2019, d.m. 27 febbraio 2020) (provv. 22 luglio 2021, n. 276, doc. web n. 9689751); mentre, nel secondo, ha giudicato favorevolmente le misure adottate al fine di mitigare i rischi elevati connessi al trattamento, considerato che sono potenzialmente coinvolti i dati personali di milioni di interessati, rientranti in una specifica fascia di età (provv. 28 ottobre 2021, n. 391, doc. web n. 9722681).

***Bonus* idrico**

Il Ministero della transizione ecologica ha sottoposto all'Autorità lo schema di decreto ministeriale in merito al riconoscimento, ai sensi dell'art. 1, commi 61-65, l. n. 178/2020, di un buono pari a 1.000 euro nei confronti di coloro che intendano effettuare interventi di sostituzione di vasi sanitari in ceramica con nuovi apparecchi a scarico ridotto e di apparecchi di rubinetteria sanitaria, soffioni doccia e colonne doccia esistenti con nuovi apparecchi a limitazione di flusso d'acqua (cd. *bonus* idrico).

Avendo il Ministero tenuto conto delle indicazioni fornite dall'Autorità, anche in relazione alla necessità di fare proprie le misure tecniche ed organizzative e le modalità attuative già assunte nel contesto di altri interventi assimilabili che utilizzano parzialmente la medesima piattaforma, il Garante ha espresso parere favorevole (provv. 16 settembre 2021, n. 333, doc. web n. 9713770).

Carta europea della disabilità

L'Autorità è stata chiamata a pronunciarsi anche sullo schema di provvedimento dell'Inps, attuativo della relativa disciplina normativa (costituita dall'art. 1, comma 563, l. n. 145/2018, come modificata dall'art. 66, comma 2, d.l. n. 77/2021, come convertito, con modificazioni, dalla l. n. 108/2021, nonché dal d.P.C.M. 6 novembre 2020), concernente la Carta europea della disabilità in Italia, ossia uno strumento,

alternativo al verbale cartaceo anche in formato *omissis,* che consente alle persone diversamente abili di usufruire delle agevolazioni a loro dedicate (in particolare da parte delle p.a.) mediante un QR *code* che, senza fornire ulteriori informazioni o dati, consente di visionare lo stato invalidante attualizzato.

Il Garante, vagliata la relativa valutazione d'impatto sulla protezione dei dati, ha espresso parere favorevole, tenuto conto delle modifiche apportate allo schema di provvedimento a seguito delle interlocuzioni avute con l'Inps. Il parere contiene tuttavia osservazioni riguardanti alcuni profili di criticità, quali l'adozione di misure che, per impostazione predefinita, garantiscano l'accesso alle sole informazioni indispensabili all'erogazione del servizio offerto, nonché l'indicazione sull'avvalimento dell'Istituto poligrafico e Zecca dello Stato e del gestore esterno, da parte dell'Inps, in qualità di responsabili del trattamento ai sensi dell'art. 28 del RGPD (provv. 14 ottobre 2021, n. 368, doc. web n. 9716806).

4.2.2. Isee

Il Ministero del lavoro e delle politiche sociali ha chiesto al Garante il parere sullo schema di decreto concernente l'individuazione delle modalità estensive dell'Isee corrente, con il quale si dispone l'aggiornamento dei dati relativi alla situazione patrimoniale all'anno precedente alla presentazione della Dsu, con il conseguente adeguamento delle modalità di rilevazione delle omissioni o difformità e di esecuzione dei controlli sui dati autodichiarati, al fine di consentire l'accesso alle prestazioni dei nuclei familiari in stato di bisogno per i quali la situazione patrimoniale riferita ai due anni precedenti (come invece previsto in via ordinaria dall'art. 10, comma 4, d.lgs. n. 147/2017) non rappresenti la situazione corrente.

Il Garante si è pronunciato positivamente, a condizione, però, che i flussi di dati personali previsti tra l'Inps e l'Agenzia delle entrate avvengano con le modalità definite nel disciplinare tecnico attuativo adottato dall'Istituto medesimo ai sensi dell'art. 12, comma 2, del d.P.C.M. 5 dicembre 2013, n. 159, non essendo sufficiente il richiamo a meri accordi convenzionali tra i due enti (provv. 13 maggio 2021, n. 189, doc. web n. 9699649).

4.2.3. Banca dati del collocamento mirato

Il Ministero del lavoro e delle politiche sociali ha sottoposto all'esame dell'Autorità lo schema di decreto del Ministro che istituisce e regola la banca dati del collocamento mirato, ai sensi dell'art. 9, comma 6-*bis,* l. 12 marzo 1999, n. 68, e dell'art. 8, d.lgs. 14 settembre 2015, n. 151, ossia una sezione della banca dati politiche attive e passive detenuta dal Ministero medesimo, finalizzata a razionalizzare la raccolta sistematica dei dati disponibili sul collocamento mirato, semplificare gli adempimenti, rafforzare i controlli e migliorare il monitoraggio e la valutazione degli interventi concernenti il diritto al lavoro delle persone disabili.

Lo schema ha tenuto conto delle indicazioni fornite dall'Autorità nel corso di interlocuzioni informali – quali quelle concernenti l'individuazione delle informazioni pertinenti ed indispensabili per le finalità di inserimento lavorativo, tra quelle contenute nel verbale di accertamento delle condizioni di disabilità, o quelle volte a chiarire le tipologie di dati oggetto degli scambi informativi con soggetti, quali il Dipartimento della funzione pubblica presso la Presidenza del Consiglio dei ministri e l'Inail; il Garante ha quindi espresso parere favorevole, pur rilevando la necessità di raccordare le specifiche competenze dell'Anpal con la banca dati in questione, nonché osservando che l'accesso ai soggetti legittimati non può essere consentito senza limitazioni di visibilità, ma solo alle tipologie di dati personali puntualmente individuati (provv. 11 novembre 2021, n. 396, doc. web n. 9731800).

4

4.2.4. Controlli sul bonus *Covid per titolari di incarichi politici*

Sulla base di alcune notizie di stampa, l'Autorità ha condotto un accertamento nei confronti dell'Inps con riferimento ai controlli antifrode effettuati in merito all'erogazione di prestazioni a sostegno del reddito, legate alla situazione emergenziale da Covid-19 e previste dal d.l. n. 18/2020 (cd. *bonus* Covid). Da tale accertamento è emerso che l'Istituto ha acquisito i dati personali riferiti a parlamentari e amministratori regionali e locali da banche dati esterne della Camera e del Ministero dell'interno, per poi successivamente elaborarli e raffrontarli con quelli dei soggetti richiedenti il *bonus* Covid in proprio possesso, senza però aver predeterminato con certezza per tutti i menzionati soggetti se il rivestire una carica politica rappresentasse una condizione ostativa al riconoscimento dell'indennizzo.

Il Garante, pur riconoscendo che i trattamenti effettuati dall'Inps (con i relativi controlli) al fine di concedere o revocare benefici economici, agevolazioni o altri emolumenti, sono sicuramente riconducibili a rilevanti compiti di interesse pubblico, ha rilevato nel caso di specie, una violazione del principio di liceità, correttezza e trasparenza del trattamento (art. 5, par. 1, lett. *a*), del RGPD).

Inoltre, è stato rilevato che il trattamento, in violazione del principio di minimizzazione dei dati (art. 5, par. 1, lett. *c*), del RGPD), aveva invece coinvolto tutti i richiedenti il *bonus* Covid, compresi quelli le cui domande già, in sede di controllo di primo livello, erano state rigettate e che l'Inps aveva attribuito agli interessati un codice fiscale calcolato automaticamente e solo in via presuntiva, in violazione del principio di esattezza (art. 5, par. 1, lett. *d*), del RGPD). Per le medesime ragioni è stata, conseguentemente, accertata anche la violazione dei principi di *privacy by design* e *by default* (art. 25 del RGPD), nonché è stato rilevato che la non adeguata ponderazione circa la sussistenza di un rischio elevato ha comportato la mancata effettuazione della necessaria valutazione d'impatto sulla protezione dei dati (art. 35 del RGPD); infine, è emerso che l'Istituto non ha neanche comprovato in maniera congrua le ragioni delle decisioni assunte, violando in questo modo il principio di *accountability* (artt. 5, par. 2, e 24, del RGPD).

In considerazione di tutto ciò, il Garante ha comminato all'Inps una sanzione da 300.000 euro e ha ingiunto al medesimo Istituto di cancellare tutti i dati personali fino a quel momento trattati in violazione del principio di minimizzazione e di effettuare la valutazione di impatto sulla protezione dei dati (provv. 25 febbraio 2021, n. 87, doc. web n. 9556958).

4.2.5 Altri provvedimenti correttivi

Il Garante ha altresì comminato una sanzione da 12.000 euro all'Inps per non aver fornito, nei termini richiesti, il dovuto riscontro ad un interessato che aveva esercitato, per due volte, il diritto di accesso ai dati personali relativamente a una comunicazione a terzi dei dati personali riferiti al proprio estratto contributivo, e, quindi, per aver violato gli artt. 5, par. 1, lett. *a*), 12 e 15 del RGPD. Nella medesima occasione, sono state archiviate le doglianze relative a presunte violazioni connesse all'accesso effettuato in passato da un dipendente ai dati personali riferiti all'interessato, tenuto conto del notevole lasso temporale trascorso, anche alla luce dei tempi di conservazione di atti e documenti, che avrebbero impedito all'Istituto di recuperare la documentazione idonea a comprovare la legittimità dell'accesso in questione (provv. 15 aprile 2021, n. 139, doc. web n. 9592133).

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

Anche nel 2021 il Garante ha interagito con il Ministero dell'istruzione, le università, le istituzioni scolastiche ed altri soggetti pubblici nel corso di incontri e contatti volti a fornire chiarimenti e indicazioni in merito alla corretta applicazione della disciplina in materia di protezione dei dati personali.

Carta dello studente IoStudio

In tale ambito, particolare rilievo ha assunto il provvedimento con il quale il Garante ha espresso, ai sensi degli artt. 36, par. 4, e 57, par. 1, lett. *c*), del RGPD, parere favorevole sullo schema di decreto predisposto dal Ministero dell'istruzione concernente la definizione dei criteri e delle modalità di realizzazione e distribuzione della Carta dello studente denominata IoStudio ai sensi dell'art. 10, comma 5, ultimo periodo, d.lgs. n. 63/2017 (provv. 30 settembre 2021, n. 359, doc. web n. 9713787).

Lo schema di decreto presentato prevede che, agli studenti della scuola secondaria di secondo grado statale e paritaria e agli studenti frequentanti i percorsi di istruzione e formazione professionale, venga attribuita, su richiesta, la Carta dello studente: una tessera nominativa, utilizzabile anche nella forma di applicazione web, cui sono associate funzionalità volte ad agevolare l'accesso a beni e servizi di natura culturale, servizi per la mobilità, ausili di natura tecnologica e multimediale per lo studio e per l'acquisto di materiale scolastico, allo scopo di garantire e supportare il diritto allo studio.

Alla Carta sono associate funzionalità per accedere al sistema nazionale di erogazione dei *voucher* in forma virtuale (borse di studio e benefici analoghi).

Lo schema di decreto ha tenuto conto delle indicazioni fornite dal Garante, in particolare, riguardo: l'individuazione dei dati personali che il Ministero, in qualità di titolare del trattamento e nel rispetto dei principi di liceità, correttezza, trasparenza e minimizzazione dei dati, acquisisce dall'Anagrafe nazionale dello studente, in relazione alle finalità di volta in volta perseguite; i profili connessi alla trasparenza del trattamento e alle modalità di esercizio dei diritti degli interessati; le procedure da seguire in caso di mancata ricezione, smarrimento, distruzione, o sottrazione della Carta; le misure tecniche e organizzative nonché le modalità del trattamento e i termini di conservazione dei dati; i profili relativi ai rischi che presenta il trattamento, effettuato su larga scala e relativo a soggetti minori, nonché l'individuazione di adeguate misure di sicurezza tecniche e organizzative e di congrui tempi di conservazione dei dati da effettuarsi nell'ambito di una valutazione di impatto ai sensi dell'art. 35 del RGPD.

Anagrafe nazionale dell'istruzione superiore

Il Garante ha espresso, inoltre, in via d'urgenza parere favorevole sullo schema di decreto predisposto dal Ministro dell'università e della ricerca, di concerto con il Ministro per l'innovazione tecnologica e la transizione digitale e con il Ministro per la p.a., concernente l'Anagrafe nazionale dell'istruzione superiore (Anis) (provv. 2 dicembre 2021, n. 428, doc. web n. 9731869).

L'Anis, la cui piena operatività avverrà a seguito di uno specifico decreto attuativo, mira ad assicurare alle istituzioni della formazione superiore e alle p.a., la disponibilità dei dati necessari per lo svolgimento delle funzioni di competenza e contiene i dati anagrafici degli interessati, i dati relativi alle iscrizioni, all'istituzione di appartenenza, ai corsi di studio e ai titoli conseguiti dagli studenti nonché l'indicazione del periodo di conservazione di tali informazioni.

L'Anagrafe ha, inoltre, lo scopo di favorire l'interoperabilità con le altre banche dati, anche di interesse nazionale ai sensi dell'art. 60 del Cad e l'automazione delle procedure di iscrizione *online* ai corsi delle istituzioni della formazione superiore, anche attraverso l'accesso, in consultazione, alle banche dati di altre amministrazioni.

4

Il decreto prevede, al fine di assicurare l'esattezza e l'aggiornamento dei dati, che questi siano costantemente allineati, in conformità alle linee guida adottate dall'AgID in materia di interoperabilità, con i dati contenuti nell'Anagrafe nazionale degli studenti, dei diplomati e dei laureati degli istituti tecnici superiori e delle istituzioni della formazione superiore e, con riguardo ai dati anagrafici, con l'Anpr senza dare luogo a duplicazione dei dati.

Lo schema di decreto, che tiene conto delle osservazioni del Garante, contiene le principali garanzie a tutela dei diritti e delle libertà fondamentali degli interessati nonché misure di base per la sicurezza e integrità dei dati.

Tali osservazioni hanno riguardato diversi profili quali l'individuazione dei dati oggetto del trattamento da parte del Ministero e delle finalità dell'Anis; dei soggetti legittimati ad accedere alla banca dati; dei tempi di conservazione delle diverse categorie di dati in relazione a ciascuna finalità perseguita; del ruolo assunto dai soggetti coinvolti nel trattamento di dati personali, in relazione alla specifica finalità perseguita, precisando che il Ministero, analogamente alle istituzioni della formazione superiore con riguardo ai dati di loro competenza, opera in qualità di titolare del trattamento dei dati contenuti nell'Anis; delle misure a tutela degli interessati, tenuto conto dei rischi elevati che presenta il trattamento, realizzato su larga scala, sia in termini di numerosità degli interessati che di estensione geografica, nonché delle adeguate misure tecniche e organizzative e dei congrui tempi di conservazione dei dati, da effettuare nell'ambito di una valutazione di impatto ai sensi dell'art. 35 del RGPD (art. 9 dello schema); delle garanzie per assicurare il rilascio agli interessati delle certificazioni anche relative ai titoli di studio da parte delle istituzioni della formazione superiore – cui la funzione certificatoria è attribuita dalla normativa di settore anche attraverso la specifica interfaccia *online* di Anis

L'Autorità ha reso il proprio parere sul presupposto che in ogni caso la piena operatività dell'Anis e l'avvio dei conseguenti trattamenti di dati, avverranno solo a seguito della completa definizione del quadro giuridico di riferimento mediante l'emanazione del successivo decreto attuativo, da sottoporre al parere del Garante.

Il Garante ha infine evidenziato, data la concomitante operatività dell'Anis con la preesistente Anagrafe nazionale, la necessità di evitare la sovrapposizione delle due anagrafi auspicando a tal fine, che il quadro normativo di settore venga integrato regolando l'utilizzo di tali anagrafi e le modalità di interazione tra le stesse.

4.3.1. I trattamenti di dati personali in ambito scolastico e universitario nel contesto dell'emergenza epidemiologica da Covid-19

DDI e sistemi di supervisione delle prove d'esame a distanza

Nel 2021, sono pervenuti numerosi reclami, segnalazioni e quesiti connessi all'ampio ricorso da parte di scuole e atenei alle piattaforme per l'attività didattica a distanza e a sistemi di supervisione delle prove d'esame da remoto (cd. *proctoring*) utilizzati al fine di assicurare la continuità didattica con modalità compatibili con le esigenze di salute pubblica connesse all'emergenza epidemiologica da Covid-19.

Al riguardo l'Autorità ha rafforzato la collaborazione istituzionale con il Ministero dell'istruzione anche nell'ambito del gruppo di lavoro congiunto relativo ai trattamenti di dati personali di alunni e docenti effettuati mediante il registro elettronico e altri principali strumenti di svolgimento della didattica a distanza e didattica digitale integrata (DAD e DDI).

Più in dettaglio il Garante ha evidenziato taluni profili critici con particolare riferimento alle modalità di identificazione/autenticazione degli utenti che accedono alla piattaforma (personale scolastico, studenti e famiglie); alla definizione dei ruoli, anche ai fini della protezione dei dati, dei diversi soggetti coinvolti in relazione ai flussi di dati che il progetto comporta. L'Autorità ha inoltre raccomandato al

Ministero di rafforzare la propria attività di vigilanza nell'ambito delle procedure di accreditamento delle principali piattaforme per la DAD adottate dalle scuole, richiedendo l'aggiornamento dei protocolli d'intesa, siglati dal Ministero, con i fornitori (attualmente disponibili nell'apposita sezione del sito istituzionale del Ministero: https://www.istruzione.it/ProtocolliInRete/Protocolli_Accordi.html) al fine di garantire livelli omogenei di tutela sotto il profilo della protezione dei dati.

Con riferimento al settore universitario, in particolare ai sistemi di supervisione (*proctoring*) per identificare gli studenti che si sottopongono a prove d'esame a distanza e monitorare il loro comportamento durante lo svolgimento delle stesse, il Garante nel richiamare la posizione espressa dal Presidente dell'Autorità nel corso di un'audizione al Senato, ha ricordato che tali sistemi "non devono essere indebitamente invasivi e comportare un monitoraggio dello studente eccedente le effettive necessità", in quanto, sebbene il rispetto delle regole di svolgimento delle prove vada garantito anche *online*, non possono considerarsi accettabili sistemi che comportano "una sorveglianza elettronica priva dei necessari limiti e garanzie" (cfr. parr. 2 e 3.1.1).

Su tale delicata tematica, a seguito di un reclamo proposto da uno studente, il Garante ha avviato una complessa istruttoria nei confronti di un ateneo privato, che, nel contesto dell'emergenza epidemiologica da Sars-CoV-2, aveva impiegato un sistema di supervisione degli esami a distanza basato sul trattamento di dati biometrici relativi alla geometria del volto degli studenti, previa acquisizione del consenso degli stessi.

Il Garante, ha, anzitutto, chiarito, sia per i soggetti pubblici sia per quelli privati, che i trattamenti dei dati degli studenti finalizzati al rilascio di titoli di studio aventi valore legale o quelli connessi allo svolgimento di attività soggette alla vigilanza del Ministero dell'università e della ricerca trovano il loro fondamento nella necessità di "adempiere un obbligo legale al quale è soggetto il titolare del trattamento" o di dare "esecuzione [a] un compito di interesse pubblico o connesso all'esercizio di pubblici poteri" (art. 6, par. 1, lett. *c*) ed *e*), e, con riguardo alle categorie particolari di dati, art. 9, lett. *g*), del RGPD), non essendo, invece, invocabili altre basi giuridiche quali il consenso e/o il contratto.

Con specifico riguardo ai presupposti di liceità per il trattamento dei dati biometrici, il Garante ha rilevato la mancanza di una base giuridica, e ritenuto che il consenso degli studenti non potesse costituirla (essendo il trattamento effettuato ai fini del rilascio di titoli di studio aventi valore legale) né potesse ritenersi una manifestazione di volontà libera (art. 4, par. 1, n. 11), del RGPD), in ragione dello squilibrio della posizione degli studenti rispetto al titolare del trattamento (cfr. cons. n. 43 del RGPD). Ha inoltre ritenuto che i trattamenti di dati consistenti nell'analisi del comportamento degli studenti nel corso della prova d'esame non potessero considerarsi necessari per l'esecuzione di un compito di interesse pubblico, dovendo, quindi, il trattamento essere previsto da una norma di legge o di regolamento che, nel caso di specie, era insussistente.

Sono stati rilevati ulteriori profili di violazione della normativa quali l'inidoneità dell'informativa fornita agli studenti; la non conformità dei trattamenti ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, minimizzazione e limitazione della conservazione; i presupposti di liceità per il trasferimento dei dati personali degli studenti a un fornitore dell'ateneo stabilito negli Stati Uniti d'America, anche alla luce della sentenza della CGUE del 16 luglio 2020 (*Data Protection Commissioner* contro Facebook Ireland Limited e Maximillian Schrems, Causa C-311/18); la non sufficiente adeguatezza della valutazione d'impatto sulla protezione dei dati predisposta dall'università.

4

Il Garante ha, infine, disposto la limitazione del trattamento, vietando all'ateneo ogni ulteriore operazione di trattamento, con riguardo ai dati biometrici degli studenti e ai dati sulla cui base veniva effettuata la profilazione degli interessati mediante il sistema di supervisione in questione, nonché ha vietato il trasferimento dei dati personali degli interessati negli Stati Uniti d'America, in assenza di adeguate garanzie per gli stessi (provv. 16 settembre 2021, n. 317, doc. web n. 9703988).

4.3.2. Il trattamento di dati personali relativi allo stato vaccinale di studenti e famiglie

Un rilevante numero di reclami, segnalazioni e richieste di chiarimenti ha riguardato alcune iniziative, realizzate in ambito scolastico, finalizzate a conoscere, anche indirettamente, lo stato vaccinale degli studenti e delle rispettive famiglie.

Al riguardo il Garante ha inviato una lettera al Ministero dell'istruzione affinché quest'ultimo provvedesse a sensibilizzare gli istituti scolastici in relazione ai rischi per i diritti e le libertà degli interessati derivanti dall'assunzione di tali iniziative. Di tale circostanza si è dato conto in un comunicato stampa (23 settembre 2021, doc. web n. 9702160) chiarendo, in particolare, che non è consentito agli istituti scolastici conoscere lo stato di vaccinazione da Covid-19 degli studenti, ai quali non è richiesto, quale condizione generale per accedere alle strutture delle istituzioni scolastiche, educative e formative e ai relativi sevizi, il possesso e l'esibizione della certificazione verde in corso di validità. Anche con riguardo ai familiari, sebbene, in base a quanto previsto dal d.l. 22 aprile 2021, n. 52, chiunque acceda alle strutture scolastiche, deve possedere ed esibire la certificazione verde Covid-19, le amministrazioni scolastiche non possono trattare informazioni relative all'avvenuta o meno vaccinazione, dovendosi limitare a verificare, mediante il personale autorizzato, il mero possesso della certificazione all'ingresso dei locali scolastici e non potendo, in particolare, conoscere la condizione alla base della quale la certificazione è rilasciata (vaccinazione, guarigione o esito negativo del tampone).

Nella nota inviata al Ministero dell'istruzione, il Garante ha sottolineato che eventuali richieste, rivolte dal personale agli studenti (anche mediante domande generalizzate formulate nei confronti della classe, con invito a rispondere, anche, per alzata di mano), o comportamenti comunque volti ad acquisire informazioni sull'avvenuta vaccinazione degli stessi o dei loro familiari, potrebbero suscitare situazioni di disagio per gli alunni in ragione delle scelte adottate dalle rispettive famiglie. Con l'occasione il Garante ha invitato il Ministero a richiamare l'attenzione dei dirigenti scolastici e del personale docente e non docente sugli effetti di simili comportamenti e sulle rispettive responsabilità, anche sul piano educativo.

Comunicazione di dati sulla salute relativi ad alunni

Anche nel 2021 il Garante ha definito numerosi reclami e segnalazioni aventi ad oggetto la diffusione, su siti web istituzionali, di dati personali relativi al personale scolastico e agli alunni nonché alla comunicazione di dati personali, anche relativi alla salute, di soggetti di minore età, in assenza di un'idonea base giuridica e in violazione dei principi applicabili al trattamento dei dati (cfr. par. 14.11).

In tale ambito il Garante ha censurato il comportamento di un Ufficio scolastico regionale (Usr), che – a seguito di un esposto presentato dall'interessato al Dipartimento della funzione pubblica in merito alle presunte irregolarità commesse da un istituto scolastico in relazione all'attribuzione delle ore di sostegno previste per gli alunni con disabilità – aveva inviato al richiamato Dipartimento documentazione contenente dati personali riguardanti il figlio del reclamante, comprensivi di informazioni relative allo stato di salute del minore. L'Usr, benché tenuto a rappresentare all'Ispettorato per la funzione pubblica tutti gli elementi utili a chiarire gli aspetti relativi alle modalità di assegnazione delle cattedre di sostegno, avrebbe

potuto fornire il necessario riscontro senza comunicare al Dipartimento anche i dati personali del minore. Il Garante ha pertanto irrogato al Ministero dell'istruzione una sanzione pecuniaria ritenendo che il trattamento dei dati personali dell'alunno fosse stato effettuato dall'Usr in assenza di un idoneo presupposto giuridico, in violazione dei principi applicabili al trattamento di cui all'art. 5, par. 1, lett. *a*) e degli artt. 6 e 9 del RGPD, nonché degli artt. 2-*ter* e 2-*sexies* del Codice (provv. 25 febbraio 2021 n. 67, doc. web n. 9565218).

4.3.3. Esercizio dei diritti

L'attività dell'Autorità relativa all'ambito scolastico e universitario ha riguardato, inoltre, la trattazione di reclami relativi al mancato o inidoneo riscontro a richieste di esercizio dei diritti di cui agli artt. 15-22 del RGPD.

In particolare in merito ad un reclamo concernente l'esercizio del diritto di accesso ai dati relativi a uno studente universitario, l'Autorità ha ammonito l'università ritenendo la condotta tenuta dalla stessa non fosse conforme agli artt. 12 e 15 del RGPD non avendo l'ateneo fornito un riscontro alla richiesta dell'interessato se non a seguito dell'invito ad aderire alle richieste di quest'ultimo formulato dal Garante (provv. 14 gennaio 2021, n. 2021, doc. web n. 9540654).

Analogamente è stato ammonito un istituto scolastico che aveva fornito riscontro alla richiesta di esercizio del diritto di accesso ai dati personali presentata da un reclamante solo a seguito dell'intervento dell'Ufficio e oltre il termine previsto dall'art. 12 del RGPD, senza, peraltro, avere informato l'interessato dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo o ricorso giurisdizionale entro il medesimo termine, in violazione dell'art. 12, parr. 3 e 4, del RGPD (provv. 16 dicembre 2021 n. 437, doc. web n. 9737156).

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.

Per esigenze di chiarezza espositiva si esamineranno separatamente le questioni riguardanti la pubblicazione di dati personali *online,* i casi di comunicazione di dati personali effettuate in maniera non conforme al RGPD, nonché di accesso civico a informazioni e documenti detenuti dalla p.a. (art. 5, d.lgs. n. 33/2013).

4.4.1. La pubblicazione di dati personali online *da parte delle p.a.*

Data protection by design e by default

Da menzionare un provvedimento ingiuntivo e sanzionatorio adottato nei confronti di un comune di grandi dimensioni, che in maniera non conforme al RGPD, consentiva di visualizzare tramite un'apposita maschera di ricerca *online* – attraverso l'inserimento del solo codice fiscale e senza richiedere alcuna identificazione dell'utente – dati personali di soggetti beneficiari di agevolazioni economiche in condizioni di disagio sociale (provv. 22 luglio 2021, n. 295, doc. web n. 9696764; in tema di rispetto del principio della *data protection by design* cfr. provv. 14 gennaio 2021, n. 22, doc. web n. 9543138, su cui *infra*).

Analogamente, si è ingiunto a un comune di mettere in atto misure tecniche e organizzative adeguate con particolare riferimento al servizio di pubblicazioni all'Albo pretorio, e al successivo passaggio nella sezione storica dell'Albo, in modo da evitare automatismi nella pubblicazione di atti sul sito web istituzionale che possano portare a illecite diffusioni di dati personali, integrando "nel trattamento le necessarie

garanzie al fine di soddisfare i requisiti del RGPD e tutelare i diritti degli interessati (art. 25, parr. 1 e 2, RGPD)" (provv. 8 luglio 2021, n. 301, doc. web n. 9703112).

Tecniche di oscuramento dei dati personali non efficaci

Sempre con riferimento all'art. 25 del RGPD alcune amministrazioni avevano pubblicato documenti *online* oscurando i dati personali ivi contenuti, con strumenti non idonei, in quanto agevolmente superabili, ad es. tramite una semplice operazione di "copia" delle informazioni oscurate (quali etichette oscuranti, barre di colore nero, ecc.) e di successiva operazione di "incolla" all'interno di un *file*.doc (es. *word*), che restituiva in chiaro tutti i dati personali che si volevano non rendere visibili. Per di più, la tecnica di oscuramento adottata non impediva l'indicizzazione, rimanendo pertanto possibile ricercare le informazioni oscurate contenute nei *file* pubblicati *online* tramite i motori di ricerca web. Ciò è avvenuto, ad esempio, in relazione alla pubblicazione delle copie integrali dei documenti relativi agli accessi civici presentati a una amministrazione (fra cui l'istanza e l'esito) (provv. 11 febbraio 2021, n. 55, doc. web n. 9574117) e nel caso di un documento pubblicato sul sito web istituzionale di un ente parco che conteneva informazioni su un procedimento penale a carico dei reclamanti e la data dell'udienza preliminare (provv. 8 luglio 2021, n. 302, doc. web n. 9703134, su cui anche *infra*).

In numerosi casi inoltre il Garante ha sanzionato il titolare del trattamento per illecita diffusione dei dati sul web, talvolta prescrivendo le misure da adottare.

Sanzioni o ammonimenti per illecita diffusione di dati sulla salute

Al riguardo si continuano a registrare casi in cui sono stati oggetto di pubblicazione *online* dati sulla salute in violazione dell'art. 2-*septies,* comma 8, del Codice e dell'art. 9, parr. 1, 2 e 4, del RGPD, in particolare ad opera di regioni, aziende sanitarie e comuni per la diffusione dei dati sulla salute su siti web istituzionali riferiti a:

- persone sottoposte a tampone, o risultate positive al test Covid-19, oppure poste in quarantena, resi pubblici sul sito web di un comune (provv. 14 ottobre 2021, n. 372, doc. web n. 9714644);
- soggetti indicati in un prospetto riepilogativo di posizioni debitorie, (da 13.000 a 227.000 euro) allegato a una determinazione del direttore generale di un'azienda ospedaliera, in cui erano riportati il nome e cognome dei soggetti assistiti, il periodo di ricovero, il reparto di assistenza e la cifra dovuta all'azienda (provv. 27 maggio 2021, n. 215, doc. web n. 9689307);
- soggetti danneggiati, indicati nei *file* delle statistiche sui risarcimenti danni nell'ambito di una procedura di affidamento del servizio assicurativo di responsabilità civile generale di un comune, con indicazione in chiaro, fra l'altro, del nominativo, della dinamica e tipologia di danno, della data del sinistro e dell'entità della somma ricevuta a titolo di risarcimento, dell'esistenza della lesione fisica riportata dal soggetto danneggiato e della relativa tipologia (es. frattura collo femorale per omessa manutenzione marciapiede) (provv. 29 aprile 2021, n. 168, doc. web n. 9681028);
- soggetti in condizione di disabilità, contenuti in una deliberazione della giunta regionale, facendo peraltro riferimento a una precedente pubblicazione dei medesimi dati personali, il cui trattamento era già stato oggetto di una declaratoria di illegittimità da parte del Garante nei confronti della stessa regione (provv. 8 luglio 2021, n. 269, doc. web n. 9693386);
- un reclamante beneficiario di sussidi economici nell'ambito di piani a sostegno di persone con handicap, contenuti in un provvedimento dei servizi sociali pubblicato nell'area "Sovvenzioni, contributi, sussidi, vantaggi economici", della sezione "Amministrazione trasparente" del sito web istituzionale di un comune (provv. 29 aprile 2021, n. 167, doc. web n. 9678951);
- soggetti citati in una determinazione di liquidazione, quali il nominativo del reclamante e del padre a suo carico con indicazione della relativa situazione di

disabilità, la data e il luogo di nascita, la residenza, nonché le informazioni relative alla liquidazione dell'importo del contributo previsto per il superamento e l'eliminazione di barriere architettoniche presenti nel proprio alloggio con indicazione dell'indirizzo del soggetto disabile, dei singoli lavori effettuati, compresivi di riferimenti dettagliati alle fatture e all'indicazione delle imprese a cui ci si era rivolti (provv. 16 settembre 2021, n. 324, doc. web n. 9704069).

In molti casi sono state adottate specifiche sanzioni o ammonimenti, 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, parr. 1, lett. *c*) ed *e*), 2 e 3, lett. *b*), del RGPD; nonché del principio di minimizzazione di cui all'art. 5, par. 1, lett. *c*), del RGPD. Ciò con particolare riferimento alla pubblicazione di dati e informazioni personali su siti web istituzionali di amministrazioni centrali, regioni, prefetture, università, enti parco, comuni relativi, tra l'altro, a:

Dati comuni eccedenti

- migliaia di soggetti interessati (ca. 5.000), inseriti nell'elenco dei "*Manager* qualificati e delle società di consulenza" di un ministero, al fine di consentire l'incontro tra la domanda delle società potenzialmente beneficiarie del *voucher* per l'acquisto di prestazioni consulenziali di natura specialistica e l'offerta di consulenza da parte dei *manager* stessi, con indicazione in chiaro del nominativo, codice fiscale, indirizzo *e-mail* e *curriculum vitae* integrale (con ulteriori dati personali, quali numero cellulare, istruzione e formazione, in alcuni casi anche copia del documento di riconoscimento ecc.) (provv. 11 febbraio 2021, n. 54, doc. web n. 9556625). Il ministero (titolare del trattamento) è stato anche sanzionato per non aver designato, entro la data del 25 maggio 2018 in cui è divenuto applicabile il RGPD, il Rpd e per non aver comunicato al Garante entro la medesima data i relativi dati di contatto come previsto dalla disciplina europea;
- un reclamante (quali il nominativo e l'indirizzo di residenza), contenuti nel testo e nell'oggetto di un decreto dirigenziale adottato da una regione, nell'ambito di un procedimento di revoca del finanziamento concesso alla ditta individuale intitolata al citato reclamante (provv. 22 luglio 2021, n. 280, doc. web n. 9695441);
- centinaia di soggetti – fra cui i procuratori di due società e i loro familiari maggiorenni conviventi – inseriti in documenti prodotti a uso interno da una prefettura nell'ambito di una richiesta di certificazione antimafia e resi accessibili *online* per un errore materiale (provv. 29 settembre 2021, n. 350, doc. web n. 9719797);
- un minore di 9 anni e alla madre che non aveva pagato le rette della mensa del figlio, contenuti in un atto da notificare a persone senza fissa dimora reso visibile in forma integrale sull'Albo pretorio *online* di un comune di grandi dimensioni. Nel caso di specie, è stato inoltre ingiunto all'ente di conformare le notifiche degli atti nei confronti dei predetti soggetti alla normativa statale di settore contenuta negli artt. 140 ss. del c.p.c. (per la notifica degli atti giudiziari) e nell'art. 60, d.P.R. n. 600/1973 (per la notifica degli atti tributari), che in nessun caso prevedono la pubblicazione integrale dell'atto da notificare (provv. 27 gennaio 2021, n. 39, doc. web n. 9556172);
- un reclamante (fra cui, oltre nome e cognome, anche data e luogo di nascita, residenza, Pec, numero di cellulare, firma autografa), contenuti nelle domande poste dallo stesso all'amministrazione in occasione di un *question time* e nelle risposte fornite dalla p.a. (provv. 25 febbraio 2021, n. 73, doc. web n. 9574764);

Benefici economici a persone in stato di disagio

- soggetti beneficiari e non beneficiari di contributi economici inferiori a mille euro (quali nominativo, importo del canone di abitazione mensile e annuo pagato, contributo economico assegnato per il pagamento del predetto canone), riservati a persone con un basso reddito familiare e che avevano ricevuto una riduzione superiore al 30% del reddito complessivo del nucleo familiare per cause riconducibili all'emergenza epidemiologica da Covid-19, idonei a rivelare una situazione di disagio economico-sociale degli interessati (provv. 16 settembre 2021, n. 323, doc. web n. 9713735);

Procedimenti edilizi

- un reclamante e i suoi familiari (fra cui nominativo, data e luogo di nascita, codice fiscale, residenza), contenuti in diverse ordinanze sindacali, con cui è stato ordinato lo sgombero immediato di immobili e l'ingiunzione di pagamento della connessa sanzione amministrativa, nell'ambito di una vicenda riferita a un procedimento relativo a opere eseguite in assenza del permesso di costruire (provv. 11 marzo 2021, n. 91, doc. web n. 9578258);

Procedimenti giudiziari

- alcuni reclamanti, relativi a un procedimento penale (provv. 8 luglio 2021, n. 302, doc. web n. 9703134, cit.);
- un reclamante (quali il nominativo, la data e il luogo di nascita, l'indirizzo di residenza, il codice fiscale, il codice iban personale su cui accreditare le somme dovute dal comune, nonché dettagli particolareggiati del contenzioso nei confronti dell'ente dinnanzi al tribunale ordinario) contenuti in alcune determinazioni dirigenziali e nei relativi allegati (provv. 16 settembre 2021, n. 325, doc. web n. 9714622);

Registro degli accessi civico e documentale

- numerosi soggetti interessati che hanno formulato richieste di accesso al comune a dati contenuti nel registro degli accessi civico e documentale (quali, fra l'altro, nome richiedente, data della richiesta, oggetto, esito, motivazioni del diniego) (provv. 22 luglio 2021, n. 281, doc. web n. 9696645);

Provvedimenti in materia di lavoro pubblico

- numerosi soggetti, dipendenti e lavoratori in generale delle p.a. (ad es.: procedimenti disciplinari, notizie sulle mansioni svolte, procedure concorsuali, graduatorie, avanzamenti di carriera, ecc.). Il punto e i numerosi provvedimenti sono riportati nell'apposito *focus* dedicato alla materia, (cfr. par. 14.6).

4.4.2. Comunicazioni di dati personali effettuate in maniera non conforme al RGPD

Visibilità nella intranet e comunicazione illecite di dati personali

Si ricordano, inoltre, episodi in cui è stata censurata la condotta dell'amministrazione per illecita comunicazione di dati personali. Al riguardo, va menzionato il caso della pubblicazione, nella rete intranet di un'azienda ospedaliera, accessibile a tutti i dipendenti tramite *username* e *password,* di dati e informazioni personali di altri dipendenti (provv. 14 gennaio 2021, n. 22, doc. web n. 9543138, cfr. 4.4.1).

Parimenti, va richiamato anche il provvedimento di ammonimento, in violazione del principio di minimizzazione dei dati, nei confronti di un comune che, nell'ambito di un procedimento di accesso agli atti, aveva notificato alla società controinteressata l'istanza di accesso trasmettendo il documento di riconoscimento del reclamante mentre la disciplina di settore prevede sia inviata al controinteressato la mera istanza di accesso (provv. 27 maggio 2021, n. 259, doc. web n. 9690937).

4.4.3. L'accesso civico

In materia di diritto di accesso civico e protezione dei dati personali il Garante ha adottato numerosi pareri nei confronti di Responsabili della prevenzione della corruzione (Rpct) e di difensori civici ai sensi dell'art. 5, commi 7 e 8, d.lgs. n. 33/2013.

Carenza di motivazione

In alcune occasioni l'Autorità ha chiesto all'amministrazione di motivare meglio il provvedimento di riscontro dell'accesso, in quanto il richiamo al limite concernente la protezione dei dati personali era generico o inconferente (cfr. provv.ti 13 maggio 2021, n. 200, doc. web n. 9678035; 6 maggio 2021, n. 184, doc. web n. 9740778).

Documenti inseriti in procedimenti civili

Si menziona altresì il caso in cui è stato evidenziato che i motivi ostativi all'accoglimento dell'accesso civico riguardavano la circostanza che i documenti richiesti erano "inseriti in procedimenti civili" che potevano essere sottratti all'accesso civico ai sensi dell'art. 76 delle disposizioni per l'attuazione del codice di procedura civile e disposizioni transitorie, nonché delle linee guida dell'Anac in materia di accesso civico. Di conseguenza, per tali profili, il Garante ha rinviato ad osservazioni contenute in precedenti pareri dell'Autorità (provv. 31 marzo 2021, n. 121, doc. web n. 9697887).

In altri casi, il Garante ha fornito pareri 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. Ciò con particolare riferimento a:

Dati di studenti relativi all'emergenza sanitaria

- dati relativi all'emergenza sanitaria detenuti da istituti scolastici (numero settimanale, da inizio della raccolta, diviso per singolo circolo/scuola e singolo plesso: degli alunni positivi in isolamento, in quarantena e sottoposti a tampone; di casi in attesa di esito; di classi in isolamento o quarantena e di classi focolaio). Al riguardo, è stato osservato che i dati riferiti a persone fisiche, identificate o identificabili, che hanno contratto il virus da Covid-19 rientrano nella definizione di dati sulla salute, i quali – come affermato in altri pareri – sono esclusi dall'accesso in virtù delle eccezioni assolute di cui all'art. 5-*bis,* comma 3, d.lgs. n. 33/2013. Inoltre, è stato osservato che le informazioni riferite a persone fisiche, identificate o identificabili, che – pur non essendo positive al Covid-19 – erano state sottoposte a tampone (molecolare o antigenico), o a quarantena oppure a isolamento erano in ogni caso di natura particolarmente delicata, essendo peraltro riferite nel caso in esame a soggetti minorenni. Peraltro, le informazioni che erano state richieste, anche se prive dell'indicazione del nome e del cognome degli alunni, contenevano dati di dettaglio che, "laddove combinati con informazioni verbali facilmente acquisibili soprattutto in realtà scolastiche contenute", potevano consentire di risalire all'identità dei soggetti coinvolti. Ciò anche considerando il ristretto ambito di riferimento, la variabilità del numero di casi (che settimanalmente potevano essere anche esigui), il particolare regime di pubblicità dei dati ricevuti tramite accesso civico e il raffronto dei dati richiesti con altre informazioni eventualmente in possesso di terzi (provv. 23 aprile 2021, n. 157, doc. web n. 9582723);

Registrazioni, verbali o relazioni

- registrazione audio della seduta dell'assemblea dei soci di una società a totale partecipazione pubblica, tenutasi in modalità telematica a causa delle normative anti contagio da Covid-19 (provv. 28 gennaio 2021, n. 21, doc. web n. 9565200);
- relazione riservata sull'attività di polizia locale, di cui era stata data lettura in una seduta non aperta al pubblico di un consiglio comunale ai sensi delle relative disposizioni statutarie (provv. 11 febbraio 2021, n. 58, doc. web n. 9567180);
- verbali delle riunioni del collegio dei revisori dei conti di un ente pubblico. Al riguardo, è stato evidenziato che l'amministrazione ha fornito al richiedente una motivazione contenente un mero e generico richiamo al diritto alla

riservatezza anche se intere parti dei documenti richiesti non contenevano dati personali. L'amministrazione è stata pertanto invitata a fornire una congrua motivazione nel provvedimento di riscontro all'istanza di accesso civico e a tener conto degli obblighi di pubblicazione concernenti i dati relativi ai controlli sull'organizzazione e sull'attività dell'amministrazione ai sensi dell'art. 31, d.lgs. n. 33/2013 (provv. 13 maggio 2021, n. 200, doc. web n. 9678035);

- pagine di un verbale di una seduta del consiglio di un ordine degli avvocati, relative alle richieste di spiegazioni al presidente del consiglio dell'ordine, da parte di alcuni iscritti, circa un'audizione effettuata dinnanzi a una commissione del Consiglio superiore della magistratura per la quale era stata disposta la riservatezza della discussione, generando ragionevoli aspettative di confidenzialità in capo ai partecipanti alla discussione delle questioni poste all'ordine del giorno (provv. 21 maggio 2021, n. 205, doc. web n. 9688057);

Dati di lavoratori

- provvedimenti del Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia con i quali è stata concessa la "mobilità esterna" a propri dipendenti. Al riguardo, è stato ritenuto corretto concedere un accesso civico parziale ai dati richiesti, scegliendo modalità meno pregiudizievoli per i diritti di riservatezza dei soggetti interessati, consentendo l'ostensione di una "tabella riepilogativa, contenente i dati sintetici per il periodo temporale richiesto", priva di dati personali (provv. 23 aprile 2021, n. 159, doc. web n. 9668095);
- atti e documenti acquisiti dal Mise in relazione alla domanda di iscrizione all'elenco da utilizzare per la procedura comparativa relativa al conferimento dell'incarico di segretario generale di camera di commercio. Al riguardo, è stata sollecitata una nuova valutazione sull'ostensione dei dati e delle informazioni personali contenuti nei documenti richiesti, supportata da congrua e coerente motivazione circa l'effettiva sussistenza del limite di cui all'art. 5-*bis,* comma 2, lett. *a*), d.lgs. n. 33/2013, che tenga conto della posizione ricoperta dal soggetto controinteressato e delle informazioni attualmente già oggetto di pubblicità a esso riferite (provv. 6 maggio 2021, n. 184, doc. web n. 9740778, cit.);
- documenti concernenti concorsi e nulla osta per la copertura di ruoli dirigenziali in una azienda sanitaria (provv. 10 giugno 2021, n. 238, doc. web n. 9681945);
- graduatorie dei dipendenti relative a progressioni economiche orizzontali, con dettaglio dei punteggi attribuiti (provv. 13 maggio 2021, n. 199, doc. web n. 9672790);

Partecipanti a procedure concorsuali

- dati e informazioni personali – di diversa natura e specie – riferiti ai 61 candidati ammessi alla prova preselettiva per un concorso pubblico presso una provincia, quali nome, cognome, indirizzo e posta elettronica. Al riguardo, è stato evidenziato che la disciplina di settore non prevede obblighi di pubblicità dei dati personali riferiti ai singoli partecipanti al concorso pubblico e che la generale conoscenza della partecipazione al concorso e la volontà di cambiare ruolo o amministrazione di appartenenza può determinare conseguenze sul piano relazionale e professionale dei partecipanti, producendo un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei soggetti controinteressati, non aderente alle relative ragionevoli aspettative di confidenzialità (provv. 10 giugno 2021, n. 237, doc. web n. 9681122);

Recupero crediti per danno erariale

- atti della p.a. adottati per il recupero del credito da parte dell'amministrazione a seguito di una sentenza della Corte dei conti di condanna per danno erariale nei confronti di un soggetto che aveva lavorato presso un ente pubblico, come previsto dall'art. 214, d.lgs. n. 174/2016 (provv. 28 ottobre 2021, n. 383, doc. web n. 9721510);

- fatture relative a pagamenti per alberghi, ristoranti o bar in occasione di soggiorni e spese di rappresentanza di una società in *house* del comune (provv. 22 gennaio 2021, n. 18, doc. web n. 9559967);

Fatture e pagamenti

- documentazione riguardante una procedura di condono edilizio contenente dati e informazioni personali di diversa specie e natura, riferiti agli atti compiuti dall'amministrazione (sopralluoghi, note e controdeduzioni, richiesta di pareri legali), alla proprietà dei soggetti controinteressati, a sanzioni amministrative comminate e poi annullate (provv. 18 agosto 2021, n. 305, doc. web n. 9717761);

Titoli edilizi

- copia integrale delle dichiarazioni reddituali riferite a quattro anni presentate da un soggetto al tempo titolare di un incarico di assessore provinciale detenute all'Agenzia delle entrate. Al riguardo non sono stati rinvenuti motivi per discostarsi dalle valutazioni effettuate dalla predetta Agenzia, che – ai sensi della normativa vigente e delle indicazioni contenute nelle linee guida dell'Anac – ha rigettato l'istanza di accesso civico alla copia integrale delle dichiarazioni dei redditi presentate dal contribuente e detenute ai fini di accertamento fiscale (provv. 15 ottobre 2021, n. 365, doc. web n. 9721245).

Dichiarazione dei redditi

4.5. *I trattamenti effettuati presso regioni ed enti locali*

4.5.1. L'accesso ai documenti amministrativi e l'accesso da parte dei consiglieri comunali

Continuano a pervenire richieste di parere, da parte di amministrazioni o di singoli cittadini, in materia di accesso ai documenti amministrativi. Al riguardo, è stato ribadito che la disciplina in materia di protezione dei dati personali fa salve le norme vigenti in materia di accesso ai documenti amministrativi, le quali attribuiscono all'interessato il diritto di prendere visione ed estrarre copia di tali documenti (artt. 59 e 60 del Codice, disposizione quest'ultima peraltro espressamente richiamata dall'art. 24, comma 7, l. n. 241/1990). Compete poi all'amministrazione destinataria della richiesta di accesso verificare, caso per caso, l'interesse e i motivi sottesi alla relativa istanza, nonché valutare la sussistenza di una delle ragioni per le quali l'accesso può essere differito o sottratto alla conoscibilità del richiedente, essendo la stessa in possesso di tutti i necessari elementi di ponderazione dell'istanza presentata.

Sono pervenute anche numerose richieste di parere, da parte delle amministrazioni, in materia di accesso agli atti da parte di consiglieri comunali ai sensi dall'art. 43, comma 3, d.lgs. n. 267/2000, con particolare riferimento alle richieste aventi ad oggetto le liste degli aventi diritto a buoni spesa o altre forme di retribuzione elargite per far fronte all'emergenza da Covid-19 o elenchi dei nominativi dei soggetti posti in quarantena o risultati positivi al Covid-19. Sul punto, è stato ribadito che è l'amministrazione destinataria dell'istanza a dover entrare nel merito della valutazione della richiesta nel rispetto dei principi di limitazione della finalità e di minimizzazione e, quando la richiesta di accesso riguarda particolari categorie di dati (art. 9 del RGPD) o dati relativi a condanne penali o a reati (art. 10 del RGPD), consentendo l'accesso alle sole informazioni indispensabili per lo svolgimento del mandato. L'Autorità ha rammentato che resta ferma la necessità, da parte del consigliere richiedente, di rispettare, in ogni caso, l'obbligo del segreto "nei casi specificamente determinati dalla legge", nonché i divieti di divulgazione dei dati personali (si pensi ad es. all'art. 2-*septies,* comma 8, del Codice, che vieta la diffusione dei dati idonei a rivelare lo stato di salute). Ne consegue che sono i consiglieri medesimi a rispondere dell'eventuale utilizzo delle informazioni, anche sul piano della disciplina in materia di protezione dei dati personali.

4

Numerose richieste di parere in materia di accesso agli atti da parte di consiglieri comunali ai sensi dall'art. 43, comma 3, d.lgs. 267/2000, avevano ad oggetto le richieste di accedere direttamente ai protocolli informatici delle amministrazioni mediante il rilascio di apposito *user id* informatico e *password* di servizio senza limitazione di uso, postazione, orari e modalità. Al riguardo, coerentemente a recenti pronunce giurisdizionali, è stato ribadito che il rilascio delle credenziali per l'accesso al protocollo informatico dell'ente, di fatto, consentirebbe ai consiglieri comunali di accedere alla generalità indiscriminata dei documenti dell'ente in mancanza di apposita istanza, comportando un monitoraggio assoluto e permanente sull'attività degli uffici, tale da violare la *ratio* dell'istituto, in quanto eccedente il perimetro delle prerogative attribuite ai consiglieri.

Registrazione seduta consiglio comunale mediante *body cam*

A seguito di un reclamo, è stato sanzionato un comune in relazione alla registrazione di una seduta del consiglio comunale mediante l'utilizzo di dispositivi video indossabili, cd. *body cam,* senza aver reso ai soggetti ripresi un'informativa sul trattamento dei dati personali (con riguardo alla pubblicazione da parte dello stesso comune, sul proprio sito web istituzionale di atti e documenti contenenti informazioni riguardanti il reclamante (cfr. par. 14.11) (provv. 11 novembre 2021, n. 399, doc. web n. 9725891).

4.5.2. Mobilità e trasporti

Utilizzo di *app*

A seguito di alcune notizie stampa l'Autorità ha appreso che in un comune di grande dimensione i permessi per l'accesso e la sosta nelle zone a traffico limitato (Ztl) da esporre sui veicoli, riportavano sul frontespizio un cd. QR *code,* che consente a chiunque, mediante l'utilizzo di una generica applicazione per dispositivi mobili, di accedere a dati personali relativi al titolare del permesso Ztl o al suo utilizzatore (es. nome e cognome, nel caso di persona fisica, del titolare del permesso, nome e cognome dell'utilizzatore del permesso, la categoria del richiedente, nonché la targa del veicolo autorizzato). L'Autorità ha, altresì, verificato che, modificando il valore del parametro denominato "Pid" (semplicemente incrementando o diminuendo l'identificativo numerico del permesso) all'interno dell'indirizzo web del servizio di verifica, era possibile visualizzare anche i dati personali relativi ad altri permessi Ztl, pur non avendo a disposizione il corrispondente QR *code.* Ciò accadeva in quanto il servizio *online* di verifica dei permessi Ztl risultava liberamente accessibile, non essendo protetto da alcuna procedura di autenticazione, comportando un'illecita diffusione dei dati da parte del titolare del trattamento, in violazione degli artt. 5 e 6 del RGPD e dell'art. 2-*ter* del Codice, e comprovando una mancata adozione di idonee misure di sicurezza ai sensi dell'art. 32 del RGPD in capo al titolare e al responsabile del trattamento.

Inoltre, il trattamento in esame risultava svolto da un soggetto, designato quale responsabile del trattamento dall'ente comunale titolare del trattamento. Tuttavia, nel corso dell'istruttoria è emerso che il predetto servizio di verifica dei permessi Ztl risultava erogato tramite risorse di rete (nomi a dominio e reti Ip) riferibili ad una terza società, che svolgeva un servizio di *hosting* per conto del responsabile del trattamento, i cui rapporti con gli altri soggetti coinvolti nel trattamento non erano stati regolati ai sensi dell'art. 28 del RGPD con conseguente violazione di tale disposizione normativa in capo al titolare del trattamento. Infatti l'Autorità ha avuto modo di chiarire che la fornitura del servizio di *hosting* implica in ogni caso il trattamento di dati personali (art. 4, par. 1, n. 1), del RGPD), effettuandone la registrazione e la conservazione, la cui trasmissione è implicita nell'uso dei protocolli di comunicazione telematica, quali l'indirizzo Ip del dispositivo utilizzato dall'utente, la data e l'ora della connessione e l'indirizzo Ip del *server* che ospitava il servizio in esame (provv.ti. 11 febbraio 2021, n.

48, doc. web n. 9562831 e n. 49, doc. web n. 9562852).

L'Autorità, inoltre, ha rilasciato su richiesta dalla Regione Lombardia un parere sullo schema di delibera della Giunta regionale che disciplina il trattamento dei dati personali connesso all'operatività della *mobile app* Sconto Carburante, di cui all'art. 8-*bis,* l.r. 20 dicembre 1999, n. 28. La *mobile app,* in particolare, è stata realizzata per erogare uno sconto sui rifornimenti di carburante presso gli impianti di distribuzione abilitati ai cittadini residenti in prossimità del territorio svizzero nonché per prevenire ed evitare frodi e abusi nella fruizione del beneficio da parte dell'utente e da parte dei gestori degli impianti di distribuzione carburante.

Nel corso delle interlocuzioni con la Regione l'Autorità è intervenuta al fine di assicurare, anche per ragioni di trasparenza, una descrizione più dettagliata della tipologia di dati oggetto di trattamento e delle condizioni di liceità dello stesso, l'individuazione dei vari soggetti coinvolti nel trattamento (regione, comuni, Aci, Agenzia delle entrate, Guardia di finanza), con la precisazione dei flussi di dati personali attivati tra gli stessi, nonché la descrizione della architettura e del ciclo funzionale dell'*app* in esame (parere 1° novembre 2021, n. 393, doc. web n. 9728140).

Regolazione delle soste e dei parcheggi

L'Autorità ha ricevuto diversi reclami e segnalazioni riguardanti la regolazione dei servizi di sosta e parcheggi comunali da parte di gestori di pubblici servizi.

In un caso, l'Autorità ha esaminato il trattamento dei dati personali contenuti nei cd. parcometri evoluti installati sul territorio di una grande città, accertando la mancanza di informativa agli interessati, la mancata designazione dei soggetti coinvolti quali responsabili del trattamento, la mancata definizione dei tempi di conservazione e la mancata adozione di idonee misure di sicurezza, in violazione degli artt. 5, 12, 13, 25, 28 e 32 del RGPD. Nei confronti del responsabile del trattamento e del sub-responsabile del trattamento, è stata accertata principalmente l'assenza della disciplina del rapporto tra il titolare e i responsabili del trattamento ai sensi dell'art. 28 del RGPD, richiesta quale condizione di liceità del trattamento in mancanza di indicazione di altri specifici presupposti che abbiano legittimato il trattamento dei dati personali. Sul punto è stato ribadito che gli eventuali contratti di servizio o altri atti interni (quali i bandi di gara) non soddisfano le caratteristiche dell'atto giuridico volto a regolamentare il rapporto con il responsabile, non contenendo gli elementi previsti dall'art. 28 del RGPD (provv.ti 22 luglio 2021, n. 293, doc. web n. 9698597 e n. 294, doc. web n. 9698724).

In un altro caso, l'Autorità ha appreso che, al fine di sottoscrivere l'abbonamento al servizio di "sosta autorizzata" nel territorio comunale, la cui gestione era stata affidata ad una società privata, veniva richiesta agli utenti, per accedere ad alcune agevolazioni, la compilazione di appositi moduli, contenenti dati eccedenti (ad es. contratto di affitto o possesso dell'immobile o in alternativa pagamento dell'ultima Tari), in violazione dell'art. 5 del RGPD. Dall'istruttoria è emersa, inoltre, l'assenza di nomina della società affidataria del servizio quale responsabile del trattamento, nonché il mancato conferimento, da parte del titolare del trattamento, dell'informativa agli interessati relativa al trattamento in esame, in violazione degli artt. 5, 12, 13, 25 e 28 del RGPD. Si è accertato, invece, nei confronti della società privata che gestisce il servizio, la violazione degli artt. 5 e 6 del RGPD, in quanto l'assenza della disciplina del rapporto tra il titolare e i responsabili del trattamento ai sensi dell'art. 28 del RGPD comporta che il trattamento è stato effettuato in assenza delle condizioni di liceità previste dal RGPD e dal Codice (provv. 29 settembre 2021, n. 351, doc. web n. 9716256).

Misure di sicurezza

A seguito di un reclamo l'Autorità ha verificato che una società aveva stipulato con un comune un contratto (regolando il rapporto anche ai sensi dell'art. 28 del RGPD) per l'affidamento del servizio di gestione delle violazioni al codice della strada nonché delle violazioni amministrative diverse dal codice della strada di competenza dell'ente,

4

inclusa l'attività di riscossione ordinaria e coattiva. A seguito di un reclamo, era emerso che fino ad una certa data ogni cittadino poteva accedere alle informazioni personali relative alle multe inserendo semplicemente un numero di verbale (a numerazione progressiva) e una data (coerente con la numerazione dei verbali) senza indicare la targa. Così facendo era possibile acquisire i dati personali degli interessati quali: la targa, l'ora in cui è stata rilevata l'infrazione, il tipo di infrazione, l'importo da pagare e la fotografia dell'automobile. Nel corso dell'istruttoria è emerso che, verosimilmente a causa di un aggiornamento del *software* fornito dalla società, l'inserimento del campo "targa" non era più obbligatorio per l'accesso ai dati dei verbali trattati nell'ambito del servizio di pagamento delle multe, a differenza di quanto precedentemente impostato e richiesto esplicitamente dal comune nel contratto. È stata pertanto accertata la mancata adozione, da parte della società, di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, in violazione degli artt. 5, par. 1, lett. *f*) e 32 del RGPD.

Utilizzo della Pec per la notifica delle contravvenzioni al codice della strada

L'Autorità ha ricevuto diversi reclami 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.

Come già precedentemente avvenuto, l'Autorità ha avviato un'attività di collaborazione con il Ministero dell'interno affinché venissero fornite ulteriori indicazioni, al fine di rendere le modalità di notifica via Pec delle contravvenzioni al codice della strada maggiormente compatibili con la disciplina in materia di protezione dei dati personali.

A seguito di questa interlocuzione, il Ministero dell'interno ha adottato la circolare del 17 novembre 2021 a mezzo della quale 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" (provv. 2 dicembre 2021, n. 419, doc. web n. 9733053).

Piattaforma unica nazionale dei Cude

L'Autorità è stata interpellata dal Ministero delle infrastrutture e della mobilità sostenibile al fine del rilascio del parere sullo schema di decreto che disciplina la Piattaforma unica nazionale informatica dei contrassegni per i disabili (Cude, Contrassegno unificato disabili europeo) – prevista l'art. 1, comma 489, della l. 30 dicembre 2018, n. 145 – istituita presso il predetto Ministero nell'ambito dell'archivio nazionale dei veicoli di cui all'art. 226, d.lgs. 30 aprile 1992, n. 285, per consentire la verifica delle targhe associate a permessi di circolazione dei titolari di contrassegni.

Al riguardo, con la partecipazione dell'Autorità, è stata individuata una soluzione tecnica per l'implementazione della Piattaforma che, in applicazione dei principi di minimizzazione dei dati e integrità e riservatezza (art. 5, par. 1, lett. *c*) ed *f*) e 32 del RGPD), prevede che non vengano acquisiti i dati identificativi dei titolari di Cude, ma un codice alfanumerico assegnato dal comune al titolare del contrassegno, utilizzato ai fini dell'associazione alla targa del veicolo. Pur prendendo favorevolmente atto di tale impostazione, nel parere rilasciato sullo schema di decreto l'Autorità ha chiesto che tale decreto fosse integrato da un documento che disciplini puntualmente tutti gli elementi richiesti dagli artt. 6, par. 3, e 9, par. 2, lett. *g*), del RGPD, nonché dall'art. 2-*sexies,* par. 1, del Codice, e in particolare contenga una descrizione sistematica dei trattamenti, dei flussi di dati, del ruolo e delle responsabilità degli attori nel trattamento dei dati (Mit, comuni, etc.), delle misure tecniche e organizzative implementate per garantire un livello di protezione adeguato ai rischi del trattamento, ai sensi degli artt. 5, par. 1, lett. *f*), 24, 25 e 32 del RGPD (provv. 15 aprile 2021, n. 143, doc. web n. 9590407).

4.5.3. Il trattamento di dati personali effettuati nell'ambito della gestione dell'emergenza epidemiologica da Covid-19

Anche nel 2021 sono pervenute numerose richieste di parere da parte delle amministrazioni nell'ambito della gestione delle attività necessarie a fronteggiare l'emergenza epidemiologica da Covid-19, nonché quesiti da parte dei singoli cittadini, in riscontro alle quali l'Autorità ha integrato le FAQ pubblicate nella sezione Covid-19 del sito istituzionale in particolare per quanto riguarda l'accesso dei consiglieri comunali ad elenchi di beneficiari di buoni o altri servizi.

Piattaforma per le domande di sussidi alimentari

L'Autorità ha avviato un'istruttoria nei confronti di un grande comune a seguito del reclamo di un cittadino che aveva lamentato che i dati personali, contenuti nella domanda di sussidi alimentari, presentata tramite una piattaforma informatica accessibile dal sito del comune, erano stati acquisiti da un soggetto non autorizzato, il quale li avrebbe utilizzati per finalità estranee a quelle di supporto all'utenza. Per assistere gli utenti nella compilazione, il comune si era avvalso di soggetti esterni (enti del terzo settore, sindacati e parrocchie, cd. OpT), che aveva accreditato ad usare la piattaforma informatica. L'istruttoria ha accertato che gli operatori di qualsiasi organizzazione accreditata potevano consultare tutte le pratiche inserite nella piattaforma e visualizzare i dati anagrafici e la fascia economica Isee dei richiedenti, senza che venissero registrate le operazioni di consultazione effettuate, con conseguente impossibilità di identificare gli utenti che avevano effettuato le predette consultazioni. Era stata rilasciata a ciascuna OpT un'unica utenza di accesso utilizzabile da tutti i propri addetti e qualunque operatore poteva così accedere ai dati di tutte le domande, anche presentate presso altri OpT. La funzione di ricerca dei beneficiari, inoltre, prevedeva l'inserimento dei soli primi tre caratteri del codice fiscale, rendendo così facilmente accessibili per un numero elevato di posizioni, le informazioni relative alla condizione di fragilità dei richiedenti i sussidi. Avendo, quindi accertato che la piattaforma era priva delle necessarie misure tecniche e organizzative tali da assicurare un'adeguata tutela dei diritti e delle libertà degli interessati, il comune è stato sanzionato per la violazione degli artt. 5, par. 1, lett. *f*), 25 e 32 del RGPD (provv. 15 aprile 2021, n. 140, doc. web n. 9587053).

4.6. *Il documento di indirizzo su designazione, posizione e compiti del Rpd in ambito pubblico*

All'esito di un'attività istruttoria per la trattazione di reclami, segnalazioni e quesiti, nonché per l'effettuazione di una specifica attività ispettiva nei confronti di società che forniscono il servizio di Rpd per enti pubblici e per un'indagine comparativa svolta con le autorità degli altri Paesi UE sotto forma di assistenza reciproca volontaria, il Garante ha adottato il 29 aprile 2021 il "Documento di indirizzo su designazione, posizione e compiti del Rpd in ambito pubblico" per fornire chiarimenti su numerosi profili concernenti il ruolo, la posizione e i compiti del Rpd in ambito pubblico e a suggerire misure per rafforzarne il ruolo nelle amministrazioni pubbliche (ove la designazione del Rpd è obbligatoria). Tra i profili oggetto di trattazione del documento si segnalano, in particolare: la valorizzazione del Rpd quale punto di contatto per l'Autorità presso l'ente; questioni concernenti l'obbligo di designazione; una serie di questioni concernenti la scelta di un Rpd esterno; la pubblicazione e la comunicazione all'Autorità dei dati di contatto del Rpd; il coinvolgimento da parte del titolare, lo svolgimento dei compiti da parte del Rpd e la costituzione di un *team* di collaboratori; vari aspetti concernenti l'incompatibilità con altri incarichi e il conflitto di interessi, sia con riferimento alla posizione

del Rpd interno che alla posizione del Rpd esterno (provv. 29 aprile 2021, n. 186, doc. web n. 9589104).

4.7. *Ordini professionali*

L'attività dell'Autorità relativa agli ordini professionali ha riguardato la trattazione di reclami relativi al mancato o inidoneo riscontro a richieste di esercizio dei diritti di cui agli artt. 15-22 del RGPD e alla diffusione di dati personali in assenza di un'idonea base giuridica.

In particolare, in due distinti casi, gli ordini professionali territoriali, in qualità di titolari del trattamento, avevano dato riscontro a richieste di esercizio del diritto di accesso a dati personali (art. 15 del RGPD) ben oltre il termine di un mese previsto dall'art. 12 del RGPD, senza, peraltro, aver informato gli interessati, entro il medesimo termine, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo o ricorso giurisdizionale, in violazione dell'art. 12, parr. 3 e 4, del RGPD. In una delle due decisioni, il Garante ha evidenziato come l'istanza formulata dall'interessato non potesse ritenersi "manifestamente infondata" (art. 12, par. 5, del RGPD), atteso che la normativa in materia di dati personali non richiede che l'interessato debba motivare la propria richiesta di accedere ai dati che lo riguardano, ben potendo il diritto di accesso essere esercitato anche con riguardo a dati personali che, come nel caso di specie, sono stati forniti al titolare del trattamento direttamente dall'interessato, il quale può avere, ad esempio, interesse a verificare che i propri dati siano esatti e aggiornati (provv.ti 15 aprile 2021, n. 141, doc. web n. 9673732; 16 settembre 2021, n. 320, doc. web n. 9704032).

In un altro caso, oltre ai medesimi profili relativi all'esercizio del diritto di accesso, l'Autorità, a seguito di un reclamo, ha affrontato il tema della liceità della diffusione *online* di dati personali. Nel caso di specie, un ordine degli avvocati territoriale aveva pubblicato sul proprio sito web istituzionale il contenuto di un messaggio di posta elettronica certificata, inviato dai reclamanti al consiglio dell'ordine e ai singoli colleghi consiglieri, contenente considerazioni personali degli autori della comunicazione. Al riguardo, il Garante ha ritenuto che il messaggio di posta elettronica in questione, pur avendo ad oggetto argomenti attinenti all'attività del consiglio dell'ordine, contenesse riflessioni e valutazioni critiche degli autori e che la decisione di inviare la stessa a tutti i consiglieri non fosse idonea ad incidere sulla qualificazione del contenuto della comunicazione, che si configurava, in ogni caso, come corrispondenza privata, sicuramente non destinata, nell'intenzione dei mittenti, a una diffusione, che è, pertanto, avvenuta in assenza di un'idonea base giuridica (cfr. artt. 5, par. 1, lett. *a*) e 6 del RGPD, nonché 2-*ter* del Codice, nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139) (provv. 5 aprile 2021, n. 146, doc. web n. 9674060).

Sempre con riguardo ai trattamenti effettuati dagli ordini professionali, il Garante ha espresso parere favorevole sullo schema di delibera del Consiglio nazionale forense (Cnf) recante la "determinazione delle specifiche tecniche del sistema informatico centrale adottato ai sensi e per gli effetti del decreto Ministero della giustizia 16 agosto 2016, n. 178", sul presupposto che le specifiche tecniche oggetto di parere tenessero adeguatamente conto delle indicazioni fornite dall'Ufficio nelle interlocuzioni avute con il Cnf, volte a garantire che le operazioni e le modalità di trattamento fossero descritte accuratamente, anche al fine di assicurare il rispetto del principio di liceità, correttezza e trasparenza (artt. 5, par. 1, lett. *a*), del RGPD), e che fossero adottate specifiche misure tecniche e organizzative idonee a garantire un livello di

sicurezza adeguato ai rischi presentati dal trattamento (artt. 5, par. 1, lett. *f*), 25 e 32, del RGPD) (provv. 10 giugno 2021, n. 233, doc. web n. 9681140).

4.8. *Digitalizzazione della p.a.*

Nel corso del 2021, il processo di digitalizzazione della p.a. ha ricevuto un impulso significativo, anche al fine di dare attuazione al Pnrr che l'Italia si è impegnata a realizzare nei confronti dell'Unione europea. In questo contesto il Garante ha esercitato la propria funzione consultiva in relazione agli interventi promossi dalle istituzioni governative.

4.8.1. Pareri al Ministro dell'innovazione tecnologica e della transizione digitale

Caratteristiche dello Spid

Il Garante ha rilasciato parere positivo sullo schema di decreto di modifica del d.P.C.M. 24 ottobre 2014 recante la definizione delle caratteristiche di Spid, proposto dal Ministro per l'innovazione tecnologica e la digitalizzazione, volto ad adeguare il testo alla normativa europea, incluso il regolamento (UE) 910/2014 (c.d. regolamento eIDAS), con particolare riferimento ai requisiti che i gestori dell'identità digitale devono possedere ai fini dell'accreditamento (provv. 15 aprile 2021, n. 135, doc. web n. 9590366).

Piattaforma per la notificazione atti p.a.

Il Garante ha reso parere favorevole sullo schema di d.P.C.M. (da adottare ai sensi dell'art. 26, comma 15, d.l. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla l. 11 settembre 2020, n. 120) in materia di piattaforma per la notificazione degli atti della p.a., attraverso la quale si intende, a fini di notificazione di atti, provvedimenti, avvisi e comunicazioni (in alternativa alle modalità previste da altre disposizioni di legge), consentire alle amministrazioni di rendere telematicamente disponibili i corrispondenti documenti informatici, che, a loro volta, il gestore della piattaforma renderà disponibili ai destinatari, mediante accesso personale o a mezzo delegati, per il reperimento, la consultazione e l'acquisizione degli stessi.

Il testo recepisce infatti le indicazioni fornite dall'Autorità con particolare riferimento a profili quali: la precisazione, da parte del mittente, se l'atto da notificare riguardi o meno l'attività imprenditoriale o professionale eventualmente svolta dal destinatario, nel rispetto del principio di limitazione della finalità del trattamento (art. 5, par. 1, lett. *b*), del RGPD); l'acquisizione, da parte del gestore, del domicilio digitale generale del destinatario solo ove necessario e con riferimento al domicilio disponibile al momento dell'invio, nel rispetto dei principi di minimizzazione dei dati, esattezza e *privacy by design* e *by default* (artt. 5, par. 1, lett. *c*) e *d*) e 25 del RGPD); la possibilità, per il destinatario, di monitorare in ogni tempo gli accessi operati per suo conto sulla piattaforma, quale ulteriore misura di garanzia nei confronti di possibili accessi non autorizzati; la ridefinizione del ruolo assunto, nel trattamento, dall'addetto al recapito postale e dal fornitore del servizio universale. È stata altresì prevista la consultazione del Garante sulla valutazione d'impatto redatta dal gestore, che deve individuare anche le misure tecniche e organizzative di dettaglio, non disciplinate nello schema di decreto, volte a mitigare i rischi elevati per i diritti e le libertà degli interessati, quali quelli relativi alla possibilità, per il destinatario, di delegare l'accesso a terzi, e quelli relativi alla definizione dell'ordine dei domicili digitali nei confronti dei quali effettuare le notificazioni (provv. 14 ottobre 2021, n. 369, doc. web n. 9716841).

4.8.2. Pareri all'AgID

Dati statistici relativi ai servizi erogati dai gestori Pec

Il Garante si è pronunciato favorevolmente sullo schema di linee guida per la normalizzazione dei dati statistici relativi ai servizi erogati dai gestori Pec, conservazione e fornitori di servizi fiduciari qualificati, redatte dall'AgID e riguardanti la trasmissione all'Agenzia medesima di informazioni che non includono dati personali relativi agli utenti dei predetti servizi, ma esclusivamente dati aggregati relativi alla fornitura degli stessi da parte dei singoli soggetti accreditati (provv. 27 gennaio 2021, n. 24, doc. web n. 9544069).

Interoperabilità tecnica delle p.a.

Il Garante ha espresso parere favorevole, su richiesta dell'AgID, sugli schemi delle linee guida sull'interoperabilità tecnica delle p.a. che, in particolare, individuano le tecnologie e gli standard che le p.a. devono tenere in considerazione durante la realizzazione dei propri sistemi informatici (contribuendo alla definizione del modello di interoperabilità della p.a. per assicurare lo scambio di dati tra le amministrazioni e tra queste e i soggetti privati) e delle linee guida tecnologie e standard per la sicurezza dell'interoperabilità tramite Api dei sistemi informatici (di cui all'art. 73, comma 3-*ter,* lett. *b*), d.lgs. 7 marzo 2005, n. 82).

I testi definiscono un quadro di garanzie e di misure volte ad assicurare l'integrità e la riservatezza dei dati oggetto di comunicazione nelle interazioni tra i sistemi informatici coinvolti nel processo di interoperabilità, nonché a soddisfare esigenze di *privacy by design* e *by default* (artt. 5, par., 1, lett. *f*), 25 e 32, del RGPD). Il parere evidenzia però che i flussi di dati personali dovranno comunque trovare un legittimo fondamento in una base giuridica idonea ai sensi della disciplina in materia di protezione dei dati personali e corredata delle adeguate garanzie a tutela dei diritti e delle libertà degli interessati tra soggetti che rivestono ruoli conformi a quanto stabilito dal RGPD (provv. 8 luglio 2021, n. 260, doc. web n. 9682994).

Indice nazionale dei domicili digitali delle persone fisiche

Altro parere richiesto dall'AgID concerne le linee guida dell'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese (cd. Inad), cioè l'elenco pubblico dei domicili digitali eletti da persone fisiche, professionisti che svolgono una professione non organizzata in ordini, albi o collegi ed enti di diritto privato, sulla base del combinato disposto di cui agli artt. 3-*bis,* 6-*quater* e 6-*quinquies,* d.lgs. 7 marzo 2005, n. 82.

Al riguardo, il Garante ha preliminarmente rilevato profili di criticità nel quadro normativo primario, con riferimento alle disposizioni che prevedono il riversamento automatico, all'interno dell'Inad, dei domicili digitali dei professionisti presenti nell'Ini-Pec e l'estensione delle finalità per le quali è possibile utilizzare i domicili digitali liberamente consultabili dall'Inad. Peraltro, è stata evidenziata anche la necessità di effettuare una riflessione più generale sul rapporto tra Inad e Anpr.

Ciò posto, il Garante, pur dando atto di alcune indicazioni accolte dall'AgID sulla base delle interlocuzioni avute con l'Autorità, ha formulato all'Agenzia una serie di condizioni e osservazioni in relazione ad alcune criticità. Esse hanno riguardato, tra l'altro, la necessità di: individuare misure volte a mitigare l'impatto negativo della scelta legislativa di eleggere automaticamente presso l'Inad il domicilio digitale dei professionisti già presente nell'Ini-Pec, nonché a informare adeguatamente gli interessati e a prevedere la cancellazione del domicilio digitale acquisito da Ini-Pec nel momento in cui il professionista, adeguatamene informato, abbia eletto un domicilio *ad hoc* per l'Inad; consentire la cessazione volontaria del domicilio digitale iscritto nell'Inad; eliminare il codice fiscale tra il *set* di dati forniti a seguito di consultazione; adottare misure di sicurezza idonee a rilevare e impedire che p.a., gestori di servizi pubblici e società a controllo pubblico possano procedere ad eventuali duplicazioni, anche parziali, della banca dati costituita presso l'Inad; valutare la sussistenza di

un'effettiva base giuridica che legittimi il trattamento di dati personali connesso alle finalità di verifica sull'esistenza, e sullo stato degli indirizzi Pec e sull'esistenza, sullo stato e sulla titolarità dell'indirizzo elettronico eletto presso un servizio elettronico di recapito certificato qualificato, nonché definire le correlate specifiche tecniche e misure di sicurezza tecniche e organizzative (provv. 22 luglio 2021, n. 288, doc. web n. 9690742).

Punto di accesso telematico delle p.a.

Il Garante ha espresso parere favorevole, sullo schema, presentato da AgID, di linee guida per accesso telematico ai servizi della p.a. (di cui all'art. 64-*bis,* d.lgs. 7 marzo 2005, n. 82), che riguarda un canale complementare agli altri canali digitali già utilizzati dai soggetti erogatori (p.a., gestori di servizi pubblici e società a controllo pubblico) per rendere disponibili agli utenti i propri servizi, per la cui progettazione, sviluppo, gestione e implementazione la Presidenza del Consiglio dei ministri si avvale di PagoPA spa (ai sensi dell'art. 8, commi 2 e 3, d.l. 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla l. 11 febbraio 2019, n. 12).

Lo schema ha tenuto conto delle indicazioni dell'Autorità, che hanno in particolare riguardato: la definizione dei ruoli assunti nel trattamento dai soggetti coinvolti, a partire dal gestore e dai soggetti erogatori, nonché le relative responsabilità nella valutazione dei rischi; la descrizione delle attività di trattamento poste in essere nel punto di accesso telematico; le modalità di adesione al punto di accesso telematico da parte dei soggetti erogatori, definendo anche i contenuti degli accordi di adesione; le garanzie da adottare in caso di trattamenti delle tipologie di dati personali di cui agli artt. 9 e 10 del RGPD; le misure volte ad assicurare un livello di sicurezza adeguato ai rischi, con particolare riguardo al tracciamento delle interazioni con le altre piattaforme, nonché degli accessi e delle operazioni compiute dai soggetti autorizzati; le modalità di integrazione del punto di accesso telematico con altre piattaforme digitali.

Nel parere, il Garante, ha tuttavia rilevato che l'analisi delle ulteriori misure volte a mitigare i rischi elevati presentati dal trattamento dovrà essere effettuata nell'ambito della valutazione di impatto sulla protezione dei dati, da sottoporre al suo esame. Inoltre, è stato evidenziato che, con riferimento alla possibilità di ricorrere ai responsabili del trattamento stabiliti in Paesi terzi, l'esportatore sarà tenuto a verificare se la legge o la prassi del Paese terzo permettono alle autorità pubbliche locali ingerenze nei diritti delle persone interessate che vadano oltre quanto strettamente necessario per conseguire l'obiettivo legittimo perseguito e non esista contro tali ingerenze una tutela giuridica efficace, e, in tale caso, dovrà adottare misure supplementari che garantiscano un livello di protezione dei dati personali sostanzialmente equivalente a quello previsto dal RGPD (provv. 1° novembre 2021, n. 394, doc. web n. 9714315).

Piattaforma digitale nazionale dati

Il Garante ha pronunciato parere favorevole sulle linee guida sull'infrastruttura tecnologica della Piattaforma digitale nazionale dati per l'interoperabilità dei sistemi informativi e delle basi di dati, in relazione alla Piattaforma digitale nazionale dati (Pdnd) (di cui all'art. 50-*ter,* d.lgs. 7 marzo 2005, n. 82), presentate da AgID. La Pdnd è l'infrastruttura tecnologica per l'interoperabilità dei sistemi informativi e delle basi di dati, finalizzata a favorire l'accesso, da parte dei soggetti legittimati in conformità alla normativa vigente, alle informazioni detenute da p.a., gestori di servizi pubblici e società a controllo pubblico.

Sono state accolte nel testo le indicazioni fornite dall'Autorità riguardanti, in particolare: l'individuazione delle attività in relazione alle quali il gestore agisce come titolare del trattamento per le attività necessarie all'implementazione e alla gestione dell'infrastruttura interoperabilità Pdnd, specificandone le relative responsabilità; la messa a disposizione degli aderenti di strumenti di gestione delle richieste di fruizione di cui sono parte; la necessità che i meccanismi di gestione, utilizzo e

aggiornamento degli attributi certificati, dichiarati e verificati, siano realizzati nel rispetto dei principi di liceità, trasparenza e correttezza del trattamento, di esattezza, di integrità e riservatezza e di *privacy by design* e *by default* (artt. 5, par. 1, lett. *a*), *d*), *f*) e 25 del RGPD); l'implementazione di meccanismi di informazione tempestiva tra il gestore e gli aderenti interessati in caso di violazioni di sicurezza o di qualsiasi minaccia che, nell'ambito del complessivo utilizzo della Pdnd, comporti un rischio per la sicurezza e per i diritti e le libertà degli interessati (artt. 5, par. 1, lett. *f*), 33 e 34, del RGPD).

Il Garante ha altresì precisato che p.a., gestori di servizi pubblici e società a controllo pubblico possono continuare a utilizzare anche i sistemi di interoperabilità già previsti dalla legislazione vigente, per i quali, sentito il Garante, sono state previste misure volte ad assicurare l'integrità e la riservatezza dei dati trattati nell'ambito del patrimonio informativo pubblico, ed ha stabilito che il gestore dovrà redigere e sottoporre al Garante la valutazione d'impatto sulla protezione dei dati, con l'indicazione delle ulteriori misure necessarie ad assicurare la conformità del complesso dei trattamenti effettuati attraverso l'infrastruttura interoperabilità Pdnd (provv. 16 dicembre 2021, n. 433, doc. web n. 9732758).

Servizi *cloud*

L'AgID ha altresì sottoposto al Garante lo schema di regolamento (di cui all'art. 33-*septies,* d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221, e come ulteriormente modificato dall'art. 7, comma 3, d.l. 6 novembre 2021, n. 152) concernente la definizione dei livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la p.a. e delle caratteristiche di qualità, di sicurezza, di *performance* e scalabilità, portabilità dei servizi *cloud* per la p.a., delle modalità di migrazione, nonché delle modalità di qualificazione dei servizi *cloud* per la pubblica amministrazione.

Il Garante, dopo aver rilevato che lo schema di regolamento non tiene in adeguata considerazione i profili di protezione dei dati personali, ha pronunciato parere favorevole, a condizione che: la classificazione dei dati e dei servizi digitali delle amministrazioni tenga conto dei rischi per i diritti e le libertà delle persone fisiche allorché ci si trovi in presenza di trattamenti di dati personali; sia coinvolto il Garante nell'elaborazione dei modelli e criteri previsti; i livelli minimi di base di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità delle infrastrutture per la p.a. e le caratteristiche di base di qualità, di sicurezza, di *performance* e di scalabilità, di interoperabilità, di portabilità dei servizi *cloud* per la p.a. siano conformi ai principi e alle regole stabiliti dalla disciplina in materia di protezione dei dati personali; infine, il processo di migrazione dei dati e dei servizi digitali verso le infrastrutture digitali dedicate o i servizi *cloud* dotati dei requisiti necessari, preveda l'individuazione dei soggetti coinvolti e i ruoli e le responsabilità da costoro assunti sul piano della protezione dei dati personali, nonché, nel caso che tale migrazione coinvolga fornitori o subfornitori stabiliti fuori dallo Spazio economico europeo (See), assicuri il rispetto degli artt. 44 e ss. del RGPD in relazione al trasferimento di dati personali verso Paesi terzi, alla luce della cd. sent. Schrems II della Corte di giustizia dell'UE e delle raccomandazioni del Comitato europeo per la protezione dei dati (provv. 16 dicembre 2021, n. 449, doc. web n. 9740711).

*4.8.3. Provvedimenti correttivi sull'*app *IO*

Nelle more dell'adozione delle citate linee guida dell'AgID di cui all'art. 64-*bis,* d.lgs. 7 marzo 2005, n. 82, a seguito di alcuni approfondimenti istruttori condotti dall'Autorità sull'*app* IO quale punto di accesso telematico ai servizi della p.a., sono emerse alcune gravi criticità con particolare riguardo alle interazioni di tale applicazione con i servizi di Google, Mixpanel e Instabug, società stabilite negli Stati

Uniti, responsabili del trattamento di PagoPA spa che si avvalgono anche di sistemi informatici ivi ubicati e di ulteriori fornitori anch'essi stabiliti in Paesi terzi. Tali criticità riguardano: l'effettuazione di un tracciamento, mediante l'utilizzo delle librerie di Mixpanel in particolare, che consente di ricondurre, a soggetti determinati identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso dei diversi servizi offerti all'interno dell'*app* IO, senza che peraltro siano chiare le finalità dei trattamenti effettuati e senza che l'utente sia adeguatamente informato e possa esprimere con piena consapevolezza il consenso di cui all'art. 122 del Codice; la sistematica raccolta e i successivi trattamenti di tali informazioni, aventi carattere estremamente personale e riferite a milioni di interessati, sui sistemi di Mixpanel, in violazione dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati e integrità e riservatezza; la mancata adozione di garanzie adeguate ai sensi degli artt. 44 e ss. del RGPD con riferimento al ricorso ai servizi offerti da Google, Mixpanel e Instabug, che a loro volta si avvalgono di numerosi fornitori stabiliti fuori dall'UE, che comporta il trasferimento dei dati verso Paesi terzi; l'attivazione, per impostazione predefinita, di tutti i servizi disponibili all'interno dell'*app* IO, con connessa abilitazione automatica della ricezione di notifiche *push* e di inoltro via *e-mail,* comportando per gli utenti l'impossibilità di scegliere gli enti e i servizi per i quali ricevere le predette notifiche e i messaggi in modalità *opt-in,* in violazione dei principi di proporzionalità e di *privacy by design* e *by default.*

Sulla base di tali accertamenti, e considerata la necessità di intervenire urgentemente, il Garante con un provvedimento correttivo in via d'urgenza, in particolare, ha ingiunto a PagoPA: la limitazione provvisoria dei trattamenti effettuati mediante l'*app* IO che prevedono l'interazione con i servizi di Google (consentendo esclusivamente i trattamenti necessari all'invio di notifiche *push* agli utenti dell'*app* IO che hanno esplicitamente e liberamente attivato tale funzionalità per taluni servizi) e di Mixpanel (sospendendo l'archiviazione dei dati sui dispositivi degli utenti, l'accesso a tali dati e la raccolta degli stessi sui sistemi di Mixpanel, nonché interrompendo ogni altro ulteriore trattamento dei dati già inviati a Mixpanel effettuato, anche da parte di altri soggetti, per finalità diverse dalla mera conservazione degli stessi); l'adozione di misure tecniche e organizzative necessarie a modificare le modalità di attivazione dei servizi disponibili all'interno dell'*app* IO e delle relative funzionalità di notifica *push* e di inoltro via *e-mail* dei messaggi, garantendo a tutti gli interessati la possibilità di una scelta libera, esplicita e specifica in relazione a ciascun servizio o ai servizi offerti da uno determinato ente (modalità *opt-in*), nonché ad assicurare le medesime garanzie nei confronti di coloro per i quali, essendo già utenti dell'*app* IO, sono stati attivati automaticamente servizi non richiesti in modo libero, esplicito e specifico (provv. 9 giugno 2021, n. 230, doc. web n. 9668051).

Nei giorni immediatamente successivi PagoPA ha fornito le indicazioni circa le iniziative adottate per porre rimedio ai rilievi formulati dall'Autorità e ottemperare tempestivamente, introducendo adeguate misure a garanzia dei diritti e delle libertà degli interessati volte a mitigare i rischi che caratterizzano i trattamenti in esame e a conformarli al RGPD e al Codice. Il Garante ha preso atto di tali rassicurazioni e ha adottato un nuovo provvedimento con il quale ha dichiarato il venire meno dei presupposti alla base della disposta limitazione provvisoria dei trattamenti di dati personali, ferma restando la limitazione provvisoria relativa ai dati raccolti e archiviati da Mixpanel prima dell'introduzione delle misure stesse (che non possono essere oggetto di trattamenti ulteriori rispetto alla mera conservazione, da garantire fino al termine dell'istruttoria in corso) (provv. 16 giugno 2021, n. 242, doc. web n. 9670061).

4.8.4. Altri provvedimenti correttivi

A seguito della sottrazione di un *hard disk* esterno contenente dati personali di dipendenti, fornitori e collaboratori esterni, il Garante ha comminato una sanzione da 8.000 euro a un'azienda regionale per la protezione ambientale per violazione degli artt. 5, par. 1, lett. *f*) e 32 del RGPD, in quanto il titolare non aveva adottato misure tecniche e organizzative adeguate per assicurare la protezione da trattamenti non autorizzati o illeciti o dalla perdita, e per garantire un livello di sicurezza adeguato al rischio, quali: accorgimenti necessari a consentire la continuità, su base permanente, e il ripristino della disponibilità dei dati personali sottratti; tecniche in grado di assicurare la non identificabilità degli interessati ai quali i dati personali contenuti nel dispositivo si riferivano (come la pseudonimizzazione o la cifratura dei dati); procedure idonee a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (provv. 14 gennaio 2021, n. 5, doc. web n. 9538748).

4.9. *Trasferimenti di dati personali verso Paesi terzi sulla base di accordi e attività di supervisione sul VIS*

Sono pervenute diverse richieste, da parte di Ministeri e altre istituzioni pubbliche, sulla conformità al RGPD di accordi con Paesi terzi che prevedano trasferimenti di dati personali.

Al riguardo, l'Autorità ha precisato che, sulla base dell'art. 46 del RGPD, in assenza di una decisione di adeguatezza adottata dalla Commissione europea ai sensi dell'art. 45, par. 3, il trasferimento è consentito solo in presenza di garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Tali garanzie possono essere previste da uno strumento giuridicamente vincolante e avente efficacia esecutiva tra organismi pubblici (art. 46, par. 2, lett. *a*), del RGPD) o, previa autorizzazione dell'autorità di controllo competente, da disposizioni da inserire in accordi amministrativi tra organismi pubblici (art. 46, par. 3, lett. *b*), del RGPD), quali ad esempio i protocolli d'intesa.

In tali occasioni, l'Autorità ha richiamato le linee guida 2/2020 sull'art. 46, par. 2, lett. *a*), e par. 3, lett. *b*), del RGPD, per i trasferimenti di dati personali tra autorità ed organismi pubblici del See e di Paesi non appartenenti al See, adottate dal Comitato europeo per la protezione dei dati, che forniscono indicazioni circa le garanzie che, anche in accoglimento degli orientamenti espressi dalla Corte di giustizia dell'UE, devono essere poste in essere attraverso uno strumento giuridicamente vincolante. Inoltre, è stato sottolineato che, ai fini del rilascio dell'autorizzazione sugli accordi amministrativi, ai sensi dell'art. 46, par. 4, l'autorità di controllo applica il meccanismo di coerenza di cui all'art. 63 del RGPD. L'Autorità ha, inoltre, aggiunto che, in assenza di una decisione di adeguatezza da parte della Commissione europea e di misure adeguate ai sensi dell'art. 46 del RGPD, alcuni trasferimenti internazionali di dati possano aver luogo in via residuale e solo a determinate condizioni (specificatamente individuate per ogni singola situazione), nell'ambito delle cd. deroghe previse dall'art. 49. Tra queste, per i casi in questione, quella relativa ai trasferimenti necessari per importanti motivi di interesse pubblico riconosciuti dal diritto dell'Unione o dal diritto dello Stato membro a cui è soggetto il titolare del trattamento, anche nello spirito di reciprocità della cooperazione internazionale, che però non può essere utilizzata in caso di trasferimenti di dati sistematici e su larga scala (come già previsto nelle linee guida 2/2018 sulle deroghe di cui all'art. 49 del RGPD).

Inoltre, nell'ambito di specifiche interlocuzioni con il Ministero degli affari esteri e della cooperazione internazionale è stato anche condiviso un modello di clausole per il trasferimento dei dati personali, che contiene le garanzie a tutela degli interessati promosse dalle richiamate linee guida 2/2020 del Comitato, da adattare e allegare agli accordi internazionali che l'Italia stipulerà in applicazione dell'art. 46, par. 2, lett. *a*), del RGPD (cfr. par. 23.1).

4.9.1. Casi specifici

Con riferimento ad un accordo internazionale, ai sensi dell'art. 46, par. 2, lett. *a*), del RGPD, tra Repubblica italiana e Repubblica di Moldavia per il trasferimento di dati personali relativi alla sicurezza sociale tra i rispettivi istituti previdenziali, l'Autorità, pur in assenza di poteri autorizzatori formali nel caso di specie, ha accolto con favore le misure condivise tra le due Istituzioni, nonché, più in generale, l'intenzione espressa dal Rpd del Ministero di mettere a punto un modello mutuabile anche ad altre analoghe situazioni, pur tenendo conto delle peculiarità di ciascun caso e restando comunque fermi possibili ulteriori margini di perfezionamento (nota 7 maggio 2021).

A seguito di una richiesta pervenuta dal Ministero delle infrastrutture e della mobilità sostenibili, relativamente ad un accordo di reciprocità con l'Ucraina in materia di conversione di patenti di guida (sempre ai sensi dell'art. 46, par. 2, lett. *a*), del RGPD), l'Autorità ha ritenuto necessario che la bozza fosse integrata con la previsione di adeguate garanzie in materia di protezione dei dati personali, eventualmente inserendole in un apposito allegato, la cui vincolatività fosse assicurata da apposita norma di rinvio, invitando, inoltre, il predetto Ministero a valutare il ricorso al già richiamato modello di clausole, da declinare secondo le specifiche esigenze connesse ai trattamenti di dati personali effettuati nel caso concreto (nota 9 giugno 2021).

In un altro caso il Ministero della difesa ha chiesto il parere su un accordo di cooperazione bilaterale nel settore della difesa tra il Governo della Repubblica Italiana e quello della Georgia, che prevede attività di cooperazione per le quali, in sede di attuazione, si potrebbe rendere necessario il trasferimento di dati personali dei dipendenti del Ministero della difesa coinvolti in programmi di attività (quali, per es. formazione e addestramento, operazioni umanitarie e di sostegno alla pace, cooperazione militare-civile, attività sociali, culturali e sportive). Gli elementi di dettaglio relativi alle modalità operative di esecuzione delle singole attività nelle quali si esplicherà la cooperazione internazionale saranno definite dalle parti mediante la sigla di ulteriori intese tecniche (*Technical Agreements* (TA) o *Executive Arrangements* (EA). Anche in tale occasione, trattandosi di un accordo ai sensi dell'art. 46, par. 2, lett. *a*), del RGPD, il Ministero è stato invitato a valutare il ricorso alle predette clausole, da adattare alle specifiche esigenze poste dalle attività di cooperazione (nota 13 agosto 2021).

Anche in un altro caso sottoposto dal Ministero degli affari esteri e della cooperazione internazionale, relativo ad una ipotesi di accordo per le adozioni internazionali con la Repubblica democratica del Congo, considerata la natura vincolante dell'accordo da stipulare, non essendo prevista un'autorizzazione specifica da parte dell'Autorità, è stato specificato che le garanzie previste dall'art. 46, par. 2, lett. *a*), del RGPD potranno essere inserite direttamente nel testo dell'accordo, oppure, in un allegato espressamente vincolante. Nel caso in esame è stato preso atto positivamente della scelta di utilizzare, quale base di partenza, il modello di clausole redatto all'esito delle interlocuzioni con l'Autorità, da declinare opportunamente, secondo le specifiche esigenze e peculiarità connesse ai trattamenti di dati personali effettuati nel caso concreto delle adozioni internazionali del Congo (nota 10 novembre 2021).

4

In risposta ad una richiesta della Presidenza del Consiglio dei ministri, relativa ad un modello tipo di "Intesa/Dichiarazione o Lettera di Intenti/*Memorandum* di collaborazione tra la Regione/Provincia Autonoma italiana e l'Ente omologo straniero", sulla base del quale la Regione Marche intendeva sottoscrivere un accordo con una Municipalità dell'Ecuador, per la promozione e l'innovazione nella produzione di cappelli, è stato evidenziato che, qualora le attività di trasferimento di dati personali necessarie a tal fine (quali, ad es. occasionali trasferimenti di dati personali previsti in caso di organizzazione di convegni, fiere, scambi) non abbiano ad oggetto scambi sistematici e su larga scala di dati personali, si sarebbe potuto utilmente tener conto delle indicazioni delle linee guida dell'EDPB 2/2018 sopra citate, potendo trovare applicazione l'ipotesi di deroga prevista dall'art. 49, par. 1, lett. *d*), del RGPD ("il trasferimento sia necessario per importanti motivi di interesse pubblico"). In caso contrario, trattandosi di un accordo amministrativo, sarebbe stato necessario acquisire l'autorizzazione dell'Autorità ai sensi dell'art. 46, par. 3, lett. *b*), del RGPD, previa applicazione del meccanismo di coerenza (art. 63 del RGPD), che prevede la notifica al Comitato europeo per la protezione dei dati (EDPB) e – ove il Protocollo medesimo venisse considerato come "questione di applicazione generale" o suscettibile di produrre effetti in più Paesi membri – anche il parere da parte di quest'ultimo ai sensi dell'art. 64, par. 2, del RGPD (nota 15 luglio 2021).

Similmente l'Autorità si è pronunciata su richiesta dell'Agenzia per la promozione all'estero e l'internazionalizzazione delle imprese italiane (Ice) in ordine a un *Memorandum of Understanding* di reciproco sostegno, da negoziare con l'omologo *Russian Export Center,* ai sensi dell'art. 46, par. 3, lett. *b*), del RGPD (nota 26 ottobre 2021).

Un altro caso ha riguardato una richiesta del Ministero dell'interno in merito ad una clausola in materia di protezione dei dati personali inserita nello schema di Convenzione di sovvenzione fondo asilo, migrazione e integrazione (Fami), da sottoscrivere con Unhcr, in relazione ai trasferimenti di dati personali relativi ad una proposta progettuale in materia di asilo e di reinsediamento di cittadini di Paesi terzi, da co-finanziare con risorse del Fami. In tale occasione – richiamato il quadro normativo sopra accennato – il Ministero è stato invitato anche a valutare il ricorso alle ipotesi di deroga, e in particolare a quella per importanti motivi di interesse pubblico (art. 49, par. 1, lett. *d*), ricordando che l'esistenza di un accordo o di una convenzione internazionale che stabilisca un determinato obiettivo, da favorire con la cooperazione internazionale, può essere un indicatore ai fini della valutazione dell'esistenza di un interesse pubblico, purché l'Unione europea o gli Stati membri abbiano sottoscritto tale accordo o convenzione, rinviando per la valutazione di tali presupposti alle linee guida del Comitato 2/2018 sopra citate (nota 26 luglio 2021).

4.9.2. L'attività di supervisione sul VIS

Ha avuto luogo dal 12 al 17 settembre la quarta valutazione Schengen dell'Italia relativa al settore della protezione dei dati. Il Gruppo di valutazione, formato da esperti designati dalle autorità di protezione dati di Paesi Schengen e dalla Commissione europea, ha verificato il grado di attuazione delle disposizioni europee sul sistema informativo Schengen (SIS-II) e sul sistema informativo visti (VIS), entrambi oggetto della supervisione del Garante (v. al riguardo parr. 8.5.1 e 23.1).

4.10. *La materia anagrafica e elettorale*

Il voto elettronico dei Comites

Il Garante ha espresso parere favorevole sullo schema di decreto del Ministero degli affari esteri e della cooperazione internazionale relativo alla sperimentazione del voto elettronico in occasione del rinnovo dei Comitati degli italiani all'estero 2021. La sperimentazione, su base volontaria, non produttiva di effetti giuridici, riguarderà l'elezione di un campione di 11 Comitati, con una campagna informativa effettuata dagli uffici consolari finalizzata ad acquisire elementi per un'analisi tecnico-informativa sulla percorribilità futura del voto elettronico e a valutare compiutamente se il sistema informatico a tal fine predisposto garantisca il rispetto dei principi di personalità, eguaglianza, libertà e segretezza del voto previsti dall'art. 48 della Costituzione.

Nonostante il recepimento delle diverse indicazioni fornite nel corso di precedenti interlocuzioni, il Garante ha, tuttavia, evidenziato alcune criticità che all'esito del completamento della fase sperimentale dovrebbero essere tenuti nella massima considerazione ai fini dell'analisi tecnico-organizzativa del voto elettronico, con riguardo sia alle modalità di comunicazione all'elettore del *validation number* (con specifico riferimento ai rischi connessi al suo invio per posta elettronica sia all'uso di dispositivi elettronici personali (pc, *smartphone, tablet*) o postazioni condivise (*internet point*), che non possono, a priori, garantire idonei livelli di sicurezza, né assicurare un utilizzo esclusivo da parte del votante. Con riguardo alla necessità di identificare in modo certo l'elettore e di garantire, allo stesso tempo, la segretezza del voto, è stato richiesto, in sede di sperimentazione, che vengano considerate tutte le possibili forme di tracciamento del processo di voto dell'elettore presenti nei sistemi informativi coinvolti nonché l'eventualità di re-identificazione di un interessato anche attraverso informazioni apparentemente anonime (cd. *single-out*) in caso, ad esempio, di voto espresso in determinate fasce orarie o da determinate località. Analoga valutazione è stata richiesta con riguardo all'invio all'elettore di un'attestazione elettronica dell'avvenuto voto, in relazione alle garanzie necessarie ad evitare che il *timing* dell'invio/ricezione del messaggio non sia utile a re-identificare il votante mediante l'associazione con il *timing* del voto espresso. Infine, in merito all'utilizzo dello Spid, è stato evidenziato che la tracciatura dei servizi acceduti – che i gestori dell'identità digitale (cd. *provider* Spid) sono tenuti ad effettuare ai sensi dell'art. 4, comma 2, d.P.C.M. 24 ottobre 2014 (cd. regole tecniche Spid) – potrebbe costituire un pregiudizio per gli interessati in quanto rende possibile per l'*identity provider* rilevare chi ha esercitato il voto in determinate tornate elettorali (provv. 19 novembre 2021, n. 405, doc. web n. 9721434).

Rilascio certificati Anpr *online*

Il Ministero dell'interno, d'intesa con il Ministro per l'innovazione tecnologica e la transizione digitale e il Ministro per la pubblica amministrazione, ha richiesto il parere sullo schema di decreto concernente le modalità di erogazione da parte dell'Anagrafe nazionale della popolazione residente (Anpr) dei servizi telematici per il rilascio di certificazioni anagrafiche *online* e per la presentazione *online* delle dichiarazioni anagrafiche relative al trasferimento di residenza da altro comune o dall'estero, alla costituzione di nuova famiglia o convivenza, ovvero mutamenti nella composizione della famiglia o al cambiamento di abitazione, di cui all'art. 13, d.P.R. 30 maggio 1989, n. 223.

Tale decreto ha previsto che il rilascio dei certificati anagrafici degli iscritti nell'Anpr, riguardanti il richiedente e i componenti della propria famiglia anagrafica, è assicurato in modalità telematica attraverso il sito web di Anpr, previa autenticazione, ai sensi degli artt. 64 e 64-*bis* del Cad, con una un'integrazione con la piattaforma PagoPA, di cui all'art. 5, comma 2, del Cad, per il pagamento dell'imposta di

bollo ai fini dell'emissione del certificato. Lo schema di decreto sul quale il Garante ha espresso parere favorevole, ha tenuto conto delle indicazioni fornite dall'Ufficio, nel corso delle interlocuzioni informali con il Ministero dell'interno, tra le quali, una più chiara definizione del perimetro soggettivo dei certificati che possono essere rilasciati al soggetto richiedente; le modalità di messa a disposizione e/o trasmissione del certificato, su richiesta dell'interessato, anziché in automatico, nell'area riservata sulla piattaforma Anpr, tramite il punto di accesso telematico di cui all'articolo 64-*bis* del Cad, al domicilio digitale o agli indirizzi disponibili nel profilo utente sulla piattaforma Anpr; la definizione dei ruoli e dei rapporti intercorrenti tra il Ministero dell'interno, la Sogei spa e PagoPA spa, ai sensi dell'art. 28 del RGPD; le modalità di utilizzo del punto di accesso telematico di cui all'art. 64-*bis* del Cad, per quanto riguarda la richiesta dei certificati, il loro rilascio e conservazione, con particolare riguardo alle caratteristiche dell'adesione dell'interessato ai servizi dell'*app* IO; la necessità di aggiornare la valutazione d'impatto sulla protezione dei dati relativa ai servizi offerti da Anpr, includendovi l'analisi del servizio in esame (provv. 14 ottobre 2021, n 367, doc. web n. 9717543).

Modifiche alle modalità emissione della Cie per i minori

L'Autorità si è inoltre pronunciata su uno schema di decreto sulla modifica delle modalità tecniche di emissione della Carta d'identità elettronica (Cie), presentato dal Ministero dell'interno, volta a ripristinare, nelle disposizioni individuanti i soggetti legittimati alla richiesta e le informazioni di dettaglio contenute nella Cie, l'espressione genitori in sostituzione di quelle di padre e madre (v. parere 31 ottobre 2018, doc. web n. 9058965).

La corretta rappresentazione del ruolo svolto, rispetto al minore, dal soggetto richiedente l'emissione della Cie è, infatti, funzionale non soltanto all'osservanza del principio di esattezza nel trattamento dei dati e al diritto all'identità del minore stesso, quanto anche al corretto svolgimento delle procedure per il suo espatrio anche sulla base di quanto previsto dal codice delle frontiere Schengen di cui al regolamento UE 2016/399.

Nel parere l'Autorità ha ritenuto il riferimento proposto dallo schema di decreto, alla nozione di genitore conforme al principio di esattezza nel trattamento dei dati personali e alla corretta rappresentazione del ruolo del richiedente la carta d'identità. Tuttavia, per i casi nei quali i soggetti richiedenti siano effettivamente il padre e la madre, ha ritenuto opportuno, proprio in base al principio europeo di esattezza, che sia mantenuta la vigente dizione, di padre affiancandola a quella di genitore, utilizzabile nelle ipotesi nelle quali i richiedenti siano soggetti altrimenti esercenti la responsabilità genitoriale (provv. 25 marzo 2021, n. 160, doc. web n. 9677947).

4.11. *Videosorveglianza in ambito pubblico*

Il trattamento di dati personali mediante sistemi di videosorveglianza da parte di soggetti pubblici è generalmente ammesso se necessario ad adempiere un obbligo legale al quale è soggetto il titolare del trattamento o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, parr. 1, lett. *c*), *e*) e 3, del RGPD, nonché 2-*ter* del Codice; cfr. par. 41 delle linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29 gennaio 2020 dal Cepd; v. anche le FAQ del Garante in materia di videosorveglianza, doc. web n. 9496574).

In tale quadro, il Garante si è occupato del caso di un istituto di formazione, che aveva installato alcune telecamere di videosorveglianza in un convitto annesso all'istituto, trattando dati personali relativi agli studenti, in gran parte minorenni,

per generiche esigenze di sicurezza e di controllo. Il sistema di videosorveglianza consentiva di riprendere non solo le porte di accesso al convitto e le aree esterne, ma anche spazi comuni all'interno dell'edificio, quali corridoi e atrii, nei quali vi è una maggiore aspettativa di riservatezza, in quanto si svolge la vita di relazione dei minori, che può essere compromessa e alterata dalla percezione di essere costantemente monitorati tramite telecamere. Quest'ultime erano, peraltro, attive anche nelle ore notturne, durante le quali può diminuire la soglia di consapevolezza e aumentare lo stato di vulnerabilità dei minori (cfr. cons. 38 e 75 del RGPD; v. anche Gruppo Art. 29, parere 2/2009 sulla protezione dei dati personali dei minori, adottato l'11 febbraio 2009, WP 160). Non essendo emersi dall'istruttoria significativi elementi – quali la particolare situazione di disagio e degrado del contesto sociale in cui opera l'istituto o la sussistenza di precedenti episodi di particolare gravità – tali da giustificare la sottoposizione di minorenni a siffatte forme invasive di controllo, il Garante ha ritenuto che il trattamento sia avvenuto in violazione degli artt. 5, par. 1, lett. *a*) e *c*) e 6 del RGPD (provv. 25 febbraio 2021, n. 74, doc. web n. 9710177).

In un altro caso, uno degli ospiti di un istituto per ciechi aveva lamentato che le telecamere interne inquadravano anche il corridoio che collega i loro alloggi con le docce comuni. Le riprese non solo erano registrate, ma erano mostrate in tempo reale sui *monitor* degli operatori della portineria, con il rischio che venissero accidentalmente visualizzate anche da visitatori o fornitori. Nel provvedimento sanzionatorio, il Garante ha sottolineato come la scelta di installare l'impianto di videosorveglianza nel corridoio che conduce alle docce fosse lesiva della sfera personale degli ospiti e non potesse ritenersi giustificata da generiche esigenze di sicurezza, che avrebbero potuto comunque essere soddisfatte dall'istituto con modalità meno invasive per gli ospiti. L'Autorità, nel rilevare che l'istituto non aveva informato correttamente i residenti sulla presenza delle telecamere, ha ordinato allo stesso di rendere disponibile agli ospiti l'informativa completa sul trattamento dei dati personali anche in formato audio (provv. 16 settembre 2021, n. 327, doc. web n. 9705650; cfr. *Newsletter* 6 ottobre 2021, n. 482, doc. web n. 9705786).

5 La sanità

5.1. *Il trattamento dei dati personali effettuato nell'ambito dell'emergenza sanitaria*

Il trattamento dei dati personali effettuato nell'ambito dell'emergenza sanitaria è stato al centro degli interventi del Garante nel settore sanitario, anche con la partecipazione a tavoli di lavoro nazionali con le altre amministrazioni deputate ad attuare e individuare gli strumenti idonei a fronteggiare la pandemia (in particolare con il Ministero della salute e la struttura del Commissario straordinario per l'emergenza) e tramite l'espressione di numerosi pareri sugli schemi delle disposizioni normative volte a contenere il diffondersi del virus Covid-19. Molteplici sono stati anche i procedimenti istruttori in ordine alle centinaia di segnalazioni e reclami pervenuti in relazione al trattamento dei dati sulla salute effettuati nel contesto emergenziale, alcuni dei quali sono stati conclusi con provvedimenti sanzionatori nei confronti del titolare del trattamento. Tra i provvedimenti adottati dal Garante merita evidenziare quelli relativi alla comunicazione agli enti preposti dei risultati dei tamponi positivi al Covid-19 senza l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio di perdita, modifica, divulgazione non autorizzata (art. 32 del RGPD). In tali istruttorie, il trattamento dei dati personali volto all'attuazione agli atti normativi adottati in relazione allo stato di emergenza deliberato dal Consiglio dei ministri in data 31 gennaio 2020, non ha rispettato i principi di cui all'art. 5 del RGPD, come quello di liceità, integrità e riservatezza dei dati, non derogati dalla disciplina emergenziale.

In particolare, in uno dei casi esaminati, un laboratorio di analisi aveva inviato ad una Asl una *e-mail* allegando, oltre ai risultati positivi del test sierologico per Covid-19 del paziente effettuato presso la stessa azienda, anche i referti positivi di 31 pazienti assistiti presso altre aziende sanitarie (provv. 13 maggio 2021, n. 202, doc. web n. n. 9678535). In un altro caso, una Asl aveva inviato l'elenco delle persone risultate positive al comune di residenza delle stesse utilizzando un indirizzo *e-mail* generico accessibile da tutti i dipendenti comunali, in luogo di quello dedicato a tali comunicazioni, rendendo così conoscibile l'elenco dei positivi a molti più dipendenti comunali di quelli autorizzati a trattare tali informazioni (provv. 13 maggio 2021, n. 208, doc. web n. 9685865).

Numerose istruttorie hanno riguardato la vulnerabilità dei portali che le regioni e le Asl hanno realizzato per offrire servizi legati alla gestione dell'emergenza sanitaria. In particolare, l'Autorità ha sanzionato un'agenzia per la tutela della salute regionale in relazione alle modalità con le quali era stato configurato il portale regionale dedicato a offrire servizi ai soggetti affetti dal Covid-19. Attraverso tale portale era infatti possibile conoscere se un cittadino dell'area metropolitana fosse, o fosse stato, positivo al Covid-19, semplicemente inserendo il codice fiscale e il numero di telefono mobile in un apposito campo (provv. 13 maggio 2021, n. 268, doc. web n. 9685332). I sistemi di monitoraggio utilizzati dall'agenzia consentivano di rilevare accessi non autorizzati solo a posteriori, risultando così inadeguati a impedire la verifica puntuale dello stato di positività (attuale o pregresso) di un soggetto. L'Autorità ha inoltre ritenuto che il trattamento censurato rientrasse tra quelli per i quali il titolare è tenuto ad effettuare, "prima di procedere al trattamento, una valutazione

dell'impatto dei trattamenti previsti sulla protezione dei dati personali" (art. 35 del RGPD). Ciò, in quanto ricorrevano certamente due dei criteri indicati dal Cepd per individuare i casi in cui un trattamento debba formare oggetto di una valutazione di impatto: trattamento di "dati sensibili o aventi carattere altamente personale" e di "dati relativi ad interessati vulnerabili", tra i quali si annoverano le persone affette da patologie.

Analoghe valutazioni sono state espresse in sede di interlocuzioni informali, a carattere d'urgenza, con numerose regioni in merito alla realizzazione di portali volti a offrire servizi sanitari digitali ai soggetti affetti da Covid-19 o a quelli posti in quarantena.

Molte istruttorie hanno riguardato anche i trattamenti effettuati per le attività di *contact tracing*. Con il provvedimento 11 novembre 2021, n. 400 (doc. web n. 9726426), l'Autorità è intervenuta sui trattamenti effettuati per ricostruire la filiera dei contatti stretti del contagiato in ambito scolastico. In particolare, un dipartimento di prevenzione di una Asl aveva chiesto di ricevere, da tutti i plessi scolastici di ogni ordine e grado della provincia, gli elenchi del personale ivi operante e degli studenti ivi iscritti, al fine di "ottimizzare le azioni di contenimento del contagio". Al riguardo, il Garante ha ricordato che la normativa allo stato vigente in materia di sorveglianza sanitaria, pur prevedendo che l'operatore di sanità pubblica, al fine di determinare le misure di contenimento del contagio più opportune, sia chiamato a ricostruire la filiera dei contatti stretti del soggetto risultato positivo al Covid-19 (art. 3, comma 6, d.P.C.M. 8 marzo 2020; circolare 22 febbraio 2020, n. 5443 del Ministero della salute e ss.mm.ii.; d.P.C.M. 13 ottobre 2020; circolari 29 maggio 2020, 18 giugno 2020, 31 gennaio 2021 e 6 maggio 2021 del Ministero della salute) non consente la raccolta preventiva dei dati dei soggetti eventualmente coinvolti nelle attività di *contact tracing*. Il Garante ha ricordato poi che anche le indicazioni del Ministero della salute prevedono la raccolta di informazioni relative ai contatti stretti del contagiato solo successivamente all'individuazione del caso confermato Covid-19. In considerazione del fatto che l'attività di *contact tracing* si fonda proprio sulla necessità di ricostruire la filiera dei reali contatti stretti del soggetto contagiato, il Garante ha rilevato che una raccolta preventiva dei dati dei soggetti appartenenti alla comunità scolastica non garantirebbe di individuare quelli che sono realmente venuti a contatto stretto con il soggetto positivo in un determinato periodo (si pensi ad es. alle eventuali assenze del personale scolastico o degli alunni o a possibili contatti stretti in ambiente scolastico con persone non precedentemente censite).

L'attività di collaborazione avviata con il Ministero della salute nel 2020 in merito all'*app* nazionale di *contact tracing* denominata Immuni è proseguita anche nel corso del 2021 attraverso il parere reso sullo schema di decreto che ha modificato la disciplina di settore prevedendo le funzionalità necessarie per consentire lo "sblocco dell'*app* Immuni in autonomia da parte del paziente", ovvero il caricamento delle chiavi (TEK) direttamente dal dispositivo mobile del soggetto risultato positivo su cui è installata l'*app* Immuni (provv. 25 febbraio 2020, n. 66, doc. web n. 9561715).

5.1.1. Il trattamento dei dati personali nell'ambito della campagna vaccinale

Sin dalle fasi iniziali della campagna vaccinale, l'Autorità è stata coinvolta dagli organi di governo centrale (Ministero della salute e Struttura commissariale per l'emergenza sanitaria) e da quelli locali (regioni e province autonome) chiamati a darle attuazione.

Nel mese di gennaio 2021 il Garante ha reso il proprio parere sullo schema di norma che si propone di disciplinare i sistemi informativi funzionali all'implementazione del piano strategico dei vaccini per la prevenzione delle infezioni da Sars-

5

CoV-2. In particolare, la disposizione dava attuazione al piano strategico per la somministrazione dei vaccini anti Covid-19, istituendo una piattaforma informativa nazionale idonea a svolgere una funzione di supplenza nell'eventualità che il sistema informativo vaccinale di una regione o di una provincia autonoma non risultasse adeguato a gestire i volumi di dati relativi alle richieste di vaccinazione (operazioni di prenotazione, registrazione delle somministrazioni, certificazione delle stesse, trasmissione dei dati al Ministero della salute). L'intervento dell'Autorità ha assicurato che la piattaforma raccogliesse, per le finalità di definizione dei fabbisogni delle dosi vaccinali, solo i dati relativi alle vaccinazioni in forma aggregata. È stato inoltre richiesto che, qualora la piattaforma operi in sussidiarietà per conto di una regione o provincia autonoma, il Commissario straordinario, a cui è affidata la gestione della piattaforma, fosse designato da queste ultime quale responsabile del trattamento ai sensi dell'art. 28 del RGPD. È stato altresì specificato di nominare responsabile del trattamento anche la società a partecipazione pubblica (Poste spa), di cui si avvale il Commissario straordinario. La disposizione su cui è stato reso il parere del Garante ha anche aggiornato la disciplina dei trattamenti di dati personali effettuati dal Ministero con l'Anagrafe nazionale vaccini (Avn), in relazione alle peculiarità della vaccinazione contro il Covid-19 (provv. 13 gennaio 2021, n. 1, doc. web n. 9563463).

L'Autorità è intervenuta sui trattamenti di dati personali necessari a estendere le attività di prenotazione e somministrazione delle vaccinazioni anti Covid-19 alle farmacie territoriali, ai medici convenzionati con il Ssn e a altri operatori sanitari, attraverso la piattaforma nazionale vaccini. Nello stesso parere è stato inoltre esaminato il ruolo del Sistema tessera sanitaria (Sistema TS) nell'assicurare la circolarità delle informazioni necessarie a consentire la vaccinazione degli assistiti nell'intero territorio nazionale, l'univocità delle prenotazioni e l'appropriatezza della somministrazione delle dosi successive alla prima. Le interlocuzioni con il Mef e con il Ministero della salute sono state incentrate in particolare sulla titolarità dei predetti trattamenti di dati personali. Più in dettaglio, sono stati espressamente distinti i trattamenti effettuati dal Mef, in qualità di responsabile del trattamento del Ministero della salute, da quelli effettuati dal Mef in qualità di titolare del trattamento. Nel primo caso, il Mef, attraverso il Sistema TS, acquisisce i dati relativi alle prenotazioni e alle somministrazioni vaccinali dall'Avn, al fine di fornire i previsti servizi di notifica delle prenotazioni multiple alle regioni o province autonome diverse da quella di assistenza, nonché di verifica dell'appropriatezza delle somministrazioni vaccinali. Il Mef opera, invece, in qualità di titolare del trattamento con riferimento ai trattamenti necessari ad assicurare i servizi di identificazione e autenticazione informatica degli operatori sanitari per l'accesso alle piattaforme regionali e alla piattaforma nazionale vaccini mediante l'utilizzo delle credenziali di accesso al Sistema TS e di interrogazione dei dati anagrafici dell'assistito fuori regione di assistenza (provv. 13 maggio 2021, n. 187, doc. web n. 9674151).

A seguito dell'attuazione della predetta piattaforma nazionale vaccini, l'Autorità ha avviato numerose istruttorie volte a garantire che le regioni e le province autonome che non intendessero avvalersene realizzassero sistemi informativi autonomi in grado di assicurare un pari livello di protezione dei dati personali degli interessati. In relazione alle diverse istruttorie sono stati resi chiarimenti alla Conferenza delle regioni e delle province autonome con particolare riguardo al consenso al trattamento dati nell'ambito della campagna di prevenzione e vaccinazione e alle modalità di accesso ai portali regionali dedicati alla prenotazione dei vaccini (nota 19 maggio 2021). In particolare, si è ravvisata l'opportunità di rappresentare alle regioni e province autonome, per il tramite della Conferenza, la necessità che le stesse configurino i propri sistemi informativi, dedicati alla prenotazione delle vaccinazioni

per il Covid-19, prevedendo che in fase di autenticazione l'interessato inserisca, in aggiunta al proprio codice fiscale, anche il numero di tessera sanitaria. Ciò, attesa la facilità di reperire in rete il codice fiscale di un interessato o di generarlo attraverso l'uso di comuni *software,* consente di minimizzare il rischio di permettere la prenotazione della vaccinazione per il Covid-19 all'insaputa dell'interessato, con evidente pregiudizio per l'ordinato svolgimento delle operazioni vaccinali e per l'interessato medesimo, in caso di mancata presentazione all'appuntamento prenotato. È stato evidenziato poi che l'uso del codice fiscale come unico elemento di accesso ai sistemi di prenotazione del vaccino rende il sistema informativo regionale più vulnerabile nei confronti di attacchi informatici volti a effettuare prenotazioni fraudolente in modo massivo. Al riguardo, l'Autorità ha ritenuto che l'onere in capo all'interessato di inserire in fase di prenotazione un dato ulteriore rispetto al codice fiscale appare ampiamente bilanciato rispetto ai rischi di non corretta identificazione dello stesso e di prenotazione di una dose vaccinale che non sarà poi utilizzata. È stato altresì chiarito che non deve essere richiesto il consenso dell'interessato al trattamento dei dati personali effettuato nell'ambito dell'esecuzione dei test Covid-19 o della prenotazione e somministrazione del vaccino, ricordando che, in virtù del principio di trasparenza, i titolari del trattamento devono invece informare l'interessato sui principali elementi del trattamento (art. 13 del RGPD e art. 17-*bis,* comma 5, d.l. n. 18/2020).

Allo scopo di agevolare le regioni e le province autonome ad attuare il piano strategico vaccini, il Garante ha adottato un decalogo sul trattamento dei dati personali connesso alle iniziative volte a promuovere il completamento della vaccinazione dei soggetti appartenenti alle categorie eleggibili (22 luglio 2021, doc. web n. 9688966).

In tale atto, il Garante ha ricordato che il trattamento dei dati personali finalizzato a promuovere l'offerta attiva del vaccino assistiti debba essere effettuato nel rispetto del diritto a non essere vaccinato anche dei soggetti non vaccinabili per motivi di salute ed ha proposto una soluzione operativa che veda coinvolti solo soggetti operanti nell'ambito del Ssn che hanno in cura l'interessato, in luogo di enti amministrativi operanti sul territorio (ad es. comuni). Il Garante ha poi richiesto che siano utilizzati i sistemi informativi regionali cui sono collegati i medici di medicina generale per l'accesso all'Avn, senza la creazione di nuove banche dati o di duplicazione di banche dati già esistenti. È stato inoltre richiesto di favorire soluzioni che prevedano che il medico di medicina generale possa rivolgere l'invito alla vaccinazione ai propri assistiti utilizzando l'indirizzo di posta ordinaria o elettronica o il numero di telefonia mobile detenuto dallo stesso, fornendo agli interessati elementi informativi essenziali sulle caratteristiche del trattamento e limitando il trattamento dei dati degli interessati alla realizzazione della campagna di sensibilizzazione. L'Autorità ha poi escluso la possibilità di raccogliere la motivazione della mancata vaccinazione e richiesto l'adozione di misure tecniche ed organizzative adeguate a mitigare il rischio di trattamenti non autorizzati o illeciti e di perdita o distruzione dei dati.

5.1.2. Il trattamento dei dati personali nell'ambito delle certificazioni verdi digitali

Il trattamento dei dati personali effettuato attraverso l'uso di certificazioni volte ad attestare lo stato vaccinale di un individuo al fine di poter usufruire di beni e servizi o di esercitare diritti e libertà fondamentali è stato al centro dell'attività dell'Autorità che è intervenuta in materia con pareri, provvedimenti e audizioni al Parlamento.

Il Garante ha espresso un avvertimento formale nei confronti di tutti i soggetti coinvolti nel trattamento e, in particolare, dei Ministeri della salute, dell'interno, dell'innovazione tecnologica e della transizione digitale e dell'economia e delle fi-

5

nanze, degli affari regionali e la Conferenza delle regioni o delle province autonome circa il fatto che i trattamenti di dati personali effettuati in attuazione delle disposizioni di cui al d.l. 22 aprile 2021, n. 52, potevano violare le disposizioni del RGPD di cui agli artt. 5, 6, par. 3, lett. *b*), 9, 13, 14, 25 e 32 (provv. 23 aprile 2021, n. 156, doc. web n. 9578184).

Il Garante ha osservato, in particolare, che il cd. decreto riaperture non garantiva una base normativa idonea per l'introduzione e l'utilizzo dei certificati verdi su scala nazionale, ed era gravemente incompleto in materia di protezione dei dati personali in quanto privo di una valutazione dei possibili rischi su larga scala per i diritti e le libertà personali. In contrasto con quanto previsto dal RGPD, il decreto non definiva con precisione le finalità per il trattamento dei dati sulla salute degli italiani, lasciando spazio a molteplici e imprevedibili utilizzi futuri, in potenziale disallineamento anche con analoghe iniziative europee. Non veniva inoltre specificata la titolarità dei trattamenti dei dati, in violazione del principio di trasparenza, rendendo così difficile se non impossibile l'esercizio dei diritti degli interessati.

Le disposizioni legislative successivamente adottate hanno parzialmente superato tali criticità, definendo in particolare la titolarità del trattamento effettuato attraverso la piattaforma nazionale-DGC (*Digital Green Certificate*) in capo al Ministero della salute (art. 42, d.l. n. 77/2021 e d.P.C.M. 17 giugno 2021), su cui il Garante ha reso il proprio parere il 9 giugno 2021, n. 229 (doc. web n. 9668064). In particolare, in tale parere il Garante ha preso atto che sono stati definiti i rapporti con il Mef e le società coinvolte nel trattamento ai sensi dell'art. 28 del RGPD, nonché individuati i soggetti che trattano le informazioni nell'ambito dell'emissione delle certificazioni verdi, quelli che possono accedervi e quelli deputati a controllare la validità e l'autenticità delle stesse. Il decreto ha inoltre definito tempi di conservazione dei dati trattati attraverso la piattaforma nazionale-DGC e le misure di sicurezza adottate dal Ministero della salute sulla base della valutazione di impatto sulla protezione dei dati effettuata ai sensi dell'art. 35 del RGPD.

Il parere è stato reso tenendo conto che il decreto ha previsto che l'*app* Verifica C19, individuata dal Ministero della salute quale strumento di controllo a disposizione del verificatore, consente infatti di rilevare esclusivamente l'autenticità, la validità e l'integrità della certificazione e di conoscere le generalità dell'interessato a cui la stessa si riferisce, senza rendere visibili le informazioni che ne hanno determinato l'emissione. Il soggetto deputato al controllo non viene, quindi, a conoscenza della condizione (vaccinazione, guarigione, esito negativo di un test Covid-19) alla base della quale è stata emessa la certificazione, né può conoscere la data di cessazione della validità della stessa. Sono stati inoltre definiti i ruoli dei soggetti verificatori e le modalità di esercizio dei diritti. Particolare attenzione è stata resa all'individuazione degli strumenti digitali per la messa a disposizione agli interessati delle certificazioni verdi Covid-19, con riferimento alle quali sono state evidenziate specifiche criticità in merito all'utilizzo dell'*app* IO, poi superate con successivo parere del 17 giugno 2021, n. 243 (doc. web n. 9670670).

L'Autorità ha poi reso il parere su una versione aggiornata del predetto decreto attuativo della disciplina sulle certificazioni verdi resasi necessaria, in vista dell'avvio del nuovo anno scolastico, per introdurre modalità semplificate di verifica delle stesse per il personale scolastico (provv. 31 agosto 2021, n. 306, doc. web n. 9694010). Il decreto ha recepito le indicazioni fornite dal Garante nell'ambito delle interlocuzioni informali con i rappresentati dei Ministeri dell'istruzione e della salute. In particolare, le istituzioni scolastiche, in qualità di datori di lavoro, si limitano a verificare – attraverso il Sistema informativo dell'istruzione Sidi e la piattaforma nazionale-DGC – il mero possesso della certificazione verde Covid-19 da parte del

personale effettivamente in servizio, trattando esclusivamente i dati a ciò necessari. I soggetti tenuti alle verifiche potranno raccogliere solo i dati strettamente necessari all'applicazione delle misure previste in caso di mancato rispetto degli obblighi sul possesso delle certificazioni verdi (ad es. assenza ingiustificata, sospensione del rapporto di lavoro e del pagamento dello stipendio).

Particolare attenzione è stata posta anche sulle misure di sicurezza. I soggetti tenuti ai controlli potranno accedere, in modo selettivo, ai soli dati del personale in servizio presso le istituzioni scolastiche di propria competenza. Per evitare eventuali abusi, le operazioni di verifica del possesso delle certificazioni Covid-19 da parte dei soggetti tenuti ai controlli sono registrate in appositi *log* (conservati per dodici mesi), senza però conservare traccia dell'esito delle verifiche.

È stato inoltre previsto che la valutazione di impatto, effettuata dal Ministero della salute, relativa ai trattamenti connessi all'emissione e alla verifica delle certificazioni verdi Covid-19, fosse integrata e aggiornata tenendo conto degli specifici scenari di rischio legati ai dati sanitari di circa un milione di lavoratori della scuola, prestando particolare attenzione alle possibili conseguenze discriminatorie, anche indirette, nel contesto lavorativo.

Nel mese di ottobre l'Autorità è tornata a esprimersi su una versione ulteriormente aggiornata del d.P.C.M. sulle certificazioni verdi del 17 giugno 2021 (provv. 11 ottobre 2021, n. 363, doc. web n. 9707431). Il testo tiene conto delle interlocuzioni con il Garante assicurando, in particolare, che l'attività di verifica del possesso delle certificazioni verdi Covid-19 possa essere effettuata anche attraverso modalità alternative all'*app* Verifica C19, quali l'impiego di un pacchetto di sviluppo per applicazioni (SDK), rilasciato dal Ministero con licenza *open source,* da integrare nei sistemi di controllo degli accessi ovvero, per i datori di lavoro pubblici e privati, mediante l'utilizzo di una specifica funzionalità della piattaforma NoiPA o del portale istituzionale Inps. È stato inoltre previsto per le p.a. con più di mille dipendenti un servizio di interoperabilità applicativa con la piattaforma nazionale-DGC. L'intervento del Garante ha assicurato che l'attività di verifica non comporti la raccolta di dati dell'interessato in qualunque forma, ad eccezione di quelli strettamente necessari, in ambito lavorativo, all'applicazione delle misure derivanti dal mancato possesso della certificazione. Il sistema utilizzato per la verifica del *green pass* non deve infatti conservare il QR *code* delle certificazioni verdi sottoposte a verifica, né estrarre, consultare registrare o comunque trattare per altre finalità le informazioni rilevate.

Per quanto riguarda la verifica mediante la piattaforma (per le p.a. aderenti), il portale dell'Inps (per i datori di lavoro con più di 50 dipendenti non aderenti a NoiPA) o mediante interoperabilità applicativa, la piattaforma nazionale- DGC consentirà di visualizzare la sola informazione del possesso o meno di un *green pass* valido. Per quanto riguarda le funzionalità disponibili sulla piattaforma NoiPA e sul portale Inps il Garante ha chiesto l'adozione delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dai trattamenti. La verifica mediante interoperabilità applicativa sarà invece resa disponibile ai datori di lavori mediante un'apposita convenzione con il Ministero della salute (v. *infra* par. 14.6).

Un successivo intervento è stato reso nel mese di dicembre su una versione ulteriormente modificata del predetto d.P.C.M. 17 giugno 2021 (provv. 13 dicembre 2021, n. 430, doc. web n. 9727220) in relazione ai trattamenti di dati personali finalizzati alla verifica del rispetto dell'obbligo vaccinale previsto per alcune categorie di lavoratori (v. *infra* par. 14.6) nonché alle misure di garanzia da rispettare nello sviluppo delle diverse modalità di verifica delle certificazioni denominate modalità rafforzata e modalità base.

5

Oggetto di analisi è stata anche la corretta individuazione del ruolo assunto dai soggetti coinvolti nei trattamenti di dati personali connessi alla verifica del rispetto dell'obbligo vaccinale, al fine di assicurare la trasparenza nei confronti degli interessati e di consentire una chiara ripartizione degli obblighi e delle responsabilità previste dal RGPD. Particolare rilievo assume il tema della revoca delle certificazioni verdi con riferimento alle ipotesi di sopraggiunta positività di un interessato che ha completato il ciclo vaccinale e di generazione o di acquisizione fraudolenta delle stesse. Nel richiamato parere del 9 giugno 2021, infatti, l'Autorità aveva già rappresentato l'indispensabilità che, all'atto della verifica delle certificazioni verdi, fosse sempre assicurata l'attualità delle condizioni ivi attestate, alla luce del fatto che l'eventuale variazione dei presupposti per il rilascio (ad es. sopraggiunta positività) avrebbe determinato rischi rilevanti in ordine alla correttezza del trattamento e alla reale efficacia della misura di contenimento.

L'intervento del Garante ha avuto ad oggetto anche iniziative locali riguardanti l'uso delle certificazioni verdi. In particolare, l'Autorità ha rilevato che l'ordinanza del presidente della regione non rappresenta una valida base giuridica per prevedere l'utilizzo, in ambito regionale, delle certificazioni verdi di cui al d.l. n. 52/2021 per finalità ulteriori rispetto a quelle indicate nello stesso decreto-legge. Ciò in quanto l'introduzione di misure di limitazione dei diritti e delle libertà fondamentali che implichino il trattamento di dati personali è oggetto di riserva di legge statale e pertanto deve avvenire attraverso una disposizione che abbia le caratteristiche richieste dall'art. 6, par. 4, del RGPD, previa acquisizione del parere dell'Autorità. Ha poi avvertito la Regione Campania che i trattamenti effettuati sulla base dell'ordinanza regionale 6 maggio 2021, n 17 non risultavano conformi alle disposizioni del RGPD, poiché la predetta ordinanza prevedeva un utilizzo eccessivo di dati da esibire in caso di controllo, in violazione del principio di minimizzazione (provv. 25 maggio 2021, n. 207, doc. web n. 9590466). In tale provvedimento è stato rilevato inoltre che l'ordinanza non individuava in modo puntuale i soggetti che potevano trattare le predette informazioni e che potevano accedervi, nonché quelli deputati a controllare la validità e l'autenticità delle certificazioni verdi, disponendo un sistema di rilascio e di verifica, difforme da quello individuato a livello nazionale. È stato inoltre evidenziato il mancato rispetto dei principi di limitazione della conservazione e di integrità e riservatezza, nonché la mancanza di una adeguata valutazione di impatto.

Il Garante è intervenuto anche nei confronti della Provincia autonoma di Bolzano ritenendo, analogamente a quanto rilevato per la Regione Campania, che l'individuazione della certificazione verde quale condizione per l'accesso a "diversi servizi turistici, alberghieri, di *wedding,* trasporti, spettacoli, etc." non può essere prevista in un'ordinanza regionale, né demandata all'unità di crisi di una regione. È stato ribadito che l'uso di certificazioni, che attestino l'avvenuta vaccinazione o guarigione da Covid-19, o l'esito negativo di un test antigenico/molecolare, diverse da quelle indicate nel citato schema di d.P.C.M., nonché l'uso di strumenti di verifica (quali ad es. *app* per dispositivi mobili) ulteriori rispetto a quelli ivi indicati non possono ritenersi ammissibili perché non garantirebbero in ogni caso il rispetto del principio di esattezza dei dati trattati e di integrità e riservatezza (art. 5, par. 1, lett. *d*) e *f*), del RGPD) (provv. 18 giugno 2021, n. 244, doc. web n. 9671917).

Anche nei confronti della Regione Sicilia è stato formulato un avvertimento sui trattamenti di dati personali effettuati in attuazione dell'ordinanza 7 luglio 2021, n. 75 del Presidente della Regione Sicilia, in quanto, in assenza di interventi correttivi, avrebbero violato le disposizioni del RGPD e del Codice (provv. 22 luglio 2021, n. 273, doc. web n. 9683814). L'ordinanza prevedeva infatti trattamenti di dati personali relativi allo stato vaccinale dei dipendenti pubblici e degli enti regionali,

determinando limitazioni dei diritti e delle libertà individuali che possono essere introdotte, come detto, solo da una norma nazionale di rango primario, previo parere dell'Autorità. Le disposizioni regionali prevedono che tutti i dipendenti a contatto diretto con l'utenza siano "formalmente invitati" a ricevere la vaccinazione e, in assenza di questa, assegnati ad altra mansione. Tali trattamenti relativi allo stato vaccinale del personale non previsti dalla legge statale, introducono, di fatto, un requisito per lo svolgimento di determinate mansioni su base regionale, generando una disparità di trattamento rispetto al personale che svolge le medesime mansioni sulla restante parte del territorio nazionale. L'ordinanza prevedeva, inoltre, trattamenti generalizzati di dati relativi allo stato vaccinale dei dipendenti, anche da parte del medico competente, non conformi alla disciplina in materia di protezione dei dati e alla disciplina in materia di sicurezza nei luoghi di lavoro. Il Garante ha altresì ritenuto che il coinvolgimento dei datori di lavoro, in assenza di misure tecniche e organizzative, poteva porsi in contrasto con le norme nazionali che vietano ai datori di lavoro di trattare informazioni relative alla salute, alle scelte individuali e alla vita privata dei dipendenti. L'Autorità, in considerazione delle gravi violazioni riscontrate, ha dunque ritenuto necessario intervenire tempestivamente per tutelare i diritti e le libertà degli interessati, prima che tali criticità producessero i loro effetti.

Il provvedimento è stato comunicato al Presidente del Consiglio dei ministri e alla Conferenza delle Regioni e delle Province autonome per le valutazioni di competenza.

5.1.3. Il trattamento dei dati personali nell'ambito della refertazione dei test per la rilevazione del Covid-19

Con parere 3 novembre 2020, reso sul d.m. adottato in pari data dal Mef, l'Autorità aveva rilevato con favore che, nonostante il contesto emergenziale, le cautele previste per la consegna dei referti in modalità digitale di cui al d.P.C.M. 8 agosto 2013 fossero applicabili anche per la messa a disposizione dell'assistito dei referti elettronici dei tamponi per la rilevazione del Covid-19 (provv. 3 novembre 2020, n. 215, doc. web n. 9563445).

Nonostante tale espressa previsione, nel 2021, sono pervenute numerose segnalazioni e reclami riguardanti la comunicazione dei referti dei predetti tamponi con modalità non rispettose della disciplina sulla protezione dei dati e della richiamata normativa di settore.

L'Autorità è poi intervenuta, al termine del procedimento aperto a seguito della notifica di un *data breach* da parte di una azienda sanitaria, a carico di quest'ultima, per la violazione degli artt. 6 e 9 del RGPD, nonché dei principi base di cui all'art. 5, par. 1, lett. *f*), del RGPD medesimo, in quanto nel riscontrare un'istanza di accesso documentale, tale azienda sanitaria aveva erroneamente inviato al soggetto istante, in assenza di base giuridica, documentazione non inerente alla richiesta di accesso ed in particolare un documento riguardante due casi di positività al Covid-19 e un altro contenente gli indirizzi *e-mail,* nonché i recapiti interni di 3 dipendenti di tale azienda sanitaria (provv. 16 dicembre 2021, n. 436, doc. web n. 9742435).

5.2. *Sanità digitale*

Nel 2021 il Garante è tornato ad occuparsi delle *app* utilizzate nelle strutture sanitarie per fornire servizi sanitari. In particolare è stata ammonita una Asl circa il trattamento di dati effettuato attraverso un'applicazione volta a consentire agli accompagnatori del paziente di un pronto soccorso di monitorare l'*iter* diagnostico

5

intrapreso. Dall'istruttoria è emerso che la valutazione di impatto effettuata dall'azienda risultava priva di una valutazione circa la necessità e la proporzionalità dei trattamenti, gli specifici rischi per i diritti e le libertà degli interessati che il trattamento in oggetto avrebbe potuto comportare, considerato che alcuni dei rischi indicati nella valutazione effettuata dal titolare non risultavano coerenti rispetto alle caratteristiche dell'applicazione in parola. Non erano inoltre state correttamente definite le misure previste per affrontare i rischi dettati dal trattamento, l'esatto periodo di conservazione dei dati, nonché i ruoli e le responsabilità del titolare e del responsabile del trattamento (provv. 13 maggio 2021, n. 201, doc. web n. 9687977).

Il Garante ha in particolare rilevato la necessità che il titolare, fin dalla progettazione, provveda a esaminare preventivamente i rischi per i diritti e le libertà degli interessati, individuando misure adeguate in funzione di tali rischi, al fine di offrire ai pazienti e ai loro accompagnatori, soluzioni idonee a tutelare in modo efficace i dati che li riguardano, tenendo in particolare considerazione l'eventuale trattamento di informazioni sulla salute di un numero considerevole di pazienti in pronto soccorso (artt. 25 e 35 del RGPD). Al riguardo, l'Autorità ha aggiunto che si dovrebbe evitare, come effettuato presso taluni presidi ospedalieri, l'utilizzabilità di tale *app* qualora l'interessato si avvalga dei servizi ospedalieri per particolari eventi o patologie (si pensi alle vittime di atti di violenza domestica).

5.2.1. Il Fascicolo sanitario elettronico

Anche nel 2021 il Garante ha continuato ad occuparsi degli effetti delle riforme normative in materia di Fse sulla protezione dei dati personali.

In particolare, con specifico riferimento alla possibilità di rendere accessibili, tramite il Fse, anche i dati derivanti dagli eventi clinici occorsi all'assistito prima della data di entrata in vigore del d.l. n. 34/2020 (*id est* 19 maggio 2020), a prescindere dalla circostanza che lo stesso interessato avesse prestato, prima di tale data, il consenso all'alimentazione del Fse all'epoca vigente, si è ribadito che il Fascicolo può essere alimentato anche con tali dati e documenti, purché ricorrano le seguenti condizioni: sia effettuata un'adeguata campagna informativa a livello nazionale e regionale volta a rendere edotti gli interessati in merito alle caratteristiche del trattamento effettuato attraverso il Fse, con particolare riferimento alle novità introdotte dal cd. d.l. Rilancio; sia garantito all'interessato di poter esercitare il diritto di opporsi alla predetta alimentazione del Fse con i dati sanitari generati da eventi clinici occorsi allo stesso antecedentemente al 19 maggio 2020, entro un termine prestabilito, non inferiore a 30 giorni. Per quanto riguarda invece i dati relativi alle prestazioni sanitarie erogate al di fuori del Ssn (che fino al 19 maggio non alimentavano il Fse), il Garante ha fornito indicazioni affinché, alla luce delle disposizioni vigenti, questi possano essere inseriti nel Fse solo se relativi a prestazioni sanitarie erogate successivamente alla predetta data di entrata in vigore del d.l. Rilancio (cfr. comunicato stampa 11 gennaio 2021, doc. web n. 9516732, nota 5 febbraio 2021 alla Regione Piemonte e circolare del Ministero della salute 17 febbraio 2021).

L'Autorità ha inoltre partecipato ai lavori del tavolo nazionale sul Fse (ex art. 26, d.P.C.M. n. 178/2015) in merito all'attività di revisione della disciplina attuativa del Fse alla luce delle modifiche normative intervenute.

Al riguardo merita evidenziare che i recenti interventi normativi di modifica dell'art. 2-*sexies* del Codice ad opera del d.l. n. 139/2021 incidono anche sulla disciplina del Fse. In particolare, il nuovo comma 1-*bis* del predetto art. 2-*sexies* del Codice prevede che i dati relativi alla salute, privati di elementi identificativi diretti, possano essere trattati dal Ministero della salute, dall'Istituto superiore di sanità (Iss), dall'Agenzia nazionale per i servizi sanitari regionali (Agenas), dall'Agenzia italiana

del farmaco (Aifa), dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà (Inmp) e dalle regioni (relativamente ai propri assistiti), anche mediante l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Ssn, ivi incluso proprio il Fse, nel rispetto delle finalità istituzionali di ciascun ente e che i predetti sistemi informativi perseguano finalità compatibili con quelle sottese al trattamento. Le modalità e le finalità di tali trattamenti saranno oggetto di un decreto del Ministro della salute da adottare, previo parere del Garante.

Il Garante sarà inoltre chiamato ad esprimersi anche con riferimento all'attuazione della disciplina sul trattamento dei dati da parte del Ministero della salute per lo sviluppo di metodologie predittive del fabbisogno della salute della popolazione (art. 7, d.l. n. 34/2020). L'attuazione di tale normativa avrà un riflesso importante sulla disciplina del Fse atteso che il d.l. n. 139/2021 ha previsto che a tali fini il Ministero sia autorizzato a procedere all'interconnessione dei sistemi informativi su base individuale del Ssn, ivi incluso il Fse, con i sistemi informativi gestiti da altre amministrazioni pubbliche che raccolgono i dati non relativi alla salute con modalità tali da garantire che l'interessato non sia direttamente identificabile (art. 7, comma 1-*bis*, d.l. n. 34/2020).

Numerose sono state altresì le istruttorie relative a segnalazioni, reclami e *data breach* sul trattamento dei dati personali effettuato attraverso il Fse nonché a molteplici provvedimenti sanzionatori nei confronti di aziende sanitarie. Alcune tra le istruttorie più rilevanti hanno riguardato il mancato rispetto delle richieste di oscuramento esercitate dall'interessato nei confronti dei dati e dei documenti accessibili attraverso il Fse. Al riguardo, è stata sanzionata una Asl per avere inserito nel Fse di una paziente minore di età un referto, relativo a una prestazione erogata da un centro di consultazione per adolescenti a cui gli stessi possono accedere in modo autonomo sul tema della contraccezione e della procreazione responsabile, con riferimento al quale l'interessata aveva esercitato il diritto di oscuramento (provv. 29 aprile 2021, n. 175, doc. web n. 9676172).

Il mancato rispetto del diritto di oscuramento esercitato da un'interessata nei confronti di un referto di interruzione di gravidanza è stato oggetto di un altro provvedimento sanzionatorio adottato nei confronti di un'azienda sanitaria (provv. 27 maggio 2021, n. 211, doc. web n. 9688471). Un errore nel sistema informatico aveva infatti determinato la visibilità del referto nel Fse anche se la richiesta di oscuramento dell'interessata era stata correttamente registrata.

Il Garante, a seguito di una notifica di violazione presentata ai sensi dell'art. 33 del RGPD, ha sanzionato un'azienda sanitaria per il mancato rispetto del diritto di oscuramento esercitato da oltre 100 interessati. Anche in questo caso, a causa di una problematica legata all'aggiornamento di un *software,* successivamente risolta, 293 documenti sanitari (di cui 163 relativi a dati di soggetti a maggior tutela dell'anonimato) riferiti a 175 interessati erano stati inseriti nei Fse sebbene gli stessi avessero esercitato il diritto di oscuramento (provv. 27 maggio 2021, n. 212, doc. web n. 9682641)

A seguito di una segnalazione, il Garante ha sanzionato un'azienda sanitaria per aver reso consultabile il referto di un minore attraverso il Fse da un soggetto che non vantava potestà legale sullo stesso. In considerazione dell'errore segnalato, dettato dall'omonimia di due pazienti, la Asl ha adottato dei sistemi di *alert* automatici per la rilevazione di tali fattispecie (provv. 24 giugno 2021, n. 251, doc. web n. 709119).

Al riguardo, si segnala il caso di un centro diagnostico che ha notificato tre violazioni di dati personali ai sensi dell'art. 33 del RGPD e nei cui confronti è stato presentato anche un reclamo in riferimento ai trattamenti di dati relativi alla salute.

5

Con provvedimento 25 marzo 2021, n. 118 (doc. web n. 9586906), il Garante ha contestato al predetto centro numerose condotte: l'avvenuta consegna a due pazienti dei referti relativi ad altri pazienti; la visualizzazione, nell'ambito del sistema di refertazione *online,* di immagini diagnostiche relative ad altri pazienti, per un totale di 35 interessati coinvolti; l'attribuzione nel Fse di un interessato di referti di altri pazienti, per un totale di 62 interessati coinvolti. L'Autorità ha accertato che le condotte descritte hanno integrato una violazione dei principi di liceità e correttezza e di integrità e riservatezza dei dati, in quanto sono state svolte comunicazioni di dati personali relativi alla salute in assenza sia di idoneo presupposto giuridico sia di misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati fin dalla progettazione del trattamento, nonché a garantire un livello di sicurezza dei dati adeguato al rischio (cfr. artt. 5, par. 1, lett. *a*) e *f*), 9, 25 e 32 del RGPD.

5.2.2. Il dossier *sanitario*

In merito al trattamento dei dati sanitari effettuato attraverso il *dossier* sanitario sono state avviate molteplici istruttorie volte a evidenziare le criticità di tale strumento e le relative responsabilità, atteso che in taluni casi le aziende sanitarie utilizzano sistemi informativi già predisposti a tal fine dalle regioni.

Tra le istruttorie definite nel 2021, si richiama quella nei confronti di una azienda sanitaria a seguito di alcuni reclami e segnalazioni e di una notifica di violazione da parte del titolare. Gli interessati avevano segnalato ripetuti accessi al loro *dossier* da parte di personale sanitario che, sebbene autorizzato al trattamento, non era coinvolto nel loro processo di cura. Il Garante ha al riguardo rilevato che le misure adottate dall'azienda non hanno evitato che personale sanitario accedesse al *dossier* sanitario di pazienti che non avevano in cura, determinando un trattamento illecito dei dati personali, in violazione degli artt. 5 par. 1, lett. *a*) e *f*) e 9 del RGPD. L'azienda ha implementato le misure volte a limitare l'accesso al *dossier* sanitario dei pazienti al solo personale sanitario curante soltanto dopo aver accertato gli episodi oggetto dei predetti reclami ed avere individuato soluzioni logico-informatiche basate sulle indicazioni già fornite dal Garante nelle linee guida del 2015 e ribadite nei provvedimenti successivamente adottati (provv. 21 aprile 2021, n. 155, doc. web n. 9678507).

Il Garante ha altresì sanzionato un istituto di ricovero e cura a carattere scientifico in relazione alla presenza nelle cartelle cliniche di documenti sanitari inconferenti dovuta a un *bug* nel servizio di stampa delle cartelle cliniche di cui l'istituto non si era reso conto se non dopo la segnalazione da parte dell'interessato (provv. 24 giugno 2021, n. 250, doc. web n. 9689566).

La presenza di documenti sanitari di soggetti diversi dall'intestatario nel *dossier* è stata oggetto anche di un'altra notifica di violazione da parte di una azienda ospedaliera, nei cui confronti il Garante ha adottato un provvedimento di ammonimento (provv. 2 dicembre 2021, n. 421, doc. web n. 9732497). L'errore, dettato da omonimia dei pazienti, ha evidenziato come le misure adottate dal titolare, già destinatario di un provvedimento correttivo sanzionatorio nel 2020 per fattispecie analoga, non erano risultate idonee a scongiurare il rischio di non corretta attribuzione dei documenti nei *dossier* sanitari (v. Relazione 2020, p. 99 ss; provv. 23 gennaio 2020, n. 18 doc. web n. 9269629).

5.3. *I trattamenti per finalità di cura e amministrative correlati alla cura*

5.3.1. I provvedimenti derivanti da data breach

Nell'ultimo anno, si è registrato un incremento delle notifiche di violazione di dati personali, ai sensi dell'art. 33 del RGPD, con particolare riferimento ai trattamenti di dati personali effettuati in ambito sanitario. Molte di queste notifiche hanno reso necessaria l'apertura di istruttorie preliminari dalle quali, in gran parte dei casi, sono scaturiti provvedimenti correttivi e sanzionatori. Le istruttorie avviate, in un numero rilevante di casi, hanno riguardato la comunicazione di dati sulla salute, anche contenuti in documentazione sanitaria, a soggetti diversi dall'interessato in mancanza di un presupposto giuridico legittimante, in violazione degli artt. 5 e 9 del RGPD, nonché in talune fattispecie, altresì, in violazione dell'art. 75 del Codice e dei principi di integrità e riservatezza dei dati (art. 5, par. 1, lett. *f*), del RGPD), nonché in assenza di misure di sicurezza adeguate (art. 32 del RGPD) e degli obblighi di *privacy by design* (art. 25 del RGPD). In particolare, le violazioni hanno riguardato: la spedizione, in formato cartaceo, di un referto relativo ad esami ematici di un bambino a un soggetto diverso da quello legittimato a riceverlo, a causa di un erroneo imbustamento della documentazione (provv. 11 febbraio 2021, n. 52, doc. web n. 9567143); la consegna, in formato cartaceo, di documentazione sanitaria relativa ad una prestazione di pronto soccorso a persona diversa dall'interessato a causa della duplicazione di documentazione (provv. 25 febbraio 2021, n. 70, doc. web n. 9574764); l'erroneo inserimento all'interno delle copie delle cartelle cliniche di referti appartenenti a soggetti diversi dall'intestatario delle stesse (provv.ti 27 gennaio 2021, n. 30, doc. web n. 9544092 e n. 29, doc. web n. 9544457); l'erronea trasmissione, a soggetto terzo non autorizzato, di documentazione sanitaria riguardante un altro paziente (provv.ti 11 febbraio 2021, n. 46, doc. web n. 9567489 e 16 settembre 2021, n. 329, doc. web n. 9718851); la comunicazione a terzi di dati di otto pazienti, anche concernenti esiti di esami ematici e delle urine, causata da un'erronea associazione tra referti e prenotazioni effettuati in tempi diversi (provv. 11 marzo 2021, n. 92, doc. web n. 9581069); l'erroneo inserimento nella copia digitale della cartella clinica di un interessato, dei referti relativi ad altri 7 pazienti (provv. 11 febbraio 2021, n. 45, doc. web n. 9561792); la trasmissione ad un soggetto diverso dall'interessato di una notifica obbligatoria di malattia infettiva e diffusiva ai sensi del d.m. 15 dicembre 1990 (provv. 29 aprile 2021, n. 174, doc. web n. 9676143); l'inserimento di una cartella infermieristica, contenente dati identificativi, di contatto e sulla salute (decorso del ricovero) e altre informazioni quali peso, altezza, parametri vitali, di un paziente all'interno di una cartella clinica di un terzo (provv. 29 aprile 2021, n. 176, doc. web n. 9678001); l'inserimento, nella documentazione clinica di un paziente ricoverato e, successivamente deceduto, consegnata alla figlia del paziente, di referti contenenti una consulenza oncologica e una ecografia all'addome, concernenti due altri soggetti (provv. 22 luglio 2021, n. 279, doc. web n. 9695041); l'inclusione di due referti, relativi ad un esame emocromocitometrico e a un elettrocardiogramma, di una paziente all'interno della busta destinata ad un altro paziente e allo stesso consegnata (provv. 25 novembre 2021, n. 410, doc. web n. 9732967); l'invio, ad una paziente, di due referti riguardanti altri due pazienti (provv. 2 dicembre 2021, n. 420, doc. web n. 9739586); gli invii agli interessati di dati relativi a soggetti terzi, da parte della medesima azienda, nei confronti della quale è stato adottato un unico provvedimento sanzionatorio (provv. 8 luglio 2021, n. 264, doc. web n. 9691011).

Altre notifiche hanno riguardato lo smarrimento di documentazione sanitaria: in particolare, un'azienda ha notificato al Garante, a distanza di circa tre mesi l'una

5

dall'altra, due violazioni di dati personali, aventi ad oggetto, in un caso, lo smarrimento di alcuni documenti contenuti all'interno della cartella clinica sanitaria di un interessato, deceduto nel 2015 (diario infermieristico, diario clinico, consensi informati, alcuni referti, due schede di dimissione ospedaliera, lettera di dimissione, esame radiologico e ematico) e, nell'altro, lo smarrimento di una cartella clinica contenente i referti di alcuni esami strumentali, raccolti da una paziente a seguito di prestazioni sanitarie svolte in altri ospedali, propedeutici all'effettuazione di un intervento chirurgico programmato. L'istruttoria si è conclusa con un provvedimento correttivo (provv. 29 aprile 2021, n. 173, doc. web n. 9672313).

Altre violazioni notificate al Garante hanno avuto ad oggetto l'invio di comunicazioni in copia conoscenza (cc), invece che in copia conoscenza nascosta (ccn). Un'azienda sanitaria ha, infatti, comunicato di aver trasmesso, via *e-mail,* un invito a compilare un questionario sullo stato di salute a 98 indirizzi, rendendoli visibili a tutti i destinatari. Il questionario era volto a raccogliere informazioni per fornire assistenza ai pazienti malati di HIV seguiti dall'ambulatorio di malattie infettive dell'azienda, considerato che le visite ambulatoriali programmate erano state sospese a causa dell'emergenza sanitaria. La predetta condotta dell'azienda in assenza di un idoneo presupposto giuridico e, quindi, in violazione, non solo degli artt. 5 e 9 del RGPD, ma anche dell'art. 75 del Codice, che fa salve le specifiche disposizioni di settore, tra le quali l'art. 5, comma 4 e l'art. 1, comma 2, l. 5 giugno 1990, n. 135, recante il piano degli interventi urgenti in materia di prevenzione e lotta all'Aids, è stata sanzionata (provv. 16 settembre 2021, n. 328, doc. web n. 9722297). Analogamente, un'altra azienda sanitaria ha inoltrato – sempre per la compilazione di un questionario, in questo caso relativo allo spettro autistico – alcune *e-mail* con destinatari multipli inseriti nel campo cc, anziché nel campo ccr/ccn, con la conseguenza che ciascun destinatario dell'*e-mail* è venuto a conoscenza degli indirizzi di posta elettronica degli altri destinatari affetti dal medesimo disturbo; ciò ha comportato la comunicazione di dati sulla salute a soggetti terzi, in assenza di un idoneo presupposto giuridico, e, quindi, in violazione dei principi applicabili al trattamento di dati personali, di cui agli artt. 5, par. 1, lett. *a*) e *f*) e 9 del RGPD (provv. 13 maggio 2021, n. 206, doc. web n. 9688020). Non diversa la violazione occorsa presso un'azienda ospedaliero-universitaria che per errore ha inviato attraverso una *mailing-list* in chiaro a diciotto mamme di bambine in cura presso il reparto endocrinologia pediatrica un invito da cui si poteva desumere la condizione di pubertà precoce delle piccole pazienti seguite dal centro. All'esito dell'attività istruttoria, il Garante ha ammonito il titolare del trattamento per violazione dei principi di liceità e correttezza del trattamento e per avere effettuato una comunicazione di dati personali in assenza di idoneo presupposto giuridico (provv. 29 settembre 2021, n. 361, doc. web n. 9720314).

Rileva altresì nell'ambito delle violazioni notificate al Garante, ai sensi dell'art. 33 del RGPD, quella che ha riguardato la pubblicazione da parte di un'azienda sanitaria, sul proprio sito istituzionale di due provvedimenti amministrativi che hanno disposto la dispensa dal lavoro per inabilità di due dipendenti risultati non idonei al servizio, unitamente agli allegati atti istruttori, contenenti dati personali idonei a rilevare lo stato di salute degli interessati. Il trattamento dei dati personali in parola è avvenuto in violazione dei principi di liceità e di minimizzazione dei dati (artt. 5, par. 1, lett. *a*) e *c*), 9, par. 2, del RGPD e del 2-*septies,* comma 8, del Codice), che prevede lo specifico divieto di diffusione dei dati sulla salute. Nel caso in esame, tenuto conto che la condotta ha esaurito i suoi effetti e che sono state fornite idonee assicurazioni da parte del titolare del trattamento, che ha implementato specifiche misure tecniche per evitare il ripetersi della condotta contestata, il Garante ha

comminato una sanzione amministrativa pecuniaria senza adottare provvedimenti di tipo prescrittivo o inibitorio di cui all'art. 58, par. 2, del RGPD (provv. 11 febbraio 2021, n. 53, doc. web n. 9572244).

Nel 2021 è stato approvato uno specifico codice di condotta relativo al trattamento dei dati personali effettuato a fini didattici e di pubblicazione scientifica (provv. 14 gennaio 2021, n. 7, doc. web n. 9535354).

Con tre distinti provvedimenti, adottati nei confronti di un medico, di una Ausl e di un'associazione di medici chirurghi, il Garante ha sanzionato la condotta relativa alla pubblicazione *online* di documenti sulla salute di un paziente contenuti nella documentazione presentata in occasione di un premio a carattere scientifico. Il caso ha preso le mosse da una comunicazione di violazione dei dati personali da parte di un'azienda sanitaria chiamata in causa da un paziente che, dopo essersi curato presso tale struttura, aveva rinvenuto fotografie, diapositive e altre informazioni riferibili alla sua salute sul sito di un'associazione medica. Nella documentazione, reperibile anche tramite comuni motori di ricerca, erano riportate informazioni molto dettagliate come le iniziali del paziente, l'età, il sesso, l'anamnesi dettagliata della patologia sofferta dallo stesso, dettagli sui ricoveri e gli interventi effettuati negli ultimi venti anni, nonché 22 fotografie che ritraevano l'interessato durante il decorso clinico. Nei predetti provvedimenti il Garante ha rilevato che non si era proceduto ad anonimizzare i documenti pubblicati né ad informare l'interessato e che non era stata richiesta alcuna autorizzazione alla predetta azienda per l'utilizzo di dati e documenti clinici di cui la stessa è titolare, essendo stata acquisita copia dei dati e dei documenti utilizzati nelle predette diapositive direttamente attraverso gli strumenti informativi aziendali (provv.ti 15 aprile 2021, nn. 142, 144 e 145, rispettivamente, doc. web nn. 9587071, 9587637 e 9587089).

In relazione alla notifica, ai sensi dell'art. 33 del RGPD, di smarrimento di documentazione sanitaria relativa a un ospite di una casa albergo per anziani, il Garante ha ammonito tale struttura per la mancata adozione di misure di sicurezza tecniche e organizzative adeguate in violazione degli artt. 5, par. 1, lett. *f*) e 32 del RGPD (provv. 14 ottobre 2021, n. 371, doc. web n. 9717745).

Un caso particolare ha riguardato la violazione di dati relativi allo stato di salute di una paziente ricoverata per un'interruzione volontaria di gravidanza che aveva esplicitamente richiesto che non fossero date informazioni sul suo stato di salute a soggetti terzi. A causa di un mancato aggiornamento dei dati di contatto dell'interessata, il personale sanitario, in una fase successiva al ricovero, ha fornito indicazioni sul reparto di degenza al marito della paziente, determinando una violazione dei principi di liceità, correttezza, esattezza, riservatezza e integrità di cui all'art. 5, par. 1, lett. *a*), *d*) e *f*), del RGPD e una comunicazione di dati in assenza di un idoneo presupposto normativo, ai sensi dell'art. 9 del RGPD (provv. 27 gennaio 2021, n. 36, doc. web n. 9544504).

Anche soggetti privati hanno provveduto a dare corso all'obbligo di notificare il *data breach* al Garante: sempre in relazione alla problematica relativa alla comunicazione di documentazione sanitaria a soggetti non legittimati, si sono conclusi con un provvedimento del Garante i casi di un'importante società, che aveva notificato una violazione di dati personali, in relazione all'avvenuta consegna, via *e-mail,* a una paziente, di documentazione contenente il referto delle analisi delle urine di un'altra paziente (provv. 21 aprile 2021, n. 148, doc. web n. 9675228) e di un'altra società, che aveva consegnato un referto, relativo ad un esame del liquido seminale, attraverso un corriere, a persona diversa dal destinatario, per errore dovuto a omonimia (provv. 27 maggio 2021, n. 213, doc. web n. 9688471).

Altre violazioni di dati personali sono state comunicate in conseguenza di attacchi

5

informatici subiti da strutture sanitarie. In particolare, una casa di cura, informata dalla Polizia postale, ha notificato una violazione di dati personali in relazione a un attacco informatico, che ha comportato la pubblicazione, sul profilo Twitter del medesimo gruppo, di immagini radiologiche riconducibili alla casa di cura. La stessa, infatti, al fine di consentire lo svolgimento di consulti medici e clinici tra l'*equipe* curante ed il professionista in grado di interpretare correttamente tali immagini, evitando l'accesso in sede, come richiesto dal contesto emergenziale da pandemia da Covid-19, aveva implementato un sistema di accesso da remoto alla diagnostica per immagini, che consentiva al medico radiologo di visionare le immagini da refertare, attraverso un apposito *software.* L'istruttoria, aperta sia nei confronti del titolare che del responsabile del trattamento, ha accertato che la menzionata installazione permetteva l'accesso al predetto *software* mediante protocollo HTTP (*HyperText Transfer Protocol*), ossia un protocollo di rete che non garantisce l'integrità e la riservatezza dei dati scambiati tra il *browser* dell'utente e il *server* che ospita il servizio/sito web e non consentiva agli utenti di verificare l'autenticità del *server* a cui si collegavano. Inoltre, al momento della violazione l'accesso al *software* da parte del radiologo era effettuato con un'utenza di tipo amministrativo (*admin*) e *password* non robusta (*admin*). Sul punto, è stato puntualizzato che l'esigenza di evitare l'accesso in sede dei professionisti e la necessità di fornire loro, nei tempi più rapidi possibili, gli strumenti per poter accedere da remoto alla diagnostica per immagini non giustificano l'utilizzo, da parte di un soggetto autorizzato, di un'utenza tecnica con privilegi amministrativi. La creazione e l'assegnazione di utenze nominali ai soggetti autorizzati al trattamento ben avrebbero potuto essere effettuate da remoto (e non necessariamente nell'ambito di un'attività di formazione dei soggetti da effettuarsi in presenza), anche nel contesto emergenziale, in un lasso di tempo ragionevole (considerato che erano trascorsi 60 giorni tra l'installazione del *software* e l'attacco *hacker*). In sintesi, nel provvedimento adottato nei confronti della società è stato ritenuto che le misure tecniche e organizzative messe in atto dalla società responsabile per il trattamento della casa di cura, per la gestione dell'accesso al *software,* con particolare riferimento all'utilizzo di protocolli di rete non sicuri (HTTP) e alla mancata definizione di *password policy* non erano idonee a garantire un livello di sicurezza adeguato ai rischi dello specifico trattamento. Ciò ha contribuito, peraltro, a creare le premesse per il verificarsi della violazione dei dati personali e, considerato che il RGPD ha disciplinato gli obblighi e le specifiche responsabilità non solo del titolare, ma anche del responsabile del trattamento, anche con riguardo alla sicurezza del trattamento (v. artt. 32 e 83, par. 4, del RGPD), è stata irrogata una sanzione nei confronti della predetta società (provv. 2 dicembre 2021, n. 423, doc. web n. 9734934).

In un distinto provvedimento, in relazione alla medesima vicenda, è stato evidenziato che l'incidente di sicurezza verificatosi non poteva essere ritenuto imputabile soltanto alla società, ma anche alla casa di cura, responsabile della mancata adozione di misure tecniche e organizzative adeguate a garantire la riservatezza e l'integrità dei dati personali trattati mediante il *software,* in violazione degli artt. 5, par. 1, lett. *f*) e 32 del RGPD (provv. 2 dicembre 2021, n. 422, doc. web n. 9734884).

Lo stesso gruppo *hacker* ha effettuato un attacco informatico nei confronti di un centro medico, consistente nell'accesso e successiva pubblicazione di un'immagine parzialmente oscurata di un elenco di nominativi e esami radio-diagnostici effettuati in una specifica data. Nella notifica di violazione comunicata all'Autorità, il centro medico aveva rappresentato che, a seguito di un Q/R (*Query & Retrieve*) sull'IP pubblico della struttura, il gruppo *hacker* era riuscito ad ottenere un quantitativo limitato di metadati DICOM riferibile ad un elenco di cinque nominativi di pazienti che avevano eseguito presso la struttura esami radio-diagnostici nella

medesima giornata. Nell'ambito dell'istruttoria effettuata dal Garante, era emerso che, al momento della violazione, il *server,* se opportunamente interrogato, restituiva i metadati richiesti (nominativo, data di nascita e tipo di esame eseguito) senza verificare l'identità e autenticare il soggetto che effettuava la richiesta, consentendo connessioni non autenticate e di essere raggiungibile dall'esterno. Pertanto, a causa della mancata adozione di una procedura di autenticazione, unitamente al fatto che il *server* fosse raggiungibile da rete internet, al momento in cui si era verificata la violazione dei dati personali, il centro è stato sanzionato per aver violato le disposizioni degli artt. 5, par. 1, lett. *f*), 25, 32, nonché gli obblighi di pubblicazione dei dati di contatto del responsabile della protezione dei dati e di comunicazione all'Autorità, ai sensi dell'art. 37, par. 1, lett. *c*), del RGPD che, da quanto risultato, non erano stati rispettati (provv. 16 dicembre 2021, n. 435, doc. web n. 9739609).

Merita in tale contesto altresì segnalare l'ammonimento comminato a seguito di una notifica di violazione effettuata da una struttura sanitaria privata determinata da un attacco cibernetico *ransomware* giacché, al momento in cui si è verificata la violazione essa non disponeva di un sistema idoneo a garantire il rapido ripristino dei dati oggetto dell'attacco sopra descritto, in violazione degli artt. 5, par. 1, lett. *f*) e 32, par. 1, lett. *b*), del RGPD (provv. 22 luglio 2021, n. 277, doc. web n. 9693442).

5.3.2. I provvedimenti derivanti da reclami e segnalazioni

Anche quest'anno il Garante ha svolto numerose istruttorie in relazione al trattamento effettuato per il perseguimento di finalità di cura e amministrative correlate alla cura.

Estremamente rilevante è stato l'intervento dell'Autorità, sulla base di un reclamo, nei confronti di un dentista che, attraverso la somministrazione di un questionario all'atto dell'accettazione dei pazienti, raccoglieva i dati relativi a presunte malattie infettive (quali la tubercolosi, l'epatite A, B, C e l'HIV) e, nel caso specifico, conosciuta l'informazione relativa all'infezione da HIV, si era rifiutato di prestare le cure. Dalla ricostruzione effettuata, è emerso che la raccolta delle predette informazioni non ha avuto il fine concreto di valutare la migliore terapia per il paziente, offrendogli la prestazione richiesta, eventualmente anche con un rafforzamento delle protezioni dal rischio del contagio, quanto, piuttosto, quello di allontanare il paziente rifiutando le cure dallo stesso richieste. Pertanto, la circostanza che la prestazione medica non sia stata, nei fatti, attuata per volontà del medico, aveva fatto venir meno il presupposto giuridico fondante il trattamento dei dati relativi alla salute, in particolare, consistente nell'acquisizione dell'informazione relativa alla presenza dell'infezione da HIV. Per tale condotta, l'Autorità ha ingiunto al dentista una sanzione per la violazione dell'art. 5 del RGPD (provv. 10 giugno 2021, n. 239, doc. web n. 9677521).

In un'altra occasione, l'Ufficio, a seguito di una segnalazione di un Comando dei Carabinieri, ha avviato un'istruttoria nei confronti di una dottoressa che aveva appeso le ricette mediche, non in busta chiusa, con le mollette da bucato fuori dalla finestra dello studio, situato al piano terra su una pubblica via, rendendole così liberamente visibili e accessibili a chiunque si trovasse a transitare nei pressi del davanzale dello studio medico. Il Garante ha contestato al medico la violazione degli artt. 5, 9 e 32 del RGPD, ingiungendogli il pagamento di una sanzione (provv. 28 ottobre 2021, n. 392, doc. web n. 9716887).

Un'altra istruttoria è stata avviata a seguito di una segnalazione da parte di una società del settore della distribuzione di alcuni dispositivi medici e di biancheria e materasseria nel settore ospedaliero, in relazione ad una procedura attuata da un'azienda sanitaria per acquisire dalla medesima società e da altre ditte competenti un

5

preventivo-offerta per la fornitura di diverse tipologie di ausili. Infatti, la comunicazione dell'azienda volta a ottenere il predetto preventivo, conteneva i dati personali di circa 60 pazienti ai quali erano destinati i presidi sanitari oltre che, in taluni casi, del medico prescrittore, in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. *f*) e 9 del RGPD e ha comminato all'azienda sanitaria una sanzione amministrativa (provv. 22 luglio 2021, n. 278, doc. web n. 9693760).

A seguito di un reclamo, il Garante ha sanzionato una fondazione sanitaria per la violazione dei principi di integrità e riservatezza e di liceità, correttezza e trasparenza, degli obblighi nonché dei doveri di protezione dei dati sin dalla progettazione (artt. 5, par. 1, lett. *a*) e *f*), 13, 25 e 32 del RGPD). L'Autorità ha accertato, infatti, che il titolare, oltre a non aver fornito l'informativa agli interessati, aveva predisposto, per la richiesta in via telematica di visite di controllo, un sito/servizio web con protocollo di rete HTTP (*HyperText Transfer Protocol*), che, per sua natura, non garantisce la riservatezza e l'integrità dei dati scambiati tra il *browser* dell'utente e il *server* che ospita il sito web del titolare e non consente agli utenti di verificare l'autenticità del sito web visualizzato (provv. 21 aprile 2021, n. 147, doc. web n. 9591223).

Altri reclami conclusi con l'adozione di un provvedimento correttivo da parte del Garante hanno riguardato la consegna di documentazione sanitaria a soggetti non legittimati. Si segnala, in particolare, il caso di una paziente che aveva lamentato l'inserimento, da parte di un centro salute mentale sardo, di alcuni fogli relativi ad un diario clinico, nel quale erano riportati parti di colloqui psicologici avuti dalla stessa paziente con gli operatori del centro, all'interno di altra documentazione relativa ad un soggetto terzo e allo stesso consegnato. La peculiarità del caso consisteva nella circostanza che il soggetto terzo, che apparteneva alla stessa comunità cittadina della reclamante, avrebbe lui stesso avvisato la paziente di quanto accaduto. Nel provvedimento adottato nei confronti dell'azienda sanitaria, nel definire l'ammontare della sanzione, si è tenuto conto di una serie di elementi, tra i quali la pronta attivazione per porre rimedio all'accaduto e la revisione di molteplici procedure riguardanti la gestione della documentazione sanitaria (provv. 14 ottobre 2021, n. 370, doc. web n. 9722265).

Analogamente, è stato oggetto di valutazione dell'Autorità una comunicazione di documentazione sanitaria a soggetti non legittimati, da parte di una società che gestisce poliambulatori la quale, secondo quanto si è appreso da specifiche istanze, in un caso aveva recapitato, ad una paziente, madre della segnalante, un referto, relativo ad un esame diagnostico dell'ecocardiogramma di un terzo, pur riportando, le immagini allegate, il nome della medesima paziente e, in un altro, aveva consegnato un referto, nel quale veniva indicata l'anagrafica di un'altra paziente della struttura, omonima nel cognome, che si era recata in un altro periodo presso la struttura. Tali comunicazioni di dati relativi alla salute erano prive di un idoneo presupposto giuridico e, nel secondo caso, violavano anche il principio di esattezza, secondo il quale devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati e quello di integrità e riservatezza (art. 5, par. 1, lett. *d*), del RGPD. Pertanto, alla società è stata comminata una sanzione considerando, peraltro, gli elementi di cui all'art. 83, par. 2, tra i quali, in un caso, la circostanza che la violazione era stata determinata dall'omonimia dei cognomi degli interessati (provv. 28 ottobre 2021, n. 385, doc. web n. 9724881).

Un reclamo concernente modalità di consegna di un referto relativo ad analisi cliniche effettuate presso una struttura sanitaria privata, ha fornito l'occasione per chiarire la prescrizione contenuta nelle linee guida in tema di referti *online,* adottate dal Garante con il provvedimento 19 novembre 2009, n. 36 (doc. web n. 1679033),

le quali continuano ad applicarsi anche dopo l'entrata in vigore del RGPD (cfr. art. 22, comma 4, d.lgs. n. 101/2018). In particolare, si è precisato che l'invio, in tempi diversi, al medesimo indirizzo di posta elettronica, di *e-mail* contenenti, rispettivamente, la *password* di apertura del *file* e lo stesso *file* non integra il requisito richiesto dalle predette linee guida relativo alla necessità di utilizzare "canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti", poiché trattasi di transazioni o sessioni di un medesimo protocollo di comunicazione e ciò, pertanto, non riduce il rischio di accesso non autorizzato al canale utilizzato (nota 25 maggio 2021).

5.3.3. I trattamenti per finalità ulteriori rispetto a quelle di cura

Il Garante ha, altresì, dato corso ad un reclamo nei confronti di un medico che aveva comunicato, in più occasioni, ai responsabili delle risorse umane di enti, presso i quali la reclamante aveva prestato la propria attività professionale, informazioni relative a trattamenti medici dalla stessa eseguiti, allo scopo di sollecitare l'ex paziente a definire le vicende relative a presunti mancati pagamenti di alcune prestazioni sanitarie fornite dal medico. Nel provvedimento adottato nei confronti del sanitario, il Garante, nel ricordare che l'informazione relativa ad un ricovero presso una clinica costituisce di per sé un dato personale relativo alla salute, ai sensi dell'art. 4, par. 1, n. 15, del RGPD indipendentemente dall'indicazione delle motivazioni cliniche e/o la patologia, che hanno determinato la necessità della prestazione medica ricevuta, ha rilevato che non è stata dimostrata alcuna delle condizioni, tra quelle indicate nell'art. 9, par. 2, del RGPD, che avrebbe potuto, superando il divieto generale di trattare i dati sulla salute, rendere lecita la comunicazione di dati sulla salute della paziente a soggetti terzi. Infatti, nel caso di specie, la condotta del medico è risultata finalizzata a ottenere il pagamento di prestazioni professionali rimaste insolute, finalità che l'ordinamento giuridico consente di perseguire con specifici strumenti di tutela. Pertanto, dichiarata l'illiceità del trattamento effettuato dal professionista, è stato adottato nei confronti dello stesso un provvedimento correttivo (provv. 25 novembre 2021, n. 411, doc. web n. 9733002).

L'Autorità a seguito di segnalazione, ha sanzionato un medico per aver comunicato dati personali di un proprio paziente, comprensivi del recapito telefonico, ad una consulente aziendale di prodotti naturali, dei quali il medico consigliava l'assunzione, in assenza del consenso del segnalante. Il Garante, in tale circostanza, ha accertato la violazione degli artt. 9 e 5, lett. *a*), del RGPD (provv. 29 settembre 2021, n. 358, doc. web n. 9720448).

Nel corso del 2021 si è conclusa l'istruttoria relativa all'utilizzo di dati contenuti in registri di casistica operatoria per la partecipazione a concorsi pubblici. In particolare, un medico che aveva trasmesso i predetti registri, contenenti l'elenco degli interventi chirurgici effettuati presso i presidi ospedalieri dove aveva prestato servizio, in allegato alla domanda di partecipazione ad un avviso pubblico, per l'affidamento di un incarico di direzione di struttura complessa. La predetta documentazione conteneva dati personali direttamente identificativi e sulla salute dei pazienti (quali diagnosi, data e tipo di intervento effettuato, tipo di anestesia somministrata) nonché quelli degli anestesisti e degli infermieri strumentisti. L'Autorità non ha rinvenuto la buona fede evidenziata dal medico, in quanto lo stesso avrebbe dovuto diligentemente conoscere la normativa applicabile, relativa alla produzione della documentazione richiesta ai fini della valutazione da parte della commissione esaminatrice e verificare, nel caso specifico, che l'avviso pubblico richiedeva di accludere una "certificazione del Direttore sanitario (...) riguardante la tipologia qualitativa e quantitativa delle prestazioni effettuate dal candidato", quindi un documento privo di dati personali. Analogamente, per l'attribuzione dei punteggi, doveva essere

5

indicata la "tipologia qualitativa e quantitativa delle prestazioni effettuate dal candidato anche con riguardo all'attività/casistica trattata nei precedenti, misurabili in termini di volume e complessità", in linea con il d.m. n. 283/1992 (v. in particolare art. 4, comma 5, del cit. decreto). È stato, quindi, ritenuto che il medico, di propria iniziativa e dunque in qualità di titolare del trattamento, avesse violato le disposizioni di cui agli artt. 13 e 26 del Codice sanzionate, rispettivamente, dagli artt. 161 e 162, comma 2-*bis,* del Codice medesimo, nella versione antecedente al d.lgs. n. 101/2018, vigente al momento in cui si sono svolti i fatti oggetto della segnalazione, per aver effettuato un trattamento di dati, in parte idonei a rivelare le condizioni di salute degli interessati, in assenza di idonei presupposti legittimanti. Pertanto, è stato adottato nei suoi confronti un provvedimento sanzionatorio (provv. 27 gennaio 2021, n. 26, doc. web n. 9547225).

La medesima istruttoria ha riguardato, altresì, un altro sanitario che aveva trasmesso, anch'esso, per la medesima finalità di partecipazione al concorso pubblico, documentazione inerente la casistica operatoria, contenente l'elenco degli interventi chirurgici effettuati nonché dati relativi alla salute dei pazienti (data dell'intervento, diagnosi, tipo di anestesia somministrata e di intervento effettuato). Avverso il provvedimento con il quale il Garante aveva ravvisato violazione della normativa in materia di protezione dei dati personali (nota 20 settembre 2019), era stato proposto dal medico un ricorso in opposizione, ai sensi degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011. Il Tribunale di Cosenza, a tal fine adito, ha rigettato la predetta opposizione, accogliendo le conclusioni dell'Autorità (sentenza 19 gennaio 2021). Tenuto conto della citata sentenza, è stato rappresentato in particolare che la commissione esaminatrice di concorso, soggetto terzo rispetto all'amministrazione che bandisce la selezione concorsuale, presso la quale erano stati effettuati gli interventi sanitari, è costituita anche da soggetti esterni alla stessa e assume una autonoma titolarità nel trattamento dei dati raccolti per l'espletamento della procedura selettiva. L'Autorità ha, pertanto, adottato nei confronti del medico un provvedimento sanzionatorio (provv. 11 marzo 2021, n. 94, doc. web n. 9590222).

Le istruttorie sopra descritte hanno coinvolto, altresì, un'azienda ospedaliera che è stata oggetto di una verifica ispettiva del Garante, volta a verificare se fossero stati effettuati, in una data precisa, accessi ai sistemi informativi aziendali da parte di uno specifico medico o di altro operatore, in relazione agli interventi effettuati dallo stesso. In occasione del predetto accertamento, è stato verificato che i *file* di *log* relativi alle operazioni di accesso al sistema informatico della sala operatoria, denominato blocco operatorio, che consente di effettuare l'estrazione dei dati relativi ai pazienti sottoposti a intervento chirurgico, erano conservati per un brevissimo tempo (circa 30 minuti, corrispondenti alla registrazione degli ultimi 10 accessi circa nel sistema), insufficiente a garantire la sicurezza dei dati. Il Garante ha al riguardo ricordato che, in relazione alla tracciabilità degli accessi, con riferimento al *dossier* sanitario, "il titolare deve individuare un congruo periodo di conservazione dei *log* di tracciamento delle operazioni che risponda, da un lato, all'esigenza per gli interessati di venire a conoscenza dell'avvenuto accesso ai propri dati personali e delle motivazioni che lo hanno determinato e, dall'altro, alle esigenze medico legali della struttura sanitaria titolare del trattamento di dati personali", individuando, come congruo, un periodo di conservazione non inferiore a 24 mesi dalla data di registrazione dell'operazione (cfr. provv. 4 giugno 2015, n. 331, doc. web n. 4084632, che continua ad applicarsi anche dopo l'entrata in vigore del RGPD, cfr. art. 22, comma 4, d.lgs. n. 101/2018). Sebbene la predetta indicazione in merito al tempo di conservazione dei *file* di *log* si riferisca al *dossier* sanitario (e non anche a singoli applicativi), la stessa avrebbe dovuta essere tenuta in considerazione da parte del titolare ai fini dell'individuazione

di un congruo periodo di conservazione dei *file* di *log* degli accessi all'applicativo che gestisce il sistema informativo della sala operatoria. Pertanto, il Garante ha rilevato l'illiceità del trattamento di dati personali effettuato dall'azienda, in violazione degli artt. 5, par. 1, lett. *f*) e 32 del RGPD e ha adottato nei confronti della stessa un provvedimento correttivo (provv. 11 marzo 2021, n. 93, doc. web n. 9583597).

Un altro caso ha riguardato, con riferimento ad uno dei più grandi centri di diagnosi prenatale d'Italia, l'acquisizione di un unico consenso al trattamento dei dati personali, sia per l'attivazione della procedura di refertazione *online,* sia per ricevere *newsletter* ai servizi erogati dalla struttura. Perdipiù la società aveva omesso di rendere agli interessati tutti gli elementi informativi indicati dall'art. 13 del RGPD ed era risultata inadempiente rispetto agli obblighi concernenti il Rpd. Nel merito della condotta, il Garante ha rilevato l'illiceità del trattamento di dati personali effettuato in violazione degli artt. 5, 9, 13 e 37 del RGPD e ha adottato un provvedimento correttivo-prescrittivo in relazione agli obblighi in materia di Rpd e di informazioni da rendere agli interessati. L'ammontare della sanzione pecuniaria è stato determinato sopratutto in ragione dell'invio di una *newsletter* a un numero elevato di pazienti (potenzialmente tutti quelli che avevano aderito al servizio di refertazione *online*) e in considerazione del fatto che le violazioni avevano, almeno con riferimento al consenso, carattere intenzionale e si erano protratte per un lungo lasso di tempo unitamente alla valutazione delle condizioni economiche della società (provv. 13 maggio 2021, n. 193, doc. web n. 9687954).

Si segnala, altresì, in relazione alla valutazione di impatto in ambito sanitario, quanto rappresentato dal Garante ad una società di riabilitazione ortopedica e neuromotoria di pazienti autistici, che aveva consultato il Garante in relazione al trattamento di dati personali da effettuare attraverso un sistema di videosorveglianza. Dalla documentazione in atti è emerso che si sarebbe voluto attivare il predetto sistema in ciascuna stanza del centro di riabilitazione, con la sola finalità di tutela dei pazienti minori e di garanzia della loro incolumità e sicurezza, considerato un precedente caso di abuso sui minori, da parte di un terapista, successivamente condannato dall'Autorità giudiziaria. L'intenzione sarebbe stata di rilevare anche dati relativi all'audio e di natura biometrica. Il Garante ha richiamato l'attenzione sui principi di limitazione della finalità e di minimizzazione, osservando che, limitatamente alla valutazione in ordine al trattamento dei dati sulla salute, il dichiarato scopo di garantire l'incolumità dei pazienti minori, in particolare, dal rischio di subire reati di natura sessuale e, quindi, di conseguire finalità di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, è attribuito, nel nostro ordinamento giuridico, esclusivamente a soggetti pubblici a ciò deputati (autorità di pubblica sicurezza e Forze di polizia), che istituzionalmente esercitano queste funzioni in modo qualificato, secondo le modalità previste dalla specifica disciplina di settore. Pertanto, il relativo trattamento dei dati può essere effettuato soltanto dai predetti soggetti, in qualità di titolari del trattamento (cfr. punto 2.2. delle linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate dal Cepd il 29 gennaio 2020; cfr. altresì, art. 1, comma 1, artt. 5 e 7, d.lgs. n. 51/2018 e il provv. 22 febbraio 2018, n. 99, doc. web n. 8005333). È stato, inoltre, rilevato che, nel caso di specie, il ricorso ad un sistema di videosorveglianza risultava essere particolarmente invasivo a fronte di gravi rischi per la tutela della intimità e riservatezza dei soggetti sottoposti a videoriprese in ragione della particolare natura dei dati trattati. Il trattamento prospettato non è stato, quindi, valutato conforme alla disciplina di settore e a quella in materia di protezione dei dati personali e, di conseguenza, non si è esaminata la richiesta di consultazione preventiva (nota 7 giugno 2021).

5

5.4. *Esercizio dei diritti*

In linea con gli anni precedenti, anche nel 2021 le istanze per l'esercizio dei diritti di cui agli artt. da 15 a 22 del RGPD rivolte a strutture sanitarie pubbliche o private quali titolari del trattamento hanno riguardato, quasi totalmente, richieste di accesso ai dati personali di cui al citato art. 15 del RGPD. In particolare, i reclami presentati all'Autorità a seguito del mancato o inidoneo riscontro alle istanze degli interessati, hanno avuto ad oggetto l'accesso ai dati contenuti in documenti sanitari e, nello specifico, alla cartella clinica propria o a quella di congiunti deceduti, ai sensi dell'art. 2-*terdecies,* residuando pochi casi di reclamo per mancato o inidoneo riscontro a richieste finalizzate all'esercizio degli altri diritti previsti dal RGPD.

In relazione a reclami presentati per il mancato o inidoneo riscontro a richieste di accesso ai dati personali, il Garante ha adottato alcuni provvedimenti sanzionatori. Nello specifico, ha sanzionato un poliambulatorio per aver fornito riscontro alla richiesta di accesso ai dati, avanzata dall'interessato, oltre il termine previsto dall'art. 12, par. 3, del RGPD (provv. 14 gennaio 2021, n. 8, doc. web n. 9542096). Inoltre, è intervenuto nei confronti di altra struttura sanitaria privata, con una sanzione pecuniaria di maggior importo rispetto al caso precedente per non avere il titolare fornito riscontro alla richiesta di accesso ai dati, presentata dall'interessato, neppure a seguito dell'invito ad aderire formulato dall'Autorità, ai sensi dell'art. 15 del regolamento del Garante n. 1/2019, ma solo a seguito dell'avvio del procedimento ex art. 166 del Codice, volto all'adozione dei provvedimenti di cui all'art. 58, par. 2, del RGPD (provv. 25 marzo 2021, n. 109, doc. web n. 9590711).

L'Autorità ha avuto modo di appurare il diffuso ricorso al diritto di accesso ai dati per ottenere, in realtà, l'accesso alla documentazione sanitaria, spesso copiosa ed ha al riguardo ribadito la diversa *ratio* sottesa agli istituti del diritto di accesso ai dati personali e del diritto di accesso documentale, ai sensi della l. n. 241/1990 e della normativa di settore (l. n. 24/2017).

Nello stesso ambito il Garante, in merito ad alcune istanze finalizzate all'accesso ai dati personali contenuti nelle perizie medico-legali, considerato il contesto di natura contenziosa descritto dagli istanti, pur evidenziando che il cons. 63 in relazione all'art. 15 del RGPD, riconosce all'interessato "(…) il diritto di accedere (…) ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati", ha, al contempo, ritenuto applicabile l'art. 2-*undecies* (limitazione ai diritti dell'interessato) del Codice, in attuazione dell'art. 23 del RGPD, il quale stabilisce che "i diritti di cui agli articoli da 15 a 22 del RGPD non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'art. 77 del RGPD qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto (…) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria (…)".

Con riguardo agli altri diritti di cui agli artt. da 16 a 22 del RGPD, il Garante ha in prevalenza concluso le istruttorie, avviate a seguito di reclamo, con un provvedimento di archiviazione. Si è trattato, nella maggioranza dei casi, di richieste degli interessati non soddisfatte dai titolari per carenza dei presupposti previsti dalle suddette disposizioni. In tali circostanze, l'Autorità ha ribadito, che i dati presenti nella cartella clinica non possono essere cancellati, essendo ammessa unicamente una loro rettifica o integrazione, in considerazione degli obblighi legali connessi alla tenuta della medesima e del fatto che tale documentazione sanitaria è qualificata dalla giurisprudenza – come può evincersi da un orientamento ormai consolidato – quale atto pubblico facente piena prova, fino a querela di falso, delle trascrizioni

delle scelte cliniche e terapeutiche effettuate. Il Garante, ha, altresì, chiarito che le possibili rettifiche e integrazioni della cartella clinica, devono essere effettuate nel rispetto del dovere di non alterare il contenuto della medesima, poiché in relazione a tale inalterabilità la Suprema Corte si è più volte espressa nel senso che "Integra il reato di falso materiale in atto pubblico l'alterazione di una cartella clinica mediante l'aggiunta di una annotazione, ancorché vera, in un contesto cronologico successivo e, pertanto, diverso da quello reale; né, a tal fine, rileva che il soggetto agisca per ristabilire la verità fattuale" (*ex multis:* Cass. pen. 29 maggio 2013, n. 37314).

6 La ricerca scientifica

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

Nel campo della ricerca scientifica, in particolare medica, biomedica e epidemiologica, merita evidenziare due provvedimenti adottati dal Garante, ai sensi degli artt. 110 del Codice e 36 del RGPD, in ragione della impossibilità di acquisire il consenso al trattamento dei dati personali da parte degli interessati.

Il primo provvedimento fa seguito a una istanza di consultazione preventiva relativa a uno studio clinico *no profit,* multicentrico, osservazionale, retrospettivo, non farmacologico, volto alla "caratterizzazione biologica del linfoma a cellule del mantello refrattario o recidivato dopo la prima linea di terapia" e concernente il trattamento di particolari categorie di dati riferiti anche a pazienti non in vita ovvero non contattabili (provv. 1° novembre 2021, n. 406, doc. web n. 9731827).

Il Garante ha espresso un parere favorevole condizionato in riferimento al progetto e alla relativa valutazione di impatto nonché alla documentazione integrativa come modificata a seguito delle preliminari criticità rilevate in fase istruttoria. In particolare, l'Autorità ha ritenuto: le basi giuridiche del trattamento correttamente individuate dal promotore che ha altresì specificato i motivi a fondamento dell'impossibilità di informare gli interessati e acquisirne il consenso, come previsto al punto 5.3 delle prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (all. n. 5 al provv. che individua le prescrizioni contenute nelle autorizzazioni generali che risultano compatibili con il RGPD e con il d.lgs. n. 101/2018 di adeguamento del Codice, 5 giugno 2019, doc. web n. 9124510); la struttura organizzativa per la realizzazione dello studio, come modificata, conforme alla normativa in materia di protezione dei dati personali.

Dopo aver accertato che lo studio comportava anche il trattamento dei dati genetici, il Garante ha richiesto al promotore, in qualità di titolare del trattamento, di adottare le misure di cui al punto 4.2, lett. *a*), *b*) e *d*) delle prescrizioni per il trattamento dei dati genetici (all. n. 4, al provv. cit. del 5 giugno 2019, doc. web n. 9124510). Ha richiesto altresì che il promotore renda pubbliche le informazioni da fornire agli interessati, ai sensi dell'art. 14 del RGPD, attraverso una specifica inserzione anche sui siti internet istituzionali dei centri di sperimentazione coinvolti nello studio, vista la loro numerosità, in conformità all'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) e che tali informative siano integrate con l'indicazione delle modalità con cui gli interessati possono accedere alle informazioni contenute nel progetto di ricerca.

In relazione ai tempi di conservazione, che nel corso dell'istruttoria sono stati ridotti a 10 anni, e agli ulteriori trattamenti che il promotore intendeva effettuare, il Garante tenuto conto del dibattito ancora in corso a livello europeo, ha ritenuto che in concreto l'assenza di specifiche misure di cui all'art. 89 del RGPD e di ulteriori garanzie per assicurare, in particolare, l'effettiva applicazione dei principi di trasparenza e di minimizzazione, nonché l'ampia estensione del tempo di conservazione previsto, rendono il trattamento ipotizzato verosimilmente lesivo di principi applicabili al trattamento dei dati personali sanciti nel RGPD e nella relativa normativa di

attuazione e integrazione giungendo, dunque, a formulare un avvertimento formale, ai sensi dell'art. 58, par. 2, lett. *a*), del RGPD al titolare del trattamento.

Il secondo provvedimento muove anch'esso da un'istanza di consultazione preventiva presentata da una società italiana, in qualità di rappresentante della società capogruppo stabilita negli Stati Uniti, promotrice di uno studio retrospettivo, sulla sicurezza post-autorizzazione all'immissione in commercio di specifici farmaci, cd. *pass* relativo ai dati di pazienti, irreperibili ovvero non contattabili (provv. 11 novembre 2021, n. 397, doc. web n. n. 9736936).

Nel corso dell'attività istruttoria, sono emerse talune criticità e incongruenze in relazione ai trattamenti di dati personali necessari per la realizzazione dello studio, relative all'effettiva applicazione del principio di trasparenza, ai ruoli dei soggetti coinvolti a vario titolo nella realizzazione dello studio, ai flussi di dati e ai tempi di conservazione degli stessi, rispetto ai quali il promotore ha fornito specifici chiarimenti e documentazione integrativa.

Il Garante ha ritenuto che il promotore abbia correttamente individuato le basi giuridiche del trattamento, specificando altresì i motivi che possono giustificare l'impossibilità di riuscire ad informare gli interessati e acquisirne il consenso con il correlato rischio di pregiudicare gravemente il conseguimento delle finalità della ricerca (5.3 prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, doc. web n. 9124510, v. *supra*).

In relazione ai ruoli, è stato chiarito che la società italiana, oltre che rappresentata dalla capogruppo statunitense in ragione del suo ruolo attivo nella definizione delle finalità e dei mezzi del trattamento, agisce in qualità di contitolare del trattamento. L'accordo di contitolarità è stato ritenuto conforme ai contenuti dell'art. 26 del RGPD. Il Garante, tuttavia, per esigenze di maggiore trasparenza, ha evidenziato l'importanza che i contitolari del trattamento specifichino in modo circostanziato i rispettivi ruoli e rapporti in relazione alle finalità e ai mezzi del trattamento, necessari per la realizzazione dello studio e, in particolare che sia ribadito, anche in tale documento, che la società statunitense riceverà dalla CRO (*Clinical Reasearch Organization*) solo il *report* finale dello studio con un livello di aggregazione tale da escludere il rischio di reidentificazione degli interessati.

Con riferimento ai tempi di conservazione, il Garante ha ritenuto congruo il periodo di due anni per lo svolgimento dello studio e, al solo fine di consentire eventuali azioni di controllo e monitoraggio da parte delle autorità competenti (Aifa e Ema), di 15 anni dalla conclusione dello studio.

Con specifico riferimento alle misure volte a garantire l'effettività del principio di trasparenza nei confronti dei pazienti arruolati allo studio, il Garante ha posto, nei confronti dei contitolari del trattamento, due specifiche condizioni ovvero che le informazioni da fornire agli interessati siano rese pubbliche attraverso una specifica inserzione anche sui siti internet istituzionali dei centri di sperimentazione coinvolti nello studio e che le informative sul trattamento dei dati personali siano modificate recando l'indicazione delle modalità con le quali gli interessati possono esercitare, nei confronti dei contitolari del trattamento, i diritti di cui agli artt. da 15 a 22 del RGPD.

7 La statistica

7.1. *La statistica ufficiale*

Il Garante, nell'anno di riferimento, ha promosso l'adozione delle nuove regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (Sistan) (provv. 15 aprile 2021, n. 133, doc. web n. 9582086).

L'Autorità ha rilevato, infatti, come il processo di revisione dei codici di deontologia e di buona condotta, che ha portato all'adozione delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistan pubblicate ai sensi dell'art. 20, comma 4, d.lgs. 10 agosto 2018, n. 101, all. A4 al Codice (provv. 19 dicembre 2018, n. 514, doc. web n. 9069677), rigorosamente circoscritto alla verifica della compatibilità con il rinnovato quadro normativo delle regole ivi contenute, abbia condotto a un ridimensionamento degli ambiti regolamentati nel settore in esame. Tale circostanza, congiuntamente al cambiamento sostanziale delle modalità di realizzazione della statistica ufficiale, anche in virtù dell'evoluzione tecnologica e dell'avanzare della *data driven economy,* rende urgente l'adozione di nuove regole deontologiche.

Nel rispetto degli artt. 2-*quater* e 106 del Codice e secondo la procedura di cui agli artt. 23 e ss. del regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante (doc. web n. 9107633), l'Autorità se ne è fatta promotrice in osservanza del principio di rappresentatività.

Tenuto conto della numerosità dei soggetti che partecipano al Sistan nonché della loro eterogeneità, il Garante ha ritenuto che il principio di rappresentatività possa ritenersi soddisfatto non solo dalla circostanza che lo schema delle nuove regole deontologiche venga presentato, tra gli altri, dall'Istat ma anche dalla presenza di ulteriori specifici requisiti quali in particolare quello relativo alla necessità che venga fornita adeguata prova della massima condivisione dello schema di regole deontologiche sottoposto all'attenzione del Garante con i soggetti che fanno parte del Sistan e con il Comstat (Comitato di indirizzo e coordinamento dell'informazione statistica).

Nel promovimento di regole deontologiche, il Garante è tenuto altresì a individuare le categorie interessate, invitandole a darne comunicazione all'Autorità, nel caso di specie unicamente i soggetti che fanno parte o partecipano al Sistan all'atto dell'entrata in vigore della deliberazione e fino all'adozione delle regole stesse (artt. 23, comma 2 e 24, comma 5 del regolamento interno).

L'Autorità ha inoltre definito i portatori di interesse qualificato: a) tutti i soggetti a cui è fatto obbligo di fornire dati all'Istat anche per le rilevazioni previste dal programma statistico nazionale (art. 7, d.lgs. n. 322/1989); b) gli interessati, nella misura in cui le regole deontologiche possono incidere sulla definizione della portata delle deroghe ai diritti di cui agli artt. 15, 16, 18 e 21 del RGPD; c) i soggetti che possono accedere, per il perseguimento di scopi scientifici, ai dati raccolti per scopi statistici in ambito Sistan. Tali soggetti sono stati invitati, a dare comunicazione all'Autorità, entro il termine di 60 giorni dalla pubblicazione della deliberazione in G.U. e a fornire informazioni e

documentazione idonee a comprovare, in particolare, il proprio interesse qualificato alla materia (artt. 23, comma 3, del regolamento interno).

Con tale provvedimento sono stati evidenziati taluni ambiti che, in base alla più recente esperienza, necessitano di specifica regolamentazione (art. 25, comma 2, regolamento interno, artt. 2- *quater* e 106 del Codice). Ci si riferisce in particolare a:

i) criteri per la valutazione del rischio di identificazione degli interessati, affinché tengano maggiormente conto del principio di responsabilizzazione;
ii) casi in cui il titolare possa raccogliere dati personali presso un soggetto rispondente in nome e per conto di un altro (cd. *proxy*) ai sensi dell'art. 105, comma 3, del Codice;
iii) comunicazione a soggetti non facenti parte del Sistan, per ulteriori scopi di ricerca scientifica, per una maggiore armonizzazione con l'art. 5-*ter*, d.lgs. n. 33/2013 e con la direttiva n. 11/2018 del Comstat recante le linee guida per l'accesso a fini scientifici ai dati elementari del Sistan;
iv) conservazione dei dati, al fine di rendere in particolare chiari e prevedibili gli ulteriori trattamenti consentiti e definire, quindi, le ulteriori finalità e tempi di conservazione dei dati raccolti per il perseguimento di scopi statistici (art. 5, par. 1, lett. *b*), del RGPD);
v) dati raccolti per uno scopo statistico che possono essere trattati per altri scopi statistici di interesse pubblico quando essi siano chiaramente determinati e limitati nel tempo e di cui è stato adeguatamente informato l'interessato (art. 6-*bis,* comma 4, d.lgs. n. 322/1989);
vi) esercizio dei diritti spettanti agli interessati anche al fine di definire la portata delle deroghe eventualmente applicabili.

Il legislatore nazionale ha accordato un ruolo determinante alla statistica ufficiale nel corso dell'emergenza sanitaria da Covid-19, laddove all'art. 13, d.l. n. 34/2020, convertito con modificazioni in l. 7 luglio 2020 n. 77, recante misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da Covid-19, ha previsto che "in considerazione dell'emergenza epidemiologica da Covid-19 e della necessità e urgenza di disporre di statistiche ufficiali tempestive, affidabili e complete sul sistema economico e produttivo nazionale e sui fenomeni sociali, epidemiologici e ambientali, nonché ai fini di ricerche di mercato, sociali e di opinione, anche a supporto degli interventi di contrasto all'emergenza sanitaria e di quelli finalizzati alla gestione della fase di ripresa", l'Istat è autorizzato a trattare, eventualmente in contitolarità con altri soggetti che fanno parte o partecipano al Sistan, dati personali anche inerenti alle particolari categorie e relativi a condanne penali e reati, fino al termine dello stato di emergenza sanitaria, dichiarato con delibera del Consiglio dei ministri del 31 gennaio 2020 e per i dodici mesi successivi (artt. 9, par. 1 e 2, lett. *g*), 10 e 89 del RGPD; art. 2-*sexies,* comma 2, lett. *cc*), del Codice). La normativa prevede, in particolare, che, in una o più direttive del presidente dell'Istat, adottate previo parere del Garante, siano indicati gli specifici scopi perseguiti, i tipi di dati, le operazioni eseguibili, le misure e le garanzie adottate per tutelare i diritti fondamentali e le libertà degli interessati, le fonti amministrative utilizzate, anche mediante tecniche di integrazione, e i tempi di conservazione (art. 13, commi 2 e 3, d.l. n. 34/2020).

Il progetto è volto a "lo studio e l'analisi del fenomeno della diffusione del contagio da Covid-19, per individuare e proporre un sistema di rilevazione tempestiva del verificarsi di focolai epidemici, utilizzando i metodi statistici". Esso consta di due fasi: la prima è denominata fase accelerata o di addestramento, ed è volta alla "messa a punto del modello previsionale che valuti, sulla base dei parametri sotto specificati, l'insorgere o no di eventuali focolai epidemici".

7

A tal fine è prevista la raccolta, presso talune regioni, di dati aggregati su base di sezione censuaria, relativi, in particolare, a titolo di studio e occupazione al fine di "valutare eventuali correlazioni tra contesto socio-demografico e il propagarsi della pandemia". La realizzazione di tale modello inerisce alle funzioni istituzionali "di previsione e di analisi economica di breve, medio e lungo periodo, e di sviluppo di modelli di microsimulazione degli effetti delle politiche di bilancio su famiglie, imprese e istituzioni" che dall'Isae (Istituto di studi e analisi economica) sono state trasferite all'Istat.

La seconda fase del progetto, volta alla realizzazione di un sistema di allerta sanitario federato, totalmente automatizzato, finalizzato al contrasto e al contenimento della diffusione del Coronavirus attraverso l'elaborazione dei dati provenienti da una molteplicità di fonti, verrà sottoposta all'Autorità solo dopo aver verificato l'efficacia del modello predittivo che si intende realizzare.

In tale quadro, l'Istat ha richiesto al Garante il parere di competenza sullo schema di direttiva avente ad oggetto "uno studio preliminare relativo alla raccolta, analisi e diffusione di indicatori al fine di sviluppare un sistema di allerta per rilevare tempestivamente focolai epidemici attraverso l'analisi automatica dell'andamento di eventi indicativi di una situazione che si discosta dall'andamento normalmente rilevato", definito progetto *Alert*-Cov.

Il progetto, seppur apparentemente volto a trattare informazioni solo aggregate e anonime, riguarda in realtà dati personali, anche inerenti alle particolari categorie (art. 9 del RGPD) che devono trovare la loro base giuridica nella normativa di settore. Ciò in quanto le regioni sono chiamate ad effettuare operazioni di estrazione, aggregazione e comunicazione dei dati e l'Istat si troverà a trattare informazioni che, seppure aggregate, non escludono in radice il rischio di reidentificazione degli interessati (artt. 7, d.lgs. n. 322/1989 e 13, d.l. n. 34/2020). L'Istat ha indicato inoltre in sei mesi il tempo di conservazione dei dati, specificando che essi verranno trattati "in ambiente protetto e crittografato" e che, decorso tale termine, essi verranno cancellati attraverso una procedura "tracciata dal sistema di *ticketing* dell'Istituto".

Su tali basi, il Garante si è espresso positivamente sul richiamato schema di direttiva del presidente dell'Istat recante individuazione dei trattamenti dei dati personali di cui agli artt. 9 e 10 del RGPD nell'ambito del lavoro statistico *Alert*-Cov, limitandosi a prescrivere l'espunzione dallo schema di direttiva di impropri riferimenti riguardanti i termini di conservazione (provv. 24 giugno 2021, n. 249, doc. web n. 9681795).

Il Garante ha altresì formulato il parere di competenza sui lavori statistici IST-02729 Registro statistico di base degli edifici e delle unità abitative – volto proprio alla costituzione di tale Registro che "consta di due archivi che raccolgono informazioni rilevanti e funzionali, in particolare, al censimento della popolazione e delle abitazioni – e IST-02638 Integrazione dei dati di indagine su redditi, consumi e ricchezza delle famiglie – volto alla costituzione di un "set di microdati con distribuzioni congiunte relative alle variabili di reddito, consumo e ricchezza" – sui quali l'Autorità si era precedentemente espressa in termini non favorevoli nel parere sul Psn 2017-2019, aggiornamento 2018-2019 (provv. 9 maggio 2018, n. 271, doc. web n. 9001732, v. Relazione 2018, p. 89).

Il Registro statistico di base degli edifici e delle unità abitative (Ruie) inerisce a quella categoria di lavori statistici (registri o sistemi informativi) da sempre oggetto di particolare attenzione da parte del Garante perché prevede l'integrazione, su base pluriennale, non solo di fonti amministrative, ma anche di dati personali, talvolta anche sensibili, relativi ad ogni aspetto della vita quotidiana degli individui, raccolti presso gli interessati. Il Ruie rappresenta uno dei principali *asset* per la produzione

statistica, di cui il principale *output,* "ovvero la lista di edifici e delle relative unità immobiliari presenti sul territorio italiano, è ad uso interno ed è strumentale alla realizzazione del Censimento della popolazione e delle abitazioni".

I dati sono trattati in forma pseudonimizzata e sono conservati per 120 anni, al fine di completare le operazioni di validazione e di confronto rispetto alla precedente rilevazione censuaria.

Per il lavoro IST-02638 "Integrazione dei dati di indagine su redditi, consumi e ricchezza delle famiglie" attualmente in fase di progettazione, l'Istat ha modificato per PSN 2020-2022 la denominazione che risulta ora "Integrazione dei dati di indagine su redditi, consumi e ricchezza delle famiglie". Il lavoro statistico in esame è volto al perseguimento di due finalità: i) sviluppare metodi statistici di integrazione dei microdati provenienti da archivi amministrativi e indagini; ii) creare una base integrata di microdati sui redditi, i consumi e la ricchezza delle famiglie in Italia, su base campionaria, a partire dalle informazioni provenienti dalle indagini sociali e dagli archivi amministrativi disponibili, nell'ottica di analizzare le condizioni economiche delle famiglie in modo multidimensionale. Tali dati sono essenziali all'implementazione di misure politiche di contrasto e riduzione delle disuguaglianze nella distribuzione dei redditi individuali e familiari.

A tal fine, l'Istituto non solo acquisisce dati presso gli archivi amministrativi di titolarità del Mef e dati ad uso pubblico, ma riutilizza specifiche variabili già raccolte nell'ambito di precedenti indagini dirette o di altre basi dati statistiche quali l'indagine sulle condizioni di vita (EU-SILC); l'indagine sulle spese delle famiglie; alcune fonti amministrative e statistiche disponibili nel Sistema integrato di microdati dell'istituto (SIM); i dati sui bilanci delle famiglie italiane (Ibf) della Banca d'Italia. Il lavoro si articola in 3 fasi di trattamento. In una prima fase sono raccolti dati derivanti dalle richiamate fonti e integrati nella base dati del lavoro in esame per la costituzione di una base campionaria più ampia all'interno del quale ogni singolo individuo è ricondotto al proprio nucleo familiare attraverso l'utilizzo del codice SIM. La seconda fase è volta alla creazione di un data base condiviso con la Banca d'Italia che svolge in autonomia uno studio statistico sui dati rilasciati da Istat, ai sensi dell'art. 21 del regolamento (CE) 11 marzo 2009, n. 223/2009. Ciascun ente effettua nei propri *server* dedicati il test delle metodologie di *statistical matching* più idonee alla produzione di indicatori sulle distribuzioni congiunte del reddito, dei consumi e della ricchezza. La terza fase è volta alla costituzione di un nuovo *data set* basato su una diversa distribuzione dei dati (distribuzione bivariata di reddito e consumo, reddito e ricchezza, consumo e ricchezza e trivariata reddito, consumo e ricchezza).

Il tempo di conservazione è stato indicato in 240 mesi, salva la precisazione che quando la produzione statistica sarà a regime, saranno anche valutate le condizioni per ridurre il tempo di conservazione dei dati, almeno nella fase 1, a 120 mesi.

Con riferimento al principio di esattezza del dato, per mitigare il rischio di non rappresentatività del campione, l'Istituto ha garantito che le informazioni saranno elaborate solo quando la numerosità campionaria sarà non inferiore a soglie predeterminate.

Su tali basi e tenuto conto dei chiarimenti forniti dall'Istituto in particolare nelle valutazioni d'impatto redatte ai sensi dell'art. 35 del RGPD e che non erano rinvenibili nella precedente documentazione, il Garante si è espresso in termini favorevoli sui lavori in esame, limitandosi a formulare specifiche prescrizioni volte ad assicurare maggiore coerenza ai prospetti informativi da inserire nel Psn (provv. 8 luglio 2021, n. 261, doc. web n. 9689672).

L'Istat ha richiesto il parere del Garante sullo schema di Programma statistico

7

nazionale 2020-2022, Aggiornamento 2021-2022 (Psn o Programma), ai sensi dell'art. 6-*bis,* comma 1-*bis,* d.lgs. 322/1989 e dell'art. 4-*bis* delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistan, all. A4 al Codice.

Il Garante ha, in primo luogo, evidenziato che a seguito degli avvertimenti in precedenza formulati, ai sensi dell'art. 58, par. 2, lett. *a*), del RGPD, con il parere 10 dicembre 2020 sul Psn 2020-2022 (provv. 16 settembre 2021, n. 315, doc. web n. 520567), è stata intrapresa una collaborazione informale con l'Istituto per semplificare e razionalizzare le schede del Psn in vista della prossima programmazione triennale (2023-2025). Ciò, in quanto esso funge sia da base giuridica per il trattamento dei dati personali per scopi statistici (artt. 6, par. 3, lett. *b*); 9, lett. *g*), del RGPD, artt. 2-*ter* e 2-*sexies* del Codice, artt. 6-*bis,* comma 1-*bis* e 13, d.lgs. n. 322/1989), sia da informativa agli interessati in relazione ai dati raccolti presso soggetti terzi (cons. 41 e art. 5, par. 1, lett. *a*), del RGPD e art. 6 delle regole deontologiche).

In riferimento ai lavori statistici che comprendono il trattamento di dati relativi a condanne penali e reati, il Garante ha ribadito che, in base all'art. 2-*octies* del Codice, il trattamento (art. 10 del RGPD) è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano 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, da adottarsi, ai sensi dell'art. 17, comma 3, l. n. 400/1988, sentito il Garante. Nelle more dell'adozione di tale decreto ministeriale, in assenza di altra disposizione di legge o regolamento, non si è rinvenuta un'adeguata base normativa che legittimi il trattamento dei predetti dati per fini statistici. A tale riguardo, è stato segnalato che, con provvedimento 24 giugno 2021, n. 247 (doc. web n. 9682603), l'Autorità ha 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.

Nel parere in esame l'Autorità, alla luce degli avvertimenti precedentemente formulati, ha riconosciuto una maggiore chiarezza dell'esposizione degli obiettivi del trattamento statistico indicati nei prospetti informativi contenuti nel Psn, nonché dell'indicazione che in relazione ai trattamenti svolti per la produzione della statistica ufficiale, nel rispetto dell'art. 89 del RGPD, non sussiste per gli interessati il diritto di opposizione, ai sensi e nei limiti di cui all'art. 21, par. 6, del RGPD.

Il Garante ha dato atto, inoltre, che l'"Istituto ha previsto che, prima dell'indicazione dei lavori statistici di titolarità di un determinato soggetto Sistan, nel Psn siano indicate le misure implementate da ciascuno di essi, ribadendo (cfr. provv. 13 febbraio 2020, n. 29, doc. web n. 9283929, punto 1.2., v. Relazione 2020, p. 115 e ss) però che risulta necessario indicare le misure tecniche e organizzative previste per il trattamento di dati personali per scopi statistici, con particolare riferimento all'impiego di quelle volte a garantire il rispetto del principio di minimizzazione attraverso tecniche di pseudonimizzazione (art. 89 del RGPD).

L'Autorità ha rilevato inoltre una persistente criticità nell'indicazione nei prospetti informativi delle modalità di trattamento dei dati, ivi inclusa la conservazione, ribadendo che la specificazione di trattamenti che possono essere definiti come intermedi risulta superflua se non addirittura fuorviante, soprattutto laddove viene indicata l'immediata anonimizzazione dei dati in lavori statistici che prevedono tempi più lunghi di conservazione. Il Garante ha ribadito quindi che è sufficiente e auspicabile in termini di trasparenza, che il titolare del trattamento da una parte indichi le misure implementate per dare attuazione al principio di minimizzazione e

dall'altra definisca il tempo di conservazione o di ulteriore conservazione (art. 6-*bis*, comma 4, d.lgs. n. 322/1989) dei dati in una forma che – anche indirettamente – consenta la reidentificazione dell'interessato.

Il Garante ha evidenziato, inoltre, come nel Psn in esame vi fossero taluni lavori statistici nei quali è prevista l'acquisizione di dati "provenienti da precedenti trattamenti statistici" ovvero da "fonti amministrative", rilevando come talvolta nella elencazione delle principali variabili da acquisire oltre al codice pseudonimo, cd. SIM, è indicato, altresì, il nome e il cognome dell'interessato, con ciò sostanzialmente vanificandosi il rispetto dei principi di minimizzazione e di sicurezza dei dati perseguiti attraverso la misura della pseudonimizzazione.

Al riguardo, è stato ribadito come i dati direttamente identificativi (quali il nome e cognome) debbano essere disaccoppiati e conservati separatamente dal codice pseudonimo attribuito alle singole unità statistiche. Ciò posto, l'Autorità prescritto, ai sensi dell'art. 58, par. 3, lett. *c*), del RGPD e dell'art. 2-*quinquiesdecies* del Codice (ora abrogato ai sensi d.l. n. 139/2021, convertito, con modificazioni, in l. n. 205/2021) di eliminare l'indicazione del nome e cognome degli interessati.

Il Garante si è riservato poi di avviare una specifica istruttoria sui numerosi lavori statistici di titolarità di altrettante regioni/provincie autonome volti alla realizzazione di studi longitudinali sulle disuguaglianze di salute determinate da differenze socioeconomiche (CAM-00001; EMR-00019; LAZ-00006; LOM-00002; PAB-00041; PUG-00001; RSI00004; TOS-00013). Si tratta di lavori tesi a individuare e valutare, tramite misure epidemiologiche, eventuali differenze di salute tra gruppi di popolazione con diversa condizione demografica, socioeconomica e ambientale e a fornire indicazioni per programmare idonei interventi volti a rimuovere condizioni sfavorevoli di vita e a tutelare i gruppi svantaggiati. Ciò anche al fine di costituire un sistema di sorveglianza di eventi sanitari in rapporto a fattori demografici, socioeconomici e ambientali. L'intendimento del Garante nasce non solo dalle specifiche implicazioni di tali lavori statistici sui diritti e le libertà fondamentali degli interessati ma anche, in termini più specifici, perché solo in alcune delle schede relative ai richiamati lavori è riportata una sintesi delle tecniche di pseudonimizzazione che le regioni intenderebbero implementare per lo svolgimento di tali studi.

Il Garante ha prescritto poi di espungere dallo schema di Psn il prospetto informativo relativo al lavoro statistico IAP-00019 *European Social Survey* in quanto, a seguito di un'approfondita attività istruttoria, l'Inapp, in qualità di titolare, ha rappresentato che non intende effettuare tale trattamento nell'ambito del Sistan, bensì conformemente alla disciplina relativa al trattamento dei dati personali per scopi di ricerca scientifica (art. 89 del RGPD; art 104 e ss. del Codice; regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, all. A5 al Codice).

In relazione al lavoro, IFT-00001 Audimob - Indagine su stili e comportamenti di mobilità dei residenti in Italia di titolarità dell'Istituto superiore di formazione e ricerca per i trasporti spa, consistente in una statistica da indagine volta a indagare la mobilità attraverso l'osservazione del fenomeno degli spostamenti sul territorio, il Garante ha prescritto, invece, di eliminare il riferimento alla raccolta del consenso degli interessati. L'Autorità ha evidenziato, infatti, che in base all'art. 5 delle regole deontologiche di settore, all. A4 al Codice la garanzia del consenso è richiesta esclusivamente nelle ipotesi in cui il lavoro statistico comporti il trattamento di particolari categorie di dati (art. 9, par. 4, del RGPD).

L'Autorità si è soffermata poi sul lavoro IST-02733 indagine sui centri antiviolenza e sui centri e servizi per le vittime della tratta volta a "fornire una rappresentazione dei servizi offerti e delle caratteristiche degli utenti dei servizi a livello nazionale da parte dei centri antiviolenza pubblici e privati al fine di orientare interventi di

7

policy". Nella sezione "descrizione sintetica" di tale lavoro statistico risultava indicata come finalità ultima dello stesso quella di "costruire un percorso che individui le strategie di uscita della violenza".

Al riguardo, il Garante, pur riconoscendo che i dati di tale elaborazione statistica costituiscono certamente un valido supporto affinché i centri antiviolenza possano orientare al meglio le strategie e i percorsi di uscita dalla violenza delle vittime, ha evidenziato come la finalità perseguita dall'Istat non possa che essere meramente statistica, in virtù del cd. divieto di ricadute amministrative di cui all'art. 105 del Codice, in base al quale "i dati personali trattati a fini statistici o di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per scopi di altra natura". L'Autorità ha quindi prescritto che il prospetto informativo del lavoro in esame sia modificato tenendo in considerazione il richiamato principio ed eliminando l'indicazione di finalità non prettamente statistiche.

Infine il Garante ha sottolineato come vi siano altre p.a. che condividono caratteristiche simili a quelle dell'Istituto in termini di raccolta massiva e rielaborazione complessa di dati personali anche riferiti a particolari categorie per scopi statistici, quale l'Inps. A tali enti l'Autorità ha raccomandato di tenere conto dei provvedimenti adottati dal Garante nei confronti dell'Istat, per una adeguata implementazione dei principi applicabili con particolare riguardo (art. 89 del RGPD) al principio di esattezza del dato (soprattutto con riferimento alla definizione dei campioni) e di responsabilizzazione e degli obblighi di *privacy by design* e *by default* (artt. 5, par. 1, lett. *d*) e par. 2; 24 e 25 del RGPD); all'implementazione di adeguate tecniche di pseudonimizzazione e di aggregazione dei dati, individuando le specifiche metodologie applicate per valutare il rischio di reidentificazione degli interessati (provv.ti 23 gennaio 2020, n. 10, doc. web n. 9261093; 13 febbraio 2020, n. 29, doc. web n. 9283929; 19 maggio 2020, n. 87, doc. web n. 9370217).

Nell'ambito dei provvedimenti rilevanti nel settore della statistica ufficiale, si segnala infine il parere sullo schema di protocollo di intesa tra Istituto nazionale di statistica e Acquirente Unico spa (AU) per la regolamentazione dell'acquisizione da parte di Istat dei dati sui consumi di energia elettrica e gas.

La legge di bilancio per il 2018 aveva previsto che il censimento della popolazione diventasse, da quel momento, un censimento permanente effettuato con cadenza annuale anche attraverso l'utilizzo integrato di fonti amministrative e di altre fonti di dati indicate nella medesima legge (art. 1, commi 227 e 228, l. 27 dicembre 2017, n. 205, bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020).

In tale nuovo contesto, tra le banche dati utilizzabili a fini censuari è annoverato il Sistema informativo integrato (SII) di AU per la raccolta di dati sui consumi di energia elettrica e gas. Tale acquisizione deve essere disciplinata da un protocollo d'intesa tra l'Istat e AU, adottato sentiti l'Arera, il Garante per la protezione dei dati personali e l'Agcm. Pertanto, l'Istat ha presentato l'istanza per l'acquisizione del previsto parere sul protocollo d'intesa predisposto congiuntamente con AU.

In via prioritaria, il Garante ha ricordato di avere già segnalato al Parlamento forti criticità, sotto i profili della necessità e proporzionalità, sul disegno di legge che prevedeva che i dati personali raccolti nel SII di AU fossero utilizzati a scopi censuari, per la delicatezza delle informazioni in esso contenute. Infatti, i dati sui consumi individuali per fascia oraria di energia e gas risultano astrattamente idonei a rivelare informazioni anche sullo stato di salute delle persone interessate (come quelle riferite a macchinari salvavita) oltre che essere indici di presenza di un individuo presso un determinato domicilio (cfr. segnalazione concernente le disposizioni in materia di

censimenti permanenti di cui al disegno di legge di bilancio, 7 novembre 2017, doc. web n. 7447536).

Il legislatore ha ritenuto comunque necessario l'esame dei predetti dati a scopi censuari, ma ha deferito agli operatori del settore l'individuazione in concreto delle specifiche tipologie di informazioni a tal fine necessarie, ribadendo l'indispensabilità di un preventivo parere del Garante.

A tale riguardo, il Garante in termini generali ha ritenuto che, un ulteriore parametro per l'individuazione dei dati da trattare in concreto vada rinvenuto altresì nella numerosità delle banche date utilizzate a scopi censuari. In tal modo affermando, in altri termini, che quanto maggiore è il numero delle basi di dati utilizzate tanto più rigoroso deve essere il controllo sull'indispensabilità di ciascuna delle informazioni che si intende acquisire (art. 5, par. 1, lett. *c*), del RGPD), essendo altresì evidente che l'impiego di numerose banche dati riduce il rischio che il conteggio statistico della popolazione sia caratterizzato da discostamenti rilevanti rispetto alla realtà fattuale.

Ciò premesso, è stato evidenziato che il d.l. 8 luglio 2010, n. 105 recante misure urgenti in materia di energia, convertito con modificazioni in legge dall'art. 1, comma 1, legge 13 agosto 2010, n. 129, ha previsto l'istituzione del SII per la gestione dei flussi informativi relativi ai mercati dell'energia elettrica e del gas, basato su una banca dati dei punti di prelievo e dei dati identificativi dei clienti finali presso AU, disponendo che le modalità di gestione dei flussi informativi attraverso il SII siano stabilite dall'Arera. In particolare, la richiamata legge prevede che "Nel rispetto delle norme stabilite dal Garante per la protezione dei dati personali, l'Autorità per l'energia elettrica e il gas adotta specifici criteri e modalità per il trattamento dei dati personali e sensibili" (art. 1-*bis,* comma 3). Tuttavia, il Garante ha sottolineato in termini critici come Arera non abbia, allo stato, sottoposto alcun atto per i profili di competenza.

Il Garante ha quindi sottolineato l'importanza di assicurare in tale contesto la proporzionalità e l'esattezza dei dati trattati.

L'Autorità ha ribadito le gravi incompatibilità con la normativa in materia di protezione dei dati personali che deriverebbero da ipotetiche ricadute amministrative sui singoli individui in caso di puntuale revisione delle anagrafi della popolazione residente fondata sull'elaborazione automatizzata dei dati contenuti negli archivi dell'Istat. Di qui l'obbligo per l'Istat di restituire ai comuni, a seguito del censimento permanente, solo dati aggregati (art. 22, comma 7, d.lgs. n. 101/2018). Infatti, i dati trattati per scopi statistici non possono essere utilizzati per altre finalità, né comportare ricadute personalizzate sugli interessati (cons. 162 del RGPD, art. 105 del Codice. Cfr. *ex multis,* pareri 15 ottobre 2015, n. 536, doc. web n. 4481301 e 29 ottobre 2015, n. 566, doc. web n. 4476104).

Con specifico riguardo al protocollo presentato il Garante ha, in particolare, richiesto che tutte le volte in cui in esso si fa riferimento ad eventuali modifiche o integrazioni dello stesso (anche dell'allegato) il medesimo protocollo deve essere nuovamente sottoposto al parere del Garante. Inoltre, per specifiche esigenze di chiarezza e trasparenza, è stato necessario che nel protocollo fosse indicato il ruolo di titolare del trattamento di AU dei dati personali contenuti nel SII (art. 24 del RGPD), ciò in base all'art. 1, comma 228, lett. *e*), l. n. 205/2017, come peraltro riconosciuto dal Garante nel provvedimento 20 giugno 2019, n. 131 (doc. web n. 9123551).

L'Autorità ha poi escluso che il protocollo potesse riguardare la raccolta di altri dati da parte di Istat presso AU o viceversa la fornitura di dati a tale società, dovendo tali ulteriori flussi di dati trovare attuazione in base alla normativa di settore (cfr. artt. 6-*bis,* d.lgs. 322/1989 e 4-*bis* delle regole deontologiche per trattamenti a fini

7

statistici o di ricerca scientifica effettuati nell'ambito del Sistan, all. A4 al Codice; cfr. provv.ti 28 ottobre 2021, n. 382, doc. web n. 9721273 e 15 ottobre 2015, n. 536, doc. web n. 4481301, d.P.C.M. 12 maggio 2016).

Il protocollo prevede che AU provveda a fornire i dati di consumo con una cadenza almeno annuale sia in riferimento al settore gas naturale che al settore elettrico-mercato libero, in relazione ad ogni singolo intestatario del contratto di fornitura di energia elettrica e gas. Ciò posto, l'Autorità ha accolto con favore la previsione di raccogliere dati aggregati a livello mensile, ritenendo tale misura idonea ad assicurare l'effettiva applicazione del principio di proporzionalità e un equo bilanciamento dei diritti e degli interessi coinvolti, in quanto attenua l'ingerenza nella vita privata di ogni cittadino senza tuttavia incidere sull'efficacia della rilevazione.

È stato notato, però come limitatamente alle informazioni relative al settore dell'energia, fosse prevista la raccolta, per ogni interessato anche dei consumi suddivisi per fascia oraria. Sul punto, è stata rilevata l'assoluta aleatorietà dell'utilità di questa informazione di dettaglio rispetto allo scopo censuario perseguito, considerato che gli orari di maggior consumo di energia elettrica possono essere determinati in base agli stili di vita degli interessati nonché alla tipologia di contratto stipulato con il fornitore. Il Garante ha sottolineato, inoltre, come tale trattamento comporti una forte ingerenza nella vita privata degli interessati, in quanto idonea a indicarne le abitudini di consumo. Tale tipologia di disaggregazione è stata ritenuta sproporzionata, sicché l'Autorità ha prescritto l'espunzione dall'all. A del Protocollo d'intesa, relativo alla raccolta di questa informazione (provv. 16 dicembre 2021, n. 434, doc. web n. 9738899).

Al di fuori dell'ambito della statistica ufficiale, merita segnalarsi il provvedimento, adottato ai sensi dell'art. 2-*ter,* comma 2, del Codice, nella versione antecedente alla modifica occorsa ad opera del d.l. n. 139/2021, convertito con modificazioni in legge n. 205/2021.

Un comune aveva inviato una comunicazione al Garante, al fine di poter fornire alcuni dati personali, diversi da quelli di cui agli artt. 9 e 10 del RGPD, estratti da banche dati amministrative (Imu e Tari), ad un'università che ne aveva fatto richiesta per la realizzazione di un progetto pilota di ricerca sul turismo residenziale. Ciò, in quanto tale flusso di dati non risultava espressamente previsto da alcuna specifica base normativa.

Lo studio risultava finalizzato alla predisposizione di una metodologia e alla sua implementazione per la rilevazione dei flussi turistici nelle case vacanze a livello regionale. Nello specifico, il progetto prevedeva non solo raccolta dei predetti dati amministrativi per la composizione di un campione statistico rappresentativo di proprietari – di prime e seconde case – e di residenti ma anche la successiva richiesta ai proprietari di immobili a destinazione turistica, di collaborare tenendo un diario sull'uso delle abitazioni, annotando gli arrivi e le partenze.

Concernendo la questione un trattamento di dati per scopi di ricerca scientifica, il Garante ha, in primo luogo, verificato che il trattamento descritto nell'istanza afferisce allo svolgimento delle funzioni istituzionali dell'ateneo e che i dati richiesti sono al tal fine pertinenti, in omaggio ai principi di liceità, di limitazione della finalità e di minimizzazione (art. 5, par. 1, lett. *a*), *b*) e *c*), del RGPD).

L'Autorità ha verificato inoltre sia le metodologie applicate ai fini dell'individuazione del campione di riferimento, in conformità al principio di esattezza dei dati (art. 5, par. 1, lett. *d*), del RGPD), sia la loro adeguatezza, tenuto conto anche del contesto e dello stato dell'arte, delle misure di pseudonimizzazione di cui si proponeva l'adozione, ai sensi dell'art. 89 del RGPD, nonché dei principi di correttezza e trasparenza, ai sensi dell'art. 5, par. 1, lett. *a*), del RGPD.

7

All'esito di tali verifiche, il Garante, nel determinare, ai sensi dell'artt. 36, par. 5, del RGPD e 2-*ter,* comma 2, del Codice, che l'amministrazione comunale potesse comunicare all'università i dati personali dalla stessa richiesti, ha formulato due specifiche ingiunzioni, ai sensi degli artt. 58, par. 2, lett. *d*), del RGPD e 2-*ter,* comma 2, del Codice. In particolare, è stato prescritto che l'università procedesse all'immediata cancellazione dei dati personali eccedenti rispetto a quelli necessari per la costituzione del campione statistico nonché dei dati personali degli interessati contattati telefonicamente non intenzionati ad aderire volontariamente al progetto di ricerca, e di integrare le informazioni da rendere oralmente nel corso della telefonata, con tutti gli elementi di cui all'art. 13 par. 1, del RGPD, usando un linguaggio semplice e chiaro, secondo quanto previsto all'art. 12, par. 1, del RGPD, rimandando espressamente alle informative complete disponibili sui siti web del comune e dell'università (provv. 25 marzo 2021, n. 110, doc. web n. 9586888).

8 I trattamenti in ambito giudiziario e da parte di Forze di polizia

8.1. *I trattamenti in ambito giudiziario*

Produzione di dati in giudizio

Diversi reclami hanno riguardato la legittimità della produzione di informazioni in giudizio in relazione alla normativa in materia di protezione di dati personali. Secondo un consolidato orientamento, l'Autorità ha precisato che spetta al Giudice, ove ritualmente richiesto, la competenza a valutare la liceità del trattamento in giudizio dei dati personali dell'interessato. Ciò in quanto 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 conformi a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali (si vedano i provvedimenti del Garante assunti con riferimento all'art. 160, comma 6, del previgente testo del Codice, di contenuto pressoché identico a quello dell'attuale art. 160-*bis,* del Codice: provv.ti 23 settembre 2010, doc. web n. 1756065; 4 novembre 2010, doc. web n. 1770943; 17 novembre 2010, doc. web n. 1779765).

L'Autorità ha esaminato un complesso reclamo nel quale i dati dell'interessata sono stati oggetto di una circolazione all'interno di un giudizio, del quale era parte, essendo venuta a conoscenza che tra gli allegati della controparte vi era una memoria contenente proprie informazioni prodotta in un altro procedimento. Al riguardo il Garante, nel fornire ulteriori chiarimenti anche successivamente all'archiviazione del reclamo, ha precisato che, ai sensi del citato articolo 160-*bis* del Codice, la circolazione in giudizio dei dati personali (anche contenuti in prove costituite o costituende) è regolata dalle disposizioni processuali applicabili e che, in ordine all'utilizzo processuale dei dati personali e alla valutazione effettuatane dall'Autorità giudiziaria, la competenza dell'Autorità incontra il limite di cui all'art. 154, comma 7, del Codice, secondo il quale "il Garante non è competente per il controllo dei trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni" (nota 24 settembre 2021).

Trattamento per accertare, esercitare o difendere un diritto in sede giudiziaria

In relazione ad un reclamo concernente la lamentata redazione da parte di un avvocato di un pignoramento presso terzi (per un credito che una società assicuratrice dichiarava di vantare nei confronti del reclamante) in un'unica stesura inviata a tutti i soggetti individuati come terzi, l'Autorità ha rilevato che il trattamento dei dati era avvenuto ai fini dell'istaurazione di un processo di esecuzione mediante atto di pignoramento, nella fattispecie presso terzi (artt. 543 e segg. c.p.c.), e pertanto "in ambito giudiziario" e che in tali casi spetta al Giudice adito, ove ritualmente richiesto, la competenza a valutare la liceità del trattamento dei dati personali dell'interessato ai sensi dell'art. 160-*bis* del Codice.

Il Garante ha altresì precisato che la legittimità del trattamento dei dati per difendere un diritto in giudizio è assicurata, per le particolari categorie di dati, dall'art. 9, par. 1, lett. *f*), del RGPD, ai sensi del quale il trattamento è lecito se necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali e *a fortiori,* per tutti i dati personali, dall'art. 6, par. 1, lett. *f*), del medesimo RGPD il quale prevede che il trattamento è lecito se necessario per perseguire un interesse legittimo del titolare (note 22 gennaio, 15 giugno e 5 novembre 2021).

Trattamento da parte di un avvocato coinvolto in un procedimento giudiziario

In un reclamo è stato lamentato l'illecito trattamento di dati personali a seguito di uno scambio di *e-mail* tra un avvocato e una società. Nella specie la reclamante lamentava la divulgazione, da parte dell'avvocato, di informazioni concernenti il riconoscimento di paternità della figlia, elemento totalmente estraneo ai mandati conferiti e di nessun interesse per il destinatario della comunicazione. Al reclamo era allegato l'estratto di una denuncia nei confronti del medesimo avvocato, depositata dal coniuge della reclamante presso la Procura della Repubblica, nella quale si lamentava una violazione della disciplina in materia di protezione dei dati personali per la medesima vicenda oggetto del reclamo. L'Autorità ha chiarito, al riguardo, di non poter interferire con l'attività in corso dell'Autorità giudiziaria penale e di dover rispettare i diritti dei soggetti coinvolti (quali, ad es. la facoltà di non rendere dichiarazioni a sé pregiudizievoli, ex art. 64 c.p.p.), e quindi di non poter effettuare gli accertamenti indispensabili per assumere le determinazioni di competenza. Ciò, anche perché le verifiche necessarie per tali determinazioni sono condizionate dall'esito del procedimento penale, quanto meno in ordine all'accertamento dei fatti. Il reclamo è stato pertanto archiviato (nota 10 febbraio 2021).

Documenti relativi a procedure di composizione di "crisi da sovraindebitamento" indicizzati su internet

L'Autorità si è occupata della tutela della riservatezza dei dati personali di coloro che sono coinvolti nella procedura di composizione in tribunale delle "crisi da sovraindebitamento", disciplinata dalla legge 27 gennaio 2012, n. 3. In particolare, due interessati si sono rivolti al Garante lamentando che, digitando su Google il proprio nominativo, si veniva indirizzati ad un pdf contenente il ricorso (e la relativa documentazione allegata) per la liquidazione del patrimonio ex art. 14-*ter* della predetta legge n. 3/2012, da cui si ricavava una descrizione dettagliata della situazione economica dei ricorrenti, la composizione del nucleo familiare e, pertanto, i dati del figlio minore, nonché informazioni sullo stato di salute della reclamante. L'Autorità ha rappresentato che il trattamento effettuato dal tribunale, consistente nella divulgazione dei dati in questione per il tramite del sito istituzionale del medesimo tribunale, è disciplinato dal RGPD e dal Codice, applicabili anche ai trattamenti di dati personali effettuati dall'Autorità giudiziaria nell'esercizio di funzioni giurisdizionali diverse da quelle penali, pur con alcune deroghe previste, in particolare, dagli artt. 23, par. 1, lett. *f*), del RGPD e 2-*duodecies* del Codice. Si applicano, quindi, ai trattamenti in questione, tra gli altri, i principi di proporzionalità, non eccedenza e minimizzazione dei dati (cfr. art. 5 del RGPD, riconducibile peraltro agli artt. 8 CEDU e CDFUE), anche con riguardo ai dati relativi alla salute (cfr. art. 9 del RGPD e 2-*septies,* comma 8, del Codice). Si è rappresentato, altresì, che la medesima disciplina prevede che, al fine di salvaguardare l'indipendenza della magistratura nell'adempimento delle sue funzioni giurisdizionali (cfr. cons. 20 del RGPD), l'autorità di protezione dati (nella specie, il Garante) non è competente per il controllo dei trattamenti effettuati dalle Autorità giudiziarie nell'esercizio delle loro funzioni (cfr. artt. 55 par. 3, del RGPD e 154, comma 7, del Codice).

In merito, invece, al rinvenimento della documentazione sul menzionato motore di ricerca, si è rappresentato che la disciplina in materia di protezione dei dati personali consente all'interessato di esercitare i diritti di cui agli artt. 15 e ss. del RGPD direttamente nei confronti del motore di ricerca titolare del trattamento (come evidenziato dal Garante anche con un provvedimento su materia analoga a quella in esame, provv. 26 novembre 2020, doc. web n. 9522225 e con note 24 febbraio 2021).

Attività di investigazione privata

Il Garante ha ammonito una società di investigazione privata che, incaricata di verificare la correttezza della condotta di una lavoratrice in merito alla fruizione di permessi retribuiti giustificati dalle condizioni di salute della madre, ha riportato nel rapporto investigativo l'indicazione della specifica malattia di cui presumibilmente quest'ultima era affetta. Il Garante ha ritenuto che, seppure l'incarico investigativo

comportava la necessità di accertare se i permessi fossero effettivamente finalizzati all'assistenza della madre, onde le informazioni relative ad un suo possibile stato patologico apparivano conferenti all'oggetto del mandato (art. 9, par. 2, lett. *f*), del RGPD), purtuttavia, l'indicazione della specifica malattia non aveva alcuna rilevanza ai fini dell'espletamento degli accertamenti commissionati all'investigatore e la loro ostensione ha quindi comportato la violazione dell'art. 5, comma 1, lett. *c)*, del RGPD, secondo cui i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Sulla base dei criteri indicati dall'art. 83 del RGPD, considerando che la condotta aveva esaurito i suoi effetti, che il trattamento di dati personali relativi allo stato di salute era legittimo ancorché eccedente, che il numero di interessati al trattamento era limitato ad uno, che non risultavano eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento né elementi tali da fare ritenere il carattere doloso della condotta dell'agente, il Garante ha ritenuto che nel caso di specie non ricorressero i presupposti per infliggere una sanzione amministrativa pecuniaria (provv. 16 settembre 2021, n. 334, doc. web n. 9718933).

Procedimento amministrativo innanzi alla Commissione per l'accesso ai documenti amministrativi

Il Garante ha ammonito una p.a. che, a fronte della richiesta di riesame di un diniego di accesso presentato da un suo dipendente alla Commissione per l'accesso ai documenti amministrativi, aveva comunicato alla Commissione stessa dati personali del reclamante ulteriori rispetto a quelli necessari a giustificare la mancata ostensione dei documenti richiesti. In particolare, l'amministrazione non si era limitata a rappresentare l'inesistenza degli atti richiesti dal dipendente – elemento sulla cui base la Commissione ha rigettato la richiesta di riesame – ma aveva aggiunto ulteriori informazioni sulla persona e personalità del medesimo. Il Garante ha ritenuto che tali ulteriori informazioni prodotte, prive di effettivo nesso con le questioni sottoposte alla competenza della Commissione, non rientrano nel margine di libertà di elaborare la propria tesi che va riconosciuto a chi è parte di un procedimento amministrativo giustiziale. Pertanto, il trattamento dei predetti dati personali è stato ritenuto non pertinente, in violazione dell'art. 5 del RGPD nonché privo delle condizioni legittimanti il trattamento dei dati personali di cui all'art. 6 del RGPD. Sulla base dei criteri indicati dall'art. 83 del RGPD, considerando che la condotta aveva esaurito i suoi effetti, che i destinatari della comunicazione si riducevano alla sola Commissione per l'accesso, che non risultavano a carico del titolare del trattamento precedenti violazioni pertinenti e che il titolare non aveva tratto alcun vantaggio economico dal trattamento, il Garante ha ritenuto che non ricorressero i presupposti per infliggere una sanzione amministrativa pecuniaria (provv. 11 novembre 2021, n. 398, doc. web n. 9725874).

8.2. *I trattamenti da parte di Forze di polizia*

Divulgazione di immagini cruenti diffuse durante una conferenza stampa

L'Autorità ha adottato un provvedimento sanzionatorio nei confronti del Ministero dell'interno per l'illecito trattamento di dati personali da parte di una questura, a seguito della divulgazione nelle pagine Facebook e Twitter di due video – contraddistinti dal logo della Polizia di Stato – originariamente realizzati dai trasgressori sulle atroci sevizie subite da un uomo, in occasione della comunicazione alla stampa delle avvenute operazioni di arresto di 8 giovani.

Dall'istruttoria è emerso che la diffusione dei video era stata effettuata per la prevenzione dei reati, non rilevando la circostanza che la Procura della Repubblica competente avesse autorizzato verbalmente il Ministero alla divulgazione agli organi di stampa dei menzionati video. Tale autorizzazione ha consentito soltanto di escludere

che la divulgazione di tali immagini fosse di per sé in violazione di legge o in grado incidere negativamente sui procedimenti penali in corso (cfr. artt. 114 e 329 c.p.p.). Seppur la finalità sottesa al trattamento in esame, ovvero quella della prevenzione dei reati, doveva ritenersi legittima, la divulgazione in questione è risultata illecita, in violazione degli artt. 3, comma 1, lett. *a*) e *c*) e 5, d.lgs. n. 51/2018 nonché 14, d.P.R. n. 15/2018, non solo perché non necessaria per la finalità di prevenzione dei reati, ma anche perché in pregiudizio della dignità dell'interessato, la cui tutela deve essere garantita anche dopo il decesso. In conseguenza, l'Autorità ha ingiunto al Ministero dell'interno, in qualità di titolare del trattamento, di pagare la somma di euro 75.000 a titolo di sanzione amministrativa pecuniaria (provv. 10 giugno 2021, n. 289, doc. web n. 9701975).

Divulgazione di notizie relative all'esecuzione di una misura cautelare detentiva nei confronti di un minorenne

In relazione ad un reclamo concernente un comunicato stampa dell'Arma dei Carabinieri relativo all'arresto di un minore e ritenuto lesivo del diritto alla riservatezza dell'interessato in quanto, pur non contenendone il nome, faceva espresso riferimento a dati riconducibili al medesimo arrestato e alla sua famiglia, l'Autorità ha ritenuto che il testo oggetto di reclamo non contenesse elementi tali da rendere identificabile il minore, tenuto conto che la realtà territoriale dove era avvenuta l'operazione di polizia era costituita da una comunità di circa 20 mila persone.

Ad ogni modo, con specifico riferimento alle modalità con cui vengono divulgate notizie riguardanti procedimenti giudiziari in cui sono coinvolti minorenni, anche ai sensi dell'art. 57, par. 1, lett. *d*), del RGPD, ha segnalato all'Arma dei Carabinieri l'opportunità di adottare la massima attenzione per far sì che l'informazione da parte delle Forze dell'ordine su procedimenti in corso, anche di rilievo pubblico, non vada a discapito dei diritti dei minori, in osservanza delle disposizioni di legge che vietano la divulgazione di notizie idonee a consentire l'identificazione dei minorenni comunque coinvolti in procedimenti giudiziari (cfr. artt. 114, comma 6, c.p.p.; 13, comma 1, d.P.R. 22 settembre 1988, n. 448; 50 Codice) (nota 8 febbraio 2021).

8.3. *Pareri su provvedimenti amministrativi o progetti in ambito giudiziario o in relazione ad attività di polizia*

Decreto ministeriale concernente la comunicazione all'autorità di p.s. delle persone alloggiate in strutture alberghiere

È stato richiesto il parere del Garante su uno schema di modifica del decreto del Ministro dell'interno 7 gennaio 2013, recante disposizioni concernenti la comunicazione alle autorità di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive, per l'adeguamento alle disposizioni successivamente intervenute (art. 5, d.l. 14 giugno 2019, n. 53, convertito, con modificazioni, dalla l. 8 agosto 2019, n. 77). Si ricorda che l'art. 109, r.d. 18 giugno 1931, n. 773 (t.u. delle leggi di pubblica sicurezza) prevede l'obbligo di comunicare le generalità degli alloggiati a carico dei gestori degli esercizi alberghieri e di tutte le altre strutture ricettive di qualunque tipo, nonché dei proprietari o gestori di case e di appartamenti per vacanze e degli affittacamere. Il Garante ha ritenuto non conforme alla disciplina in materia di protezione dei dati personali la previsione del raddoppio dei termini di conservazione dei dati raccolti dal sistema (dieci anni in luogo dei cinque previsti dalla normativa in vigore). Il Garante ha, infine, osservato trattarsi di un trattamento su larga scala, che comporta la raccolta, in forma massiva ed indiscriminata, dei dati personali attinenti ad eventi della vita privata di tutte le persone che soggiornano in strutture ricettive, sicché i relativi termini di conservazione devono contemperare le esigenze di tutela della riservatezza e quelle connesse all'attività di polizia, il cui punto di equilibrio è individuabile nel predetto termine quinquennale.

8

Decreto direttoriale recante specifiche tecniche del processo telematico civile e penale

Il Garante ha anche prescritto l'adozione di alcune misure tecniche e organizzative idonee a rendere il trattamento conforme alla disciplina rilevante in materia di protezione dei dati personali (provv. 8 luglio 2021, n. 300, doc. web n. 9690786).

La Direzione generale per i sistemi informativi automatizzati del Ministero della giustizia ha richiesto il parere del Garante su uno schema di provvedimento del direttore generale, recante le specifiche tecniche del processo telematico civile e penale, in attuazione di quanto previsto dall'art. 34, comma 1, del decreto del Ministro della giustizia 21 febbraio 2011, n. 44, e volto ad apportare modifiche ad un precedente provvedimento del 16 aprile 2014. Il Ministero ha presentato le modifiche in esame come necessarie per dare applicazione al decreto-legge 16 luglio 2020 n. 76, convertito, con modificazioni, dalla legge di conversione 11 settembre 2020 n. 120, recante misure urgenti per la semplificazione e l'innovazione digitale.

Lo schema di decreto apportava integrazioni al provvedimento del 2014, modificando, in particolare, l'art. 9-*bis* e aggiungendo l'art. 9-*ter,* al fine di consentire il censimento all'interno del registro generale degli indirizzi elettronici (ReGIndE) degli indirizzi di posta elettronica certificata (Pec) degli organi, delle articolazioni, anche territoriali e delle aree organizzative omogenee delle pubbliche amministrazioni. In dettaglio, lo schema prevedeva che ciascuna amministrazione pubblica comunicasse al Ministero la denominazione e il codice fiscale (o, in mancanza, il codice Ipa) dei propri organi o articolazioni, anche territoriali, presso cui eseguire, quando previsto, le comunicazioni o notificazioni per via telematica. Era inoltre previsto che gli elenchi dei predetti indirizzi Pec fossero consultabili dai soggetti abilitati, presso gli uffici giudiziari e gli uffici notificazioni, esecuzioni e protesti, e dagli avvocati.

Il Garante ha formulato un articolato parere fornendo all'Amministrazione numerose indicazioni (alcune a titolo di condizione) per il perfezionamento dello schema in senso conforme alle regole e alle garanzie previste dalla normativa in materia di protezione dati personali.

Tali indicazioni hanno riguardato, tra l'altro, i seguenti aspetti: definizione del codice Ipa (Indice dei domicili digitali delle p.a.) quale identificativo univoco assegnato a ciascun soggetto tenuto all'iscrizione; indicazione specifica della titolarità dei trattamenti effettuati; previsione di un obbligo di informazione reciproco fra diversi soggetti in caso di violazione dei dati personali; puntuale attuazione del principio di minimizzazione rispetto ai dati contenuti nell'oggetto delle Pec e introduzione di modalità selettive di accesso alle informazioni; previsione di un regolare riesame e aggiornamento delle misure tecniche e organizzative adottate dal Ministero, sulla base di una valutazione d'impatto sulla protezione dei dati; individuazione di misure tecniche ed organizzative volte a garantire l'integrità e la riservatezza dei dati personali trattati (provv. 15 aprile 2021, n. 134, doc. web n. 9590273).

Decreto direttoriale del Mef concernente il processo tributario telematico

Il Garante ha espresso parere favorevole su uno schema di decreto direttoriale, predisposto dal Mef, volto ad aggiornare l'utilizzo di strumenti informatici e telematici nel processo tributario, modificando alcuni aspetti del funzionamento del Sistema informativo della giustizia tributaria (S.I.Gi.T.), come le modalità di sottoscrizione dei documenti informatici, la verifica dei documenti stessi e l'utilizzo della firma digitale.

Nell'esprimere parere positivo, il Garante ha comunque richiesto all'amministrazione proponente di integrare lo schema di decreto al fine di assicurare maggiori tutele alla riservatezza dei dati delle persone interessate, adeguandolo alla normativa europea (RGPD) e nazionale (Codice) in materia di protezione dati, con particolare riferimento alla definizione delle responsabilità dei soggetti coinvolti nel trattamento dei dati e degli obblighi informativi in caso di violazione dei dati e alla previsione di

8

Progetto Sari *Real Time* del Ministero dell'interno

un periodico aggiornamento delle misure tecniche e organizzative adottate al fine di garantire un livello di sicurezza adeguato ai rischi presentati dai trattamenti (provv. 11 novembre 2011, n. 395, doc. web n. 9723857).

Il Garante ha espresso parere sfavorevole in merito ad un progetto denominato Sari *Real Time*, presentato dal Ministero dell'interno, concernente un sistema che, attraverso una serie di telecamere installate in un'area geografica pubblica predeterminata e delimitata (ad es. il luogo in cui si svolge una manifestazione pubblica), avrebbe consentito di analizzare in tempo reale i volti dei soggetti ivi presenti, confrontandoli con una banca dati predefinita per lo specifico servizio (denominata *watch-list*), con capienza massima di 10.000 volti. Ove fosse stata riscontrata, attraverso un algoritmo di riconoscimento facciale, una corrispondenza tra un volto presente nella *watch-list* ed un volto ripreso da una delle telecamere, il sistema sarebbe stato in grado di generare un *alert* per richiamare l'attenzione degli operatori. Premesso che il sistema in argomento, in quanto diretto a realizzare un trattamento di dati personali per finalità di *law enforcement,* è soggetto alla disciplina dettata dalla direttiva (UE) 680/2016 e dal d.lgs. n. 51/2018, il Garante ha verificato la mancanza di una base giuridica idonea a consentire il trattamento dei dati biometrici in argomento, ai sensi dell'art. 7 del predetto decreto. Ha inoltre osservato che il sistema avrebbe potuto realizzare un trattamento automatizzato su larga scala di dati riferiti a persone presenti a manifestazioni politiche e sociali non necessariamente oggetto di "attenzione" da parte delle Forze di polizia; ancorché la valutazione di impatto relativa al progetto indicasse che i dati di questi ultimi sarebbero stati immediatamente cancellati, nondimeno l'identificazione di una persona in un luogo pubblico avrebbe comportato il trattamento biometrico dei dati di tutte le persone circolanti nello spazio pubblico monitorato, al fine di generarne un "modello" da confrontare con quelli delle persone incluse nella *watch-list.* Pertanto, si sarebbe determinata una evoluzione della natura stessa dell'attività di sorveglianza: da sorveglianza mirata di alcuni individui a sorveglianza universale finalizzata all'identificazione di alcuni individui. Il Garante ha precisato che la base giuridica eventualmente da adottare avrebbe dovuto, in esito alla ponderazione di tutti i diritti e le libertà coinvolti, fra l'altro, rendere adeguatamente prevedibile l'uso di tali sistemi, in un quadro di garanzie tali da limitare la discrezionalità dell'utilizzo del sistema e conseguentemente del trattamento dei dati. Ciò, con riguardo ad alcuni aspetti fondamentali dell'impiego di tale tecnica di riconoscimento facciale, come, a titolo di mero esempio, i criteri di individuazione dei soggetti che possano essere inseriti nella *watch-list* o quelli per determinare i casi in cui può essere utilizzato il sistema, nonché i limiti delle tecniche in argomento, notoriamente basate su stime statistiche della corrispondenza tra gli elementi confrontati e, quindi, intrinsecamente fallibili, stimando le eventuali conseguenze per gli interessati in caso di falsi positivi (provv. 25 marzo 2021, n. 127, doc. web n. 9575877).

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

A seguito di segnalazioni ricevute, anche nel 2021 l'Autorità, nei limiti delle proprie competenze, ha assicurato il riscontro da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e di uffici periferici della Polizia di Stato alle richieste degli interessati, sia di accesso e comunicazione dei dati conservati presso il Ced, sia di eventuale rettifica dei dati medesimi, nel rispetto delle disposizioni previste dall'art. 10 della legge 1° aprile 1981, n. 121, come modificato dall'art. 175 del Codice.

8

8.5. *Il controllo sul Sistema di informazione Schengen*

Il Sistema d'informazione Schengen (SIS II) permette alle autorità nazionali doganali, di polizia e di controllo delle frontiere di scambiarsi agevolmente informazioni sulle persone che potrebbero essere coinvolte in reati gravi. Con l'eliminazione dei controlli alle frontiere interne, il SIS II svolge un ruolo essenziale nel facilitare la libera circolazione delle persone nello spazio Schengen. Nel Sistema sono inoltre contenute anche 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. La valutazione Schengen dell'Italia

Nel 2021 ha avuto luogo (dal 12 al 17 settembre) la quarta valutazione *Schengen* dell'Italia relativa al settore della protezione dei dati. Il Gruppo di valutazione, formato da esperti designati delle autorità di protezione dati di Paesi Schengen e della Commissione europea in base al nuovo meccanismo previsto dal regolamento (UE) 1053/2013, ha provveduto, attraverso visite *in loco,* a verificare il grado di attuazione dato alle disposizioni del regolamento (CE) 1987/2006 e della pertinente decisione 2007/533/GAI del Consiglio che disciplinano il funzionamento del sistema informativo Schengen, nonché del regolamento (CE) 767/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008, che regola il sistema informativo visti (VIS), istituito dalla decisione 2004/512/CE del Consiglio dell'8 giugno 2004. Una intera giornata è stata dedicata al Garante che, in qualità di autorità competente per la supervisione nazionale del Sistema informativo Schengen II e del Sistema informativo visti (VIS), ha illustrato la propria struttura, i poteri e le competenze, nonché le attività di verifica e controllo svolte con riferimento alla legittimità del trattamento dei dati operato dai due titolari del trattamento dei sistemi in questione: Ministero dell'interno e Ministero degli affari esteri, ivi comprese le verifiche svolte in alcuni consolati per quanto riguarda il VIS. Inoltre, sono stati trattati i temi dell'esercizio dei diritti di accesso, rettifica, cancellazione e della cooperazione con le altre autorità di protezione dei dati dei Paesi Schengen laddove la richiesta riguardi segnalazioni inserite da altri Paesi, diritti dell'interessato e modalità del loro esercizio, nell'ambito del rilascio dei visti e modalità di informazione degli interessati, misure di sicurezza e regole dei *log.*

Nel prosieguo delle verifiche, alle quali hanno partecipato anche rappresentanti dell'Autorità, il Gruppo di valutazione si è recato presso i due Ministeri, che hanno illustrato modalità di applicazione del quadro normativo europeo per i profili relativi alla protezione dei dati personali Al termine della visita il Gruppo ha predisposto un rapporto che, come da prassi, è stato sottoposto alle osservazioni del Garante e delle altre Autorità interessate. Il rapporto, una volta discusso nei gruppi competenti della Commissione e del Consiglio europei, sarà adottato dal medesimo Consiglio.

8.5.2. L'attività di controllo e monitoraggio del Garante sul Sistema SIS II

Il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nel SIS II, in virtù delle quali 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).

Al riguardo, il Ministero invia trimestralmente *report* statistici, privi di dati di natura personale, contenenti informazioni di dettaglio (nazionalità dei richiedenti, questure coinvolte, tipologia delle richieste, ecc.), idonee a monitorare il flusso delle istanze degli interessati e la conseguente attività di riscontro compiuta dalla Divisione

NSIS, in conformità con la raccomandazione formulata all'esito della precedente valutazione sull'applicazione dell'*acquis* di Schengen.

Tali *report* sono strumentali alla finalità istituzionale del Garante di assicurare il controllo e il monitoraggio del Sistema, con particolare riguardo all'esercizio dei diritti previsti dal regolamento (CE) 1987/2006 da parte degli interessati.

Nel corso del 2021, con ogni evidenza anche in ragione delle condizioni relative alla pandemia da Covid-19, si è assistito ad un parziale calo del numero delle richieste degli interessati indirizzate direttamente al Garante rispetto all'anno precedente; tra queste sono risultate costanti in termini percentuali quelle di interessati i quali lamentano un insoddisfacente o erroneo riscontro alle proprie richieste da parte dell'autorità nazionale di polizia e, pertanto, ricorrono al Garante al fine di vederle soddisfatte.

Infine, anche qui con ogni probabilità in conseguenza della pandemia, si è assistito ad un moderato ma costante calo delle richieste di accesso da 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 agli interessati, previa consultazione degli uffici segnalanti, per quanto consentito dalle disposizioni di cui all'art. 62 della decisione 2007/533/ GAI del Consiglio e all'art. 46 del regolamento (CE) n. 1987/2006.

9 L'attività giornalistica

Grande attenzione ha continuato ad essere dedicata ai profili legati alla libertà di manifestazione del pensiero e alla ricerca di un punto di equilibrio tra la libertà di informazione e il diritto ad essere informati, da un lato, e la protezione dei dati personali e il rispetto dell'identità personale, dall'altro. Ciò è avvenuto attraverso l'esame dei numerosi reclami e delle segnalazioni volti a lamentare lesioni del diritto alla riservatezza ad opera degli organi di informazione, anche per effetto della sempre più ampia (e prevalente) diffusione delle notizie sulla rete e sui *social media.*

9.1. *Dati statistici ed aspetti procedurali*

Le istanze all'Autorità nel settore in esame sono pervenute, in numero sostanzialmente paritario, sotto forma di reclami formali (per i quali, in taluni casi, è stata richiesta la regolarizzazione, laddove carenti dei presupposti richiesti) e di segnalazioni.

Una parte significativa (circa un terzo) dei reclami definiti nell'anno di riferimento ha riguardato le istanze rivolte ai gestori dei motori di ricerca – fra i quali emerge per rilevanza e numero di casi Google – dirette ad ottenere la deindicizzazione di contenuti reperibili in associazione al nominativo dell'interessato. Un'altra parte ugualmente rilevante dei reclami ha interessato gli organi di informazioni (testate giornalistiche in senso stretto, *blog,* siti di informazione ecc.) ed è stata caratterizzata prevalentemente dalla denuncia di pubblicazioni (articoli, commenti, estratti di *e-book*) ritenute illecite perché contenenti dati personali eccedenti o diffusi in violazione di specifici limiti (dati attinenti alla sfera sessuale, relativi alla salute, riguardanti minori). Un terzo ambito di interesse dei reclami ha riguardato la pubblicazione di dati personali (commenti, fotografie ecc.) sui *social network,* rispetto alla quale veniva lamentata l'assenza del consenso o altra base giuridica del trattamento.

In tutte queste tipologie di reclami l'esame dell'Autorità ha riguardato anche l'osservanza delle disposizioni in materia di esercizio dei diritti (artt. 15-22 del RGPD), a seguito del quale sono emersi alcuni casi di ripetuta inottemperanza da parte del medesimo titolare alle istanze preventive formulate dall'interessato, circostanza per la quale il Garante ha ritenuto applicabile una sanzione amministrativa (provv. 25 marzo 2021, n. 116, doc. web n. 9577346).

Ferma restando, anche nel periodo di riferimento, un'alta adesione da parte dei titolari del trattamento alle istanze dei reclamanti – ciò che ha consentito di definire il reclamo senza l'adozione di un provvedimento del Collegio – una parte dei reclami definiti, pari a circa un terzo delle relative istanze, ha invece portato all'adozione di decisioni collegiali che, attraverso l'esame degli elementi specifici di ogni vicenda, si sono pronunciate sulla fondatezza della doglianza prospettata, ricorrendo spesso ad un bilanciamento tra le istanze del singolo e l'interesse pubblico generale all'informazione e facendo ricorso ai poteri correttivi, ivi incluso quello sanzionatorio, previsto dal RGPD. Nei casi più gravi il Garante ha applicato, quale deterrente alla reiterazione della condotta giudicata illecita, anche misure sanzionatorie di tipo pecuniario (provv.ti 13 maggio 2021, n. 197, doc. web n. 9670001; 29 settembre 2021, n. 355, doc. web n. 9720498): la scelta è stata indotta, di regola, dalla parti-

colare gravità delle violazioni contestate, ritenendo di dover comunque mantenere una linea di particolare cautela nell'esercizio di questo nuovo potere, in un settore delicato quale quello della libertà di manifestazione del pensiero.

Le segnalazioni sono state esaminate ed istruite nei casi di particolare gravità o che comunque hanno evidenziato i presupposti per una verifica sul rispetto della disciplina in materia di protezione dei dati personali (ad es. con riferimento alle notizie sulle violenze subìte dai detenuti del carcere di Santa Maria Capua Vetere) ovvero, sempre se rientranti nell'ambito delle competenze dell'Autorità. In alcuni casi si è provveduto all'accorpamento delle segnalazioni pervenute per approfondimenti su tematiche di carattere generale.

Anche nell'anno di riferimento sono stati aperti alcuni procedimenti d'ufficio a fronte di fatti di cronaca di particolare gravità che hanno evidenziato criticità sul piano del trattamento dei dati personali (diffusione di notizie relative a procedimenti in materia di presunte violenze sessuali; il decesso di una minore vittima di una presunta sfida suicida sui *social*).

9.2. *Il trattamento dei dati nell'esercizio dell'attività giornalistica*

9.2.1. Dati giudiziari

Nel corso dell'anno l'Autorità si è dedicata al tema del trattamento di dati giudiziari da parte di testate giornalistiche e di siti web, oltre che da parte dei motori di ricerca (cfr. par. 9.4), attraverso l'individuazione dei principi volti a garantire un corretto e proporzionato trattamento di questa categoria di dati. Ciò nell'ottica di salvaguardare le esigenze informative connesse a notizie riguardanti fatti di cronaca di interesse pubblico nel rispetto dei diritti fondamentali delle persone coinvolte, sia che si tratti di vittime, sia che si tratti invece delle persone sottoposte ad indagine e/o ad operazioni di arresto.

Sono stati così ribaditi i limiti nella diffusione dei dati personali in relazione alle vicende giudiziarie riportate nelle diverse istanze presentate al Garante nel periodo di riferimento.

Nei primi mesi del 2021 è stata completata un'istruttoria avviata d'ufficio riguardante il tema ricorrente dell'utilizzo, a corredo di articoli giornalistici di cronaca giudiziaria, di immagini di persone ritratte in condizioni di restrizione della libertà fisica o comunque in situazioni che appaiono lesive della dignità dell'individuo. Nel caso di specie le immagini diffuse riguardavano soggetti, peraltro giovani di età, ripresi, in concomitanza dell'arresto, in un contesto di limitazione della libertà personale, la cui pubblicazione può ritenersi lecita solo in presenza di presupposti specifici individuati, in particolare, nella necessità di segnalare abusi (cfr. art. 8, comma 3, delle regole deontologiche) o nel consenso dell'interessato (art. 114, comma 6-*bis* c.p.p.), circostanze che, nei casi esaminati, non sono state ritenute esistenti. Né il Garante ha ritenuto sufficiente a salvaguardare i diritti degli interessati l'accorgimento, adottato da alcune testate giornalistiche, di utilizzare tecniche di oscuramento delle sole manette, ritenendo tale intervento insufficiente a garantire il rispetto dei divieti posti alla pubblicazione, dato il contesto in cui le persone coinvolte sono state raffigurate.

L'Autorità, ravvisando contrasto con le norme di settore ha vietato il trattamento, confermando con ciò la valutazione resa in sede di adozione dei precedenti provvedimenti di limitazione provvisoria. È stato altresì comminato un ammonimento nei confronti di tutti i titolari coinvolti, con l'unica eccezione di un caso in cui è stata inflitta al titolare una sanzione pecuniaria motivata dal mancato adeguamento del medesimo al precedente ordine di limitazione del trattamento

9

adottato in via d'urgenza dal Garante nell'immediatezza della pubblicazione delle immagini (provv.ti 25 febbraio 2021, n. 76 doc. web n. 9568040; n. 77 doc. web n. 9568061; n. 78, doc. web n 9568082; n. 79 doc. web n. 9568103; n. 80 doc. web n. 9568121; n. 81 doc. web n. 9568139; n. 82 doc. web n. 9568165; n. 83 doc. web n. 9568200; n. 84 doc. web n. 9568222 e n. 85 doc. web n. 9568244).

Non sono mancati casi in cui l'Autorità ha ritenuto di dover escludere la cancellazione dei dati personali nell'ambito di articoli che, opportunamente sottratti all'indicizzazione da parte dei motori di ricerca in ragione del tempo trascorso, sono confluiti nell'archivio del giornale per una legittima finalità di archiviazione di interesse storico-documentaristico che, pur differente dall'originaria finalità di cronaca giornalistica, risulta compatibile con essa, come desumibile dalla disciplina applicabile (art. 5, par. 1, lett. *b*) ed *e*), del RGDP e dall'art. 99 del Codice) e confermato dalla giurisprudenza (Cass. civ., sez. I, 27 marzo 2020, n. 7559).

Sotto altro profilo, il caso esaminato ha tuttavia evidenziato un'inadempienza dell'editore nel fornire riscontro a una richiesta preventivamente formulata dall'interessato in sede di esercizio dei diritti, ai sensi dell'art. 12, comma 4, del RGDP, inadempienza già contestata al medesimo editore in precedenti casi e, pertanto, il Garante, nel ritenere fondato il reclamo relativamente a tale profilo, ha disposto altresì una sanzione amministrativa all'editore (provv. 25 marzo 2021, n. 116, doc. web n. 9577346).

9.2.2. Dati relativi a minori

Una particolare attenzione, anche nell'anno di riferimento, è stata riservata al rispetto delle garanzie relative al trattamento dei dati riguardanti i minori, quali quelle codificate nelle regole deontologiche (art. 7) e nella Carta di Treviso.

Al riguardo è da segnalare che il 6 luglio 2021 il Consiglio dell'Ordine dei giornalisti ha deliberato un nuovo testo della Carta, di cui l'Autorità – che non è stata coinvolta nella relativa stesura – ha preso atto, pur rilevando, unitamente alla conferma dei principi di fondo, alcune criticità.

Le disposizioni a tutela dei minori sono state richiamate dal Garante nell'esaminare un reclamo di un genitore diretto a denunciare l'illiceità della pubblicazione dei dati del figlio minore e della sua storia familiare, contenuti in un estratto di un libro pubblicato su un sito dedicato alla genitorialità e, in particolare, alla tematica dei padri separati. L'Autorità, pur riconoscendo nella finalità del progetto un interesse pubblico meritevole di considerazione, ha osservato che proprio la delicatezza dei temi affrontati – coinvolgenti minori di età – richiede il più rigoroso rispetto delle disposizioni in materia di protezione dei dati personali, considerati anche gli effetti diffusivi della rete. Il Garante ha rilevato peraltro che, nonostante le misure adottate dall'editore e dall'autore del libro volte a limitare la diffusione dell'estratto oggetto di doglianza, quest'ultimo era comunque reperibile in rete tramite i motori di ricerca, sulla base di una ricerca effettuata a partire dai dati identificativi del minore; pertanto, ha disposto il divieto di ulteriore trattamento nonché, in ragione delle violazioni riscontrate, un ammonimento nei confronti dell'editore e dell'autore della pubblicazione, unitamente ad un avvertimento in merito al rispetto delle disposizioni relative all'esercizio dei diritti, stante alcune carenze riscontrate al riguardo (provv. 8 luglio 2021, n. 267, doc. web n. 9704173).

Analoga esigenza di tutela è stata riscontrata dall'Autorità in relazione all'avvenuta pubblicazione di un articolo, denunciata dall'interessato tramite la presentazione di un reclamo, contenente informazioni dettagliate sulle circostanze della morte di una donna della quale erano stati riportati i dati identificativi, ivi incluso l'indirizzo di residenza presso il quale abitavano i familiari della medesima, tra cui la figlia

minore. L'articolo riportava, inoltre, dettagli circa la relazione intima intercorrente tra la defunta e l'uomo indagato per la sua morte, determinando con ciò un ulteriore pregiudizio dei diritti dei familiari della stessa, ulteriormente esposti a violazioni della loro sfera personale. L'Autorità, pur prendendo atto dell'intervenuta rimozione dell'articolo disposta dall'editore nel corso del procedimento, ha rilevato l'eccedenza informativa dei dettagli contenuti nella narrazione del fatto, dichiarando l'illiceità del relativo trattamento e disponendo un ammonimento nei confronti dell'editore (provv. 11 marzo 2021, n. 96, doc. web n. 9577017).

9.2.3. Inchieste giornalistiche

Anche il 2021 ha visto impegnata l'Autorità nella complessa opera di bilanciamento tra i diritti della persona e la libertà di informazione, alla luce delle disposizioni contenute nelle regole deontologiche (art. 2) che prevedono talune eccezioni all'obbligo di fornire l'informativa – seppur semplificata – all'interessato al momento della raccolta dei dati nel contesto del cd. giornalismo di inchiesta.

In particolare, l'Autorità ha esaminato un reclamo diretto a denunciare l'uso di artifici nella raccolta dei dati personali della reclamante, ritenuti idonei a rivelarne il credo religioso, da parte di due giornalisti che non si sarebbero qualificati come tali, nonché a denunciare la violazione delle disposizioni in materia di esercizio dei diritti. L'Autorità ha ritenuto invece che l'operato della testata giornalistica interessata dal reclamo si fosse svolto nei confini consentiti dalle disposizioni deontologiche, allo scopo di documentare un fatto di interesse pubblico (il tragico epilogo di una spedizione alpinistica) attraverso la raccolta di informazioni volte a dare supporto all'inchiesta (i possibili legami tra l'iniziativa dell'alpinista, ritenuta temeraria dai molti esperti del settore, e la sua adesione all'associazione presieduta dalla reclamante e alla chiesa di Scientology, di cui il servizio evidenzia il reciproco legame).

Il reclamo è stato ritenuto infondato alla luce del contesto generale dei fatti – nei quali, invero, risultavano palesi la professione degli intervistatori, l'uso di strumenti di ripresa e le finalità dell'intervista – e dell'argomento di quest'ultima, trattato nel rispetto dell'essenzialità dell'informazione riguardo ad una vicenda di rilevanza pubblica. È stato tuttavia disposto un avvertimento in relazione al profilo dell'esercizio dei diritti alla luce di alcuni ritardi e carenze del titolare nel darvi riscontro (provv. 29 settembre 2021, n. 354, doc. web n. 9716402).

In altra circostanza il Garante ha invece accolto le richieste contenute in un reclamo diretto a denunciare la pubblicazione di dati idonei ad identificare l'interessata all'interno di un articolo, facente parte di una rassegna diretta a ricostruire fatti di cronaca del passato, finalizzato a ripercorrere i momenti principali di una vicenda in cui era stata coinvolta molti anni prima come autrice di un reato grave. L'interessata, che aveva già scontato da diverso tempo la pena alla quale era stata condannata, ha lamentato, in particolare, il pregiudizio derivante dalla rinnovata divulgazione dei propri dati identificativi, tenuto conto che, alla luce del tempo trascorso e del fatto che non fosse un personaggio noto, non poteva ritenersi sussistente un interesse del pubblico ad avere conoscenza della sua identità. L'Autorità ha reputato che la rinnovata pubblicazione di notizie relative a vicende passate, non determinata da ragioni di attualità, non costituisca esercizio del diritto di cronaca, ma esplicazione di un'attività storiografica che non richiede, per svolgere la propria funzione, la divulgazione dei dati identificativi dei protagonisti, a meno che i fatti non riguardino personaggi che rivestano o abbiano rivestito un ruolo pubblico, ovvero implichino, per il loro concreto svolgersi, il richiamo necessario ai nomi dei protagonisti (cfr. Cass. sez. un. n. 19681/2019). Il trattamento effettuato dall'editore è stato dunque ritenuto non necessario e lesivo del diritto

dell'interessata ad essere dimenticata (provv. 16 dicembre 2021, n. 447, doc. web n. 9737121).

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

Il rispetto dell'essenzialità dell'informazione costituisce uno dei principi-cardine della disciplina relativa alla protezione dei dati personali in ambito giornalistico. Esso trova la sua esplicitazione nel Codice (art. 137) e nelle regole deontologiche (artt. 6, 8, 10, 11) e costituisce il parametro principale che il giornalista, in prima battuta, e il Garante, successivamente, devono considerare ai fini di una informazione corretta e rispettosa dei diritti della persona.

Sulla base di tali premesse, sono stati esaminati alcuni reclami e segnalazioni relativi a fatti di cronaca di grande rilevanza generale e di forte impatto mediatico.

In particolare, nel periodo di riferimento è stata conclusa un'istruttoria che ha riguardato diverse testate in relazione alle modalità con cui è stata data notizia dell'attentato in Iraq del 2019 nel quale sono stati coinvolti militari italiani. L'istruttoria ha preso le mosse dalla segnalazione effettuata dal genitore di uno dei militari il quale ha indicato un elenco di articoli contenenti i dati identificativi del figlio e degli altri militari coinvolti nell'attentato nonché altre informazioni dettagliate, anche relative alle ferite subìte, riscontrando in siffatta diffusione di dati una violazione del diritto alla riservatezza degli interessati ed un rischio per la loro sicurezza.

L'Autorità, pur rilevando il grande interesse per la vicenda a livello nazionale e internazionale, ha disposto un ammonimento nei confronti delle testate che avevano pubblicato i dati identificativi del militare in associazione alle ferite e alle conseguenze di salute subìte per effetto dell'esplosione, in ragione delle specifiche violazioni riscontrate (artt. 137, commi 1 e 3, e 139 del Codice e gli artt. 5, 6 e 10 delle regole deontologiche, i principi generali di liceità e correttezza del trattamento dei dati personali di cui all'art. 5, par. 1, lett. *a*), del RGPD e art. 2-*quater* del Codice), vietandone altresì l'ulteriore trattamento (provv.ti 13 maggio 2021, n. 339, doc. web n. 9720469; n. 344, doc. web n. 9725219; n. 345 doc. web n. 9720285). Parimenti, ha disposto un ammonimento nei confronti di una testata che aveva diffuso, oltre ai dati identificativi dei militari, altri dati ritenuti eccedenti (luogo di nascita, residenza e composizione del nucleo familiare; provv. 13 maggio 2021, n. 347, doc. web n. 9728028). L'Autorità ha ritenuto invece di disporre un avvertimento nei riguardi delle testate che avevano riportato i dati identificativi dei militari, pur senza una specifica associazione alle conseguenze di salute subìte, evidenziando che il rispetto del principio di essenzialità dell'informazione – quale esplicitato nell'art. 6 delle regole deontologiche – richiede comunque, da parte degli operatori dell'informazione, un'attenta valutazione riguardo alla necessità e/o opportunità di diffondere i dati identificativi di soggetti appartenenti a Forze militari vittime di rappresaglie o azioni terroristiche; ciò, pur in assenza di specifici divieti normativi al riguardo, quale cautela a presidio della riservatezza e sicurezza degli interessati e dei loro familiari (provv.ti 13 maggio 2021, n. 340, doc. web n. 9721139; 341, doc. web n. 9721156; n. 342, doc. web n. 9721211; n. 343, doc. web n. 9721228; n. 346, doc. web n. 9728011; n. 348, doc. web n. 9728067. Il provv. n. 343 è stato oggetto di impugnazione dinanzi al Tribunale di Napoli).

L'Autorità ha altresì sanzionato una testata giornalistica che ha fornito nome e cognome di un reclamante, vittima di un grave infortunio sul lavoro, dando altresì notizia dell'entità del risarcimento per i danni subiti riconosciuto in via extragiudiziale. L'Autorità, infatti, ha reputato che l'articolo contenesse dati eccedenti rispetto al principio di essenzialità dell'informazione, esponendo così la vicenda ad un'attenzione che andava ben al di là della cerchia dei suoi conoscenti, senza che l'indicazione

del nominativo apparisse essenziale ai fini della corretta informazione sulla vicenda medesima (provv. 29 settembre 2021, n. 355, doc. web n. 9720498).

L'Autorità ha poi valutato le richieste provenienti dagli eredi di una persona deceduta a causa di Covid-19 che, lamentando l'avvenuta divulgazione di informazioni particolarmente delicate sullo stato di salute del *de cuius,* hanno chiesto l'accertamento dell'illiceità del trattamento dei dati del medesimo e la cessazione della relativa diffusione. Nel caso in esame, tuttavia, alla luce del fatto che il defunto era persona nota nell'ambito locale di riferimento, corrispondente all'area geografica di diffusione della testata giornalistica, e del fatto che la finalità dell'articolo, come desumibile anche dalle parole utilizzate, fosse essenzialmente riconducibile all'intento di commemorare il defunto e informare della sua scomparsa la collettività di riferimento, il Garante ha ritenuto che non fosse stato travalicato il principio di essenzialità dell'informazione, tenuto conto del fatto che all'interno dell'articolo era contenuto solo un breve accenno alle ragioni che avevano determinato il ricovero e la successiva morte del *de cuius,* senza fornire dati di dettaglio, in conformità con quanto previsto dall'art. 10 delle regole deontologiche. Tale riferimento, peraltro, poteva ritenersi motivato dalla particolare propagazione del virus nell'area geografica corrispondente all'ambito territoriale di diffusione del quotidiano oggetto di segnalazione. Le doglianze degli interessati sono state dunque ritenute infondate (provv. 29 aprile 2021, n. 180, doc. web n. 9688429).

9.3. *I* social network

Numerosi reclami e segnalazioni hanno avuto ad oggetto la pubblicazione di dati personali (commenti, fotografie ecc.) sui *social network* e, in particolare, su Facebook, Instagram e You Tube.

Le disposizioni che disciplinano tale materia sono, anche in questo caso, quelle di cui agli art. 136 e seguenti del Codice dedicate a "finalità giornalistiche e altre manifestazioni del pensiero", in quanto l'ampia formulazione delle stesse consente, quando ne ricorrano i presupposti, di estendere le garanzie e le deroghe in materia di tutela della riservatezza e della protezione dei dati anche a quelli immessi nella rete. Per i dati pubblicati tramite *social media,* similmente a quanto avviene nel caso della diffusione dei dati per finalità giornalistiche, non occorre il consenso dell'interessato, sempre che sussistano adeguate finalità di interesse pubblico.

Anche in questi casi, perciò, il bilanciamento tra la libertà di manifestazione del pensiero, da un lato, e la tutela dei dati personali, dall'altro, va effettuato caso per caso, sulla base del tipo di diffusione e della natura dell'informazione di volta in volta immessa dall'interessato o, più frequentemente, da altri soggetti.

In questo quadro, l'Autorità ha condotto una lunga istruttoria relativamente all'avvenuta pubblicazione sul profilo Facebook di un soggetto, che rivestiva la qualifica di sindaco, di immagini e video – in chiaro – di persone disabili o disagiate, anche minori di età, nonché di presunti autori di trasgressioni amministrative, esponendo altresì questi ultimi ai commenti offensivi degli utenti del *social network.* Tra i contenuti pubblicati vi era, in particolare, l'immagine di un ragazzo disabile, associata al provvedimento che assegnava ai genitori un posto auto nei pressi dell'abitazione, lasciando anche visibile l'indirizzo di residenza, nonché immagini e video di minori ripresi in condizioni di degrado, nell'ottica di documentare le condizioni di salute dei medesimi e la questione delle "baraccopoli".

Nel corso dell'istruttoria è emerso che siffatta diffusione di immagini non fosse giustificata da specifiche ragioni di interesse pubblico e che anzi fosse idonea a

9

determinare un grave pregiudizio per i soggetti ritratti, travalicando così il principio di essenzialità dell'informazione previsto dalle norme in materia di trattamento per finalità giornalistiche, applicabile anche a forme di manifestazione del pensiero non costituenti esercizio del diritto di cronaca. L'Autorità ha quindi vietato al titolare l'ulteriore trattamento dei dati, eccettuata la loro conservazione ai fini di un eventuale utilizzo in sede giudiziaria, e gli ha ordinato il pagamento di una sanzione di cinquantamila euro (provv. 13 maggio 2021, n. 197, doc. web n. 9670001, oggetto di impugnazione dinanzi al Tribunale di Messina).

In ordine ai trattamenti di dati personali effettuati dai *social network* il Garante ha svolto un'attività intensa, in sede europea, con particolare riferimento al trattamento dei dati da parte di TikTok e ha altresì adottato, in ambito nazionale, una serie di provvedimenti, in particolare al fine di limitare l'utilizzo di tale piattaforma da parte di minori di 13 anni (cfr. Relazione 2020, p. 134 e ss.).

Il Garante ha pertanto proseguito l'attività di monitoraggio riguardo all'adeguamento da parte di TikTok delle determinazioni dell'Autorità (provv.ti 22 gennaio 2021, n. 20, doc. web n. 9524194; 11 febbraio 2021, n. 61, doc. web n. 9554603; 25 marzo 2021, n. 126, doc. web n. 9574709) e degli impegni assunti nel corso degli ultimi mesi avviando anche una procedura di collaborazione con le altre autorità europee nell'ambito di un'apposita procedura di cooperazione. Proprio in tale ambito, la Società ha condiviso ulteriori informazioni relative agli strumenti tecnologici che intende mettere in campo per assicurare una migliore valutazione dell'età dei propri utenti (cfr. par. 23.3).

9.4. *Il trattamento dei dati da parte dei motori di ricerca*

I reclami proposti nei confronti dei gestori di motori di ricerca hanno costituito nel 2021 circa un terzo dei reclami complessivamente pervenuti all'Autorità nel settore della libertà di informazione. Parte di essi sono stati contemporaneamente rivolti dagli interessati anche nei confronti dei titolari dei siti web nei quali sono state pubblicate le informazioni indicizzate tramite motore di ricerca, al fine di ottenere una tutela più ampia dei diritti esercitati.

La maggior parte delle richieste di *delisting* hanno riguardato trattamenti posti in essere tramite il motore di ricerca gestito da Google LLC, cui ha fatto seguito l'attivazione di altrettanti procedimenti, un terzo dei quali sono stati definiti tramite decisione del Garante italiano, in virtù dell'autonomia spettante a ciascuna autorità di controllo rispetto ai trattamenti posti in essere dalla citata Società relativamente all'attività del motore di ricerca, per la quale non opera il meccanismo dello sportello unico (cfr. Relazione 2019, p. 111 e Relazione 2020, p. 135).

Diversamente, con riguardo alle società che gestiscono altri motori di ricerca – in particolare Microsoft Corporation (Bing) e Verizon Media (Yahoo!) – si è fatto ricorso, laddove non sia stato possibile definire il reclamo nel corso dell'istruttoria preliminare, al meccanismo di cooperazione, proponendo all'autorità capofila, in presenza dei presupposti di cui all'art. 56, par. 2, del RGPD, la definizione locale del caso.

Questa strada è stata intrapresa, in particolare, per un reclamo volto alla rimozione di alcuni risultati di ricerca reperibili, anche attraverso i citati motori di ricerca Bing e Yahoo!, in associazione al nominativo del reclamante. L'Autorità ha inviato ai predetti gestori una richiesta preliminare finalizzata a valutare la possibilità di definire la questione anteriormente all'attivazione del meccanismo di cooperazione. Nel caso di specie, mentre Verizon ha invocato la competenza della *Lead Authority* nella

trattazione del reclamo, Microsoft ha parzialmente aderito alle richieste dell'interessato, eccependo tuttavia, con riferimento a parte degli Url oggetto di reclamo, la sussistenza di un perdurante interesse del pubblico alla conoscibilità delle informazioni, tenuto conto della recente condanna del reclamante per reati particolarmente gravi e del fatto che il medesimo non aveva neppure fornito elementi relativi all'eventuale seguito giudiziario della vicenda. È stata così disposta l'apertura della procedura di cooperazione tramite l'apposita piattaforma utilizzata per la condivisione dei casi in ambiente europeo (IMI). Trattandosi di una fattispecie che, sulla base della previsione contenuta nell'art. 56.2 del RGPD, presentava specifici elementi di collegamento con la dimensione nazionale, l'Autorità italiana ha avanzato la proposta di definire il reclamo a livello locale anche in considerazione del fatto che quest'ultimo era stato proposto altresì nei confronti di altri titolari nei confronti dei quali il Garante aveva un potere decisionale autonomo: tale proposta non ha trovato tuttavia accoglimento da parte dell'Autorità irlandese, che ha invece rappresentato la necessità di valutare unitariamente i reclami aventi ad oggetto una richiesta di rimozione ai sopra indicati motori di ricerca, motivando la scelta alla luce dell'impatto che le relative decisioni possono produrre in sede di applicazione dei criteri di *delisting*. Successivamente l'Autorità italiana ha definito il reclamo per la parte di propria competenza, con una decisione di infondatezza, ritenendo che gli elementi del caso concreto – dato temporale e gravità dei reati per i quali l'interessato era stato condannato – non consentissero di ritenere prevalente il diritto invocato dall'interessato rispetto alle ragioni di interesse pubblico (provv. 27 maggio 2021, n. 221, doc. web n. 9697849).

Con riguardo invece alle richieste avanzate nei confronti di Google occorre rilevare che circa la metà di esse 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. Le decisioni assunte dall'Autorità nel periodo di riferimento (circa 37) presentano, come tipologia, un numero più o meno equivalente di valutazioni di infondatezza – attraverso le quali sono stati per lo più confermati principi già enucleati nell'ambito di precedenti provvedimenti riguardanti questioni analoghe (provv.ti 14 gennaio 2021, doc. web n. 9548213; 27 gennaio 2021, n. 32, doc. web n. 9561815; 25 marzo 2021, doc. web n. 9678576; 21 aprile 2021, doc. web n. 9695059; 29 settembre 2021, n. 357, doc. web n. 9713833; 11 novembre 2021, n. 402, doc. web n. 9725202; 16 dicembre 2021, n. 445, doc web n. 9742722) – e di accoglimento, anche solo parziale, delle istanze avanzate dagli interessati.

Le doglianze espresse dagli interessati hanno riguardato, in via principale, il pregiudizio subìto dagli stessi a causa della reperibilità in rete di informazioni riguardanti vicende giudiziarie nelle quali sono stati coinvolti e che hanno 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 si è verificato non solo riguardo ad ipotesi in cui sia stata successivamente accertata la non colpevolezza dell'interessato, ma anche nei casi in cui, pur essendo intervenuta una sentenza di condanna a suo carico, il quadro complessivo della vicenda sia mutato determinando un sostanziale superamento della notizia originaria.

Ciò è quanto avvenuto nel caso di una richiesta di rimozione di Url collegati ad articoli riguardanti un procedimento penale nel quale il reclamante era stato coinvolto qualche anno prima, divenendo destinatario di un'ordinanza di custodia cautelare, ma che si è poi concluso con un decreto di archiviazione della posizione del medesimo. Di quest'ultima circostanza non era stata tuttavia fatta alcuna menzione nei predetti articoli, né risultavano altrimenti reperibili in rete informazioni aggiornate in merito alla vicenda. L'Autorità ha, in tal caso, accolto l'istanza (provv.ti 25

9

novembre 2021, nn. 416 e 417, doc. web nn. 9732368 e 9732385) ritenendo che il diritto dell'interessato dovesse reputarsi prevalente rispetto alle ragioni di interesse pubblico dedotte dal titolare del trattamento, tenuto conto del fatto che la perdurante diffusione di informazioni non aggiornate alla luce dei menzionati esiti giudiziari costituisse un trattamento particolarmente pregiudizievole per la sfera giuridica del reclamante, risultando idoneo a fornire agli utenti della rete una rappresentazione inesatta e fuorviante in ordine al coinvolgimento del medesimo. Ai fini della decisione si è tenuto particolare conto della posizione espressa dalla CGUE nella sentenza 24 settembre 2019, pronunciata nella causa C-136/17 in cui è contenuta un'attenta disamina dell'approccio che anche il gestore di un motore di ricerca deve adottare nel trattamento delle particolari categorie di dati individuate nel RGPD, tra le quali quelle riferite ai dati giudiziari di cui all'art. 10. Nell'ambito delle finalità per le quali è consentito il trattamento di dati personali da parte del gestore di un motore di ricerca rientra sicuramente quella di rendere accessibili informazioni di interesse per il pubblico, ma tale aspetto dovrebbe essere necessariamente bilanciato con i diritti fondamentali dell'individuo, specie laddove si verta su profili particolarmente sensibili della sua vita. Su tale profilo si è incentrata maggiormente l'attenzione della Corte che, con riguardo ai dati giudiziari, ne ammette la divulgazione purché la stessa si riveli strettamente necessaria, precisando che, qualora la reperibilità di informazioni relative a fasi ormai superate di un procedimento giudiziale che abbia coinvolto l'interessato sia da ritenersi giustificata alla luce dell'interesse prevalente del pubblico ad avervi accesso, il motore di ricerca dovrà sistemare "l'elenco dei risultati in modo tale che l'immagine globale che ne risulta per l'utente di internet rifletta la situazione giudiziaria attuale", ordinandoli quindi sulla base dei risultati di ricerca più recenti.

Tale principio vale principalmente nei casi nei quali, come in quello descritto, vi sia stata un'evoluzione favorevole della vicenda giudiziaria che non risulta menzionata in nessun ulteriore articolo presente in rete, circostanza che non consente di costruire un profilo dell'interessato corrispondente alla sua attuale identità. Ma analogo ragionamento può altresì essere effettuato anche nei casi in cui, nonostante sia stato giudizialmente dimostrato un coinvolgimento dell'interessato, la vicenda presenti comunque degli elementi tali da non far ritenere sussistente un interesse pubblico attuale alla conoscibilità di informazioni che appaiono superate da fatti successivi che ne hanno, almeno in parte, modificato i contorni.

Ciò è quanto si è verificato, ad esempio, nel caso della richiesta di rimozione di Url collegati ad articoli di giornale che riportavano la notizia del coinvolgimento del reclamante in una vicenda giudiziaria relativa a reati commessi in occasione dello svolgimento della propria attività lavorativa prestata alle dipendenze di un ente pubblico ed in relazione alla quale il medesimo è stato poi condannato. L'interessato, nel presentare una richiesta di rimozione degli Url collegati a pagine contenenti la notizia, ha rappresentato che l'anno successivo alla pronuncia della condanna a suo carico gli era stata concessa la possibilità di espiare la pena in regime di affidamento in prova al servizio sociale e che, in seguito all'esito positivo di esso, il giudice aveva dichiarato l'estinzione della pena, circostanza quest'ultima non riportata all'interno degli articoli oggetto di contestazione, né altrimenti rinvenibile in rete. L'Autorità ha accolto la richiesta ritenendo che il trattamento di dati giudiziari, benché riferiti ad un procedimento penale conclusosi con la condanna dell'interessato, risultasse, anche in considerazione dell'intervenuta estinzione della pena, fuorviante ed in contrasto con i principi di esattezza ed aggiornamento dei dati espressamente previsti dal RGPD (provv. 13 maggio 2021, n. 194, doc. web n. 9681992). Analogamente è avvenuto in altri casi nei quali la ragione specifica della doglianza degli interessati riguardava la reperibilità tramite motore di ricerca, ed in associazione al nominativo

dei medesimi, di articoli riportanti notizie risalenti nel tempo e non aggiornate alla luce dell'evoluzione giudiziaria successiva che, pur avendo condotto all'accertamento della responsabilità dei reclamanti, aveva comunque portato ad una rideterminazione della pena in senso favorevole al reo (provv. 21 aprile 2021, n. 150, doc. web n. 9676101) o ad un'assoluzione rispetto ad alcuni dei capi di imputazione contestati e costituenti però l'oggetto prevalente delle informazioni riportate negli articoli fatti oggetto di reclamo (provv. 11 novembre 2021, n. 404, doc. web n. 9731844, cfr. anche provv. 24 giugno 2021, n. 253, doc. web n. 9698286).

L'operazione di bilanciamento sottesa alla valutazione delle richieste di rimozione deve tenere conto, come noto, delle esigenze di tutela espressa dagli interessati da un lato e, dall'altro, dell'interesse degli utenti della rete di disporre di informazioni utili riguardo ai medesimi. Al fine di poter apprezzare la sussistenza di un interesse pubblico attuale 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, che è poi l'obiettivo principale del trattamento effettuato dai gestori di motori di ricerca.

Tale idoneità è tuttavia risultata assente in alcune delle fattispecie sottoposte all'attenzione del Garante nelle quali è emerso che, a prescindere dalla rilevanza che poteva essere riconosciuta ad alcune informazioni relative al reclamante, parte dei risultati restituiti in esito ad una ricerca condotta in associazione al nominativo del medesimo corrispondessero a pagine ad accessibilità limitata riservate ai soli abbonati. In particolare l'Autorità, tenuto conto che ciò che risultava visibile alla generalità degli utenti non appariva sufficiente a contribuire alla realizzazione di un profilo dell'interessato effettivamente rispondente all'interesse pubblico, ha accolto parzialmente le richieste del medesimo, ordinando al gestore del motore di ricerca la rimozione dei relativi Url, atteso che la reperibilità di notizie riguardanti la vicenda sottostante, e riconosciute di interesse sia per la gravità dei fatti contestati che per il ruolo attualmente svolto dal reclamante, richiedeva la disponibilità in rete di contenuti visibili nella loro interezza o comunque riconducibili ad un *abstract* informativo sufficientemente esplicito (provv. 27 maggio 2021, n. 219, doc. web n. 9698107).

Analoga valutazione è stata effettuata con riguardo ad un'altra richiesta di rimozione di Url collegati ad articoli riportanti informazioni su procedimenti penali coinvolgenti il reclamante. In questo caso, tuttavia, è stato rilevato che le pagine reperibili tramite i predetti Url contenessero solo un *abstract* della versione integrale degli articoli corrispondenti nel quale, oltre a non essere presenti informazioni giudiziarie aggiornate, non era riportato neppure il nome dell'interessato. L'Autorità, sulla base di tali elementi, ha accolto la richiesta ritenendo che le notizie parzialmente visibili non fossero idonee a rispondere ad un interesse del pubblico alla conoscibilità di esse tale da prevalere sui diritti dell'interessato, ma che anzi le stesse potessero invece risultare pregiudizievoli per quest'ultimo, nonché fuorvianti per gli utenti della rete (provv. 21 aprile 2021, n. 151, doc web n. 9682125).

Il rispetto dell'identità personale impone la necessità di tenere particolare conto del pregiudizio che possono subire i diritti dell'interessato per effetto della reperibilità in rete di informazioni inesatte, gli effetti delle quali sono amplificate dalla potenza della rete. Alla luce di questa considerazione, la divulgazione di notizie anche recenti, relative a vicende giudiziarie conclusesi con l'assoluzione può effettivamente comportare, al di là dell'elemento temporale, un impatto sproporzionato sulla vita dell'interessato, non bilanciato, in concreto, dalla sussistenza di un interesse pubblico prevalente. Ciò è quanto è stato riconosciuto dal Garante nell'accogliere una richiesta di rimozione di Url collegati ad articoli pubblicati in epoca recente e riportanti la notizia di un procedimento penale attivato nei confronti dell'interessato e

9

conclusosi con la sua assoluzione per non aver commesso il fatto: nel caso di specie è stato ritenuto che, in considerazione delle ragioni che hanno portato all'assoluzione, del tempo decorso dal verificarsi dei fatti e dell'assenza in rete di notizie analoghe, il trattamento ulteriore dei dati dell'interessato non si rilevasse necessario a soddisfare il diritto di informazione degli utenti risultando prevalente il diritto del singolo alla tutela dei propri diritti (provv. 11 febbraio 2021, n. 56, doc. web n. 9567461).

Valutazioni analoghe sono state effettuate per accogliere una richiesta di rimozione di Url collegati a pagine contenenti *post* pubblicati da un soggetto anonimo e riferiti ad un procedimento penale riguardante un terzo diverso dall'interessato, nell'ambito del quale quest'ultimo tuttavia era stato coinvolto in veste di testimone nel giudizio di primo grado. I commenti pubblicati riportavano, in particolare, una ricostruzione del loro autore circa le motivazioni che avrebbero indotto l'interessato a rendere una testimonianza sfavorevole all'imputato, poi assolto nel giudizio di primo grado, non tenendo tuttavia in considerazione la circostanza dell'avvenuto capovolgimento del giudizio in grado di appello, fase alla quale l'interessato non aveva peraltro preso parte. La perdurante diffusione di informazioni obsolete ed inesatte, sia pure riferite in via principale ad una persona diversa, è apparsa idonea a determinare un pregiudizio rilevante in capo all'interessato non bilanciato da un interesse del pubblico ad avere conoscenza di tali informazioni che, per come riportate, risultavano persino fuorvianti (provv. 22 luglio 2021, n. 282, doc. web n. 9702072).

È stato inoltre confermato un orientamento consolidatosi negli anni e diretto ad attribuire particolare rilievo alla portata giuridica di alcuni istituti dell'ordinamento penale, tra i quali il beneficio della non menzione della condanna nel casellario giudiziale. Quest'ultimo, in particolare, è finalizzato a limitare la conoscibilità della condanna subìta da un determinato soggetto, beneficio che sarebbe, di fatto, vanificato ove fosse consentito al gestore di un motore di ricerca di trattare tale dato attraverso la reperibilità in rete di esso in associazione al nominativo dell'interessato.

Ciò è quanto avvenuto, ad esempio, nel caso della richiesta di rimozione di alcuni Url da parte di una persona coinvolta in una vicenda giudiziaria connessa alla sua attività imprenditoriale, conclusasi con una sentenza di "applicazione di una pena a richiesta della parte" (art. 444 c.p.p.) inferiore a due anni di reclusione, da cui è conseguito il beneficio della non menzione della predetta pena nel certificato del casellario giudiziale, in attuazione di quanto previsto dalle disposizioni che ne regolano la formazione (in particolare l'art. 24, comma 1, lett. *e*), d.P.R. 14 novembre 2002, n. 313 recante testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di casellario giudiziale europeo, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti anche nella formulazione successiva alle modifiche introdotte con il d.lgs. 2 ottobre 2018, n. 122). Nel caso in esame, peraltro, parte degli articoli contestati erano riferiti a fasi del procedimento penale ormai superate e contenevano, altresì, informazioni inesatte, mentre i restanti Url oggetto di richiesta conducevano a pagine contenenti notizie relative ad indagini avviate nei riguardi di altri soggetti che all'epoca erano stati coinvolti nella medesima vicenda riguardante il reclamante. La valutazione complessiva di tali circostanze ha portato l'Autorità ad accogliere le istanze del reclamante posto che, in esito ad un giudizio di bilanciamento con l'interesse pubblico, la sfera giuridica dell'interessato appariva eccessivamente pregiudicata dall'ulteriore diffusione del contenuto degli articoli (provv. 16 dicembre 2021, n. 446, doc. web n. 9737008).

La richiesta di oblio non ha invece trovato accoglimento in un caso in cui la vicenda giudiziaria descritta nell'articolo reperibile in rete in associazione al nominativo del reclamante riguardava un procedimento penale conclusosi in epoca relativamente recente (2017), a seguito dell'"applicazione della pena su richiesta della

parte", con una condanna dell'interessato ad una pena di 3 anni di reclusione (e l'interdizione perpetua dai pubblici uffici), non corredata dai benefici (non menzione nel casellario giudiziale e estinzione del reato decorsi i 5 anni dalla sentenza) previsti per pene inferiori a due anni (art. 445 c.p.p.); benefici che, in altri casi, hanno avuto rilievo ai fini dell'accoglimento della richiesta di deindicizzazione (provv. 25 novembre 2021, n. 418, doc. web n. 9733159).

Analogamente, il Garante ha dichiarato infondato un reclamo in cui la vicenda giudiziaria descritta negli articoli reperibili in rete in associazione al nominativo del reclamante riguardava un procedimento penale conclusosi nel 2018, a seguito di patteggiamento, con la condanna dell'interessato a due anni di reclusione, e quindi relativamente recente (non essendo decorso il quinquennio al quale il citato art. 445, comma 2, c.p.p., riconnette l'estinzione del reato qualora l'imputato che abbia patteggiato la pena non abbia commesso altri delitti o contravvenzioni della stessa indole) (provv. 22 luglio 2021, n. 299, doc. web n. 9767899).

Si sono poi verificati casi nei quali l'Autorità ha condotto una duplice valutazione delle richieste oggetto del reclamo, tenendo conto, da una parte, del dato temporale – la conclusione recente della vicenda giudiziaria – e della conseguente attualità dell'interesse pubblico a reperire l'informazione; dall'altra, degli effetti particolarmente lesivi dei diritti della persona derivanti dalla reperibilità dell'informazione stessa. Ciò è quanto si è verificato in un caso in cui, in associazione ai dati identificativi della reclamante, venivano restituiti – tra i risultati della ricerca in rete - articoli corredati di immagini della stessa che, sia per le caratteristiche dell'inquadratura e dell'espressione (in uno stato di evidente alterazione), sia per la presenza al loro interno del logo istituzionale della Polizia di Stato, apparivano riconducibili alla categoria delle foto segnaletiche; immagini la cui diffusione è, invero, ammessa solo per il perseguimento di specifiche finalità di giustizia e polizia (art. 14, d.P.R. 15 gennaio 2018, n. 15). Con riguardo ai relativi Url, l'Autorità si è pertanto orientata per un accoglimento parziale del reclamo con riferimento alle citate immagini (restituite anche nella sezione immagini del motore di ricerca), ingiungendo a Google la deindicizzazione dei relativi Url, e ritenendo invece rispondente ad interesse prevalente la reperibilità delle notizie relative alla vicenda giudiziaria sottostante (provv. 29 settembre 2021, n. 362, doc. web n. 9713884).

Merita infine segnalare che il tema del diritto all'oblio con riferimento alle vicende giudiziarie ha costituito oggetto di un nuovo intervento legislativo. Tra i principi a cui il legislatore delegato si deve attenere nel dare attuazione alla legge 27 settembre 2021, n. 134 (Delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari) viene indicato anche quello in base al quale "il decreto di archiviazione e la sentenza di non luogo a procedere o di assoluzione costituiscano titolo per l'emissione di un provvedimento di deindicizzazione che, nel rispetto della normativa dell'Unione europea in materia di dati personali, garantisca in modo effettivo il diritto all'oblio degli indagati o imputati" (art. 1, comma 25).

10 Cyberbullismo

Le segnalazioni pervenute in materia di cyberbullismo nel periodo di riferimento riguardano prevalentemente la pubblicazione di *post* denigratori e diffamatori, nonché di fotografie, anche a carattere intimo (spesso sfuggite al controllo dello stesso minore che le ha inserite in *chat* private). Le stesse sono state tempestivamente trattate formulando una richiesta di intervento al titolare del trattamento/gestore del sito ovvero prendendo contatti (per telefono o per *e-mail*) con il segnalante per richiedere ulteriori informazioni o fornire indicazioni utili al caso. Vi è stato poi un esiguo numero di casi nei quali non sono stati ravvisati i presupposti per poter procedere alla luce di una riscontata carenza degli elementi che la legge n. 71/2017 indica quali requisiti minimi per qualificare una condotta come atto di cyberbullismo.

In un quadro più generale di azione, si segnala la partecipazione del Garante ai lavori del tavolo tecnico sulla tutela dei diritti dei minori nel contesto dei *social network,* dei servizi e dei prodotti digitali in rete, istituito con decreto del Ministro della giustizia del 21 giugno 2021 e al quale partecipano anche Agcom e il Garante per l'infanzia. I principali ambiti di intervento di tale tavolo tecnico, individuati dal d.m. istitutivo, sono i seguenti: a) protezione dei minori nella navigazione internet; b) sensibilizzazione dei genitori; c) sfruttamento commerciale dell'immagine dei minori. Sono state al riguardo effettuate una serie di audizioni di esperti e rappresentanti operanti nel settore della tutela dei minori, al fine di ottenere un quadro di contesto sufficientemente rappresentativo ed aggiornato. È, stato altresì predisposto un questionario trasmesso alle maggiori piattaforme *social* e da queste restituito, con richiesta di confidenzialità, concernente le misure adottate in questo ambito a tutela dei minori. Il tavolo, il termine dei cui lavori è previsto per la prima parte del 2022, sta ora discutendo un documento dell'Agcom, sui sistemi di *parental control* e di filtraggio di contenuti che gli ISP dovrebbero attuare per dare attuazione all'art. 7-*bis,* d.l. 30 aprile 2020, n. 28 (Sistemi di protezione dei minori dai rischi del cyberspazio), come convertito con legge 25 giugno 2020, n. 702, su cui anche il Garante avrà modo di esprimersi; inoltre sta lavorando ad un documento riepilogativo del percorso sin qui compiuto, corredato di un articolato di proposta normativa da trasmettere al Ministro della giustizia.

11 *Revenge porn*

Un elemento di novità nell'anno 2021 è rappresentato dall'impegno rivolto dal Garante a contrastare e prevenire il fenomeno della diffusione di immagini pornografiche o sessualmente esplicite a scopo vendicativo o comunque senza il consenso della persona (*revenge porn* e pornografia non consensuale).

In particolare, a partire dal marzo 2021 l'Autorità ha offerto la propria collaborazione, nell'ambito di un progetto di Facebook Inc. (NCII, *Non-Consensual Intimate Image*) di azione preventiva al fenomeno del *revenge porn,* mettendo a disposizione un canale di emergenza per segnalare il rischio di una possibile diffusione non consensuale, all'interno delle piattaforme Facebook e Instagram, di contenuti privati a carattere sessualmente esplicito. A tal fine è stato pubblicato sul sito un modulo da compilare con le informazioni utili all'Autorità per valutare la sussistenza dei presupposti per inoltrare alla Società i dati di contatto del segnalante in vista dell'applicazione, da parte della Società stessa, di misure tecniche di blocco preventivo sulle immagini indicate dal segnalante (comunicato stampa 5 marzo 2021, doc. web n. 9553419).

Le segnalazioni ricevute da marzo fino alla fine dell'anno (circa un centinaio) sono state curate dall'Autorità nell'ambito del progetto sopramenzionato. Tuttavia la prospettiva di coinvolgere il Garante nel quadro di un'azione preventiva più ampia del fenomeno si è tradotta in una disposizione normativa, introdotta in prima battuta con il d.l. 8 ottobre 2021, n. 139 poi convertito con modificazioni dalla legge 3 dicembre 2021, n. 205, confluita nel nuovo art.144-*bis* del Codice.

In particolare, la citata disposizione ha attribuito al Garante la competenza a ricevere segnalazioni da parte di "chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso".

In base alla disposizione l'Autorità, una volta ricevuta la segnalazione e verificata la sua riconducibilità alla fattispecie sopra descritta, decide in base ai poteri conferitegli dal Codice (artt. 143 e 144).

Alla luce di tale novità legislativa, la collaborazione al progetto NCII è stata affiancata, sul finire dell'anno, dalla predisposizione delle azioni volte a coinvolgere i soggetti tramite i quali i contenuti "destinati a rimanere privati" potrebbero essere veicolati (i fornitori di servizi di condivisione di contenuti audiovisivi, ovunque stabiliti, che erogano servizi accessibili in Italia), in vista della individuazione di un recapito – da fornire al Garante o da pubblicare nel proprio sito internet – al quale possano essere comunicati i provvedimenti adottati dall'Autorità nel dare seguito alle segnalazioni ricevute e in vista dell'implementazione, da parte degli stessi, di strumenti tecnici e organizzativi volti a prevenire la paventata e non autorizzata circolazione dei contenuti descritti (art 144-*bis,* comma 6, del Codice).

12 *Marketing* e trattamento dei dati personali

12.1. *Il fenomeno del* marketing *indesiderato e l'azione di contrasto*

Le comunicazioni indesiderate a carattere commerciale e promozionale, veicolate attraverso contatti effettuati con operatore umano ovvero con strumenti automatizzati (sms, *e-mail,* fax, chiamate pre-registrate), sono state oggetto della costante azione di osservazione e contrasto dell'Autorità, anche per la capacità dell'intero fenomeno di creare un indotto di illiceità che investe numerose fasi del trattamento dei dati, quali la formazione delle banche dati, la comunicazione dei dati, i criteri di acquisizione del consenso, l'esercizio dei diritti degli interessati, la sicurezza nelle comunicazioni elettroniche. Ciò che maggiormente viene percepito dall'interessato è la lesione del diritto alla propria tranquillità individuale, ma il complesso delle violazioni alla base di un contatto indesiderato investe una dimensione più ampia che attiene alla perdita del controllo dei dati personali da parte dell'interessato medesimo, dati (di contatto, di identificazione, di pagamento, ecc.) esposti quindi a rischi di utilizzi illeciti di diversa natura.

Con riferimento agli aspetti legati al consenso, con d.l. 8 ottobre 2021, n. 139, convertito con l. 3 dicembre 2021, n. 205, è stata modificata la l. 11 gennaio 2018, n. 5, per estendere la validità della revoca del consenso anche alla ricezione delle chiamate automatizzate. Da tale modifica deve conseguire l'aggiornamento del regolamento che disciplina il funzionamento del Registro delle opposizioni (attualmente d.P.R. n. 178/2020), per consentire l'iscrizione nel registro delle utenze attualmente non presenti negli elenchi telefonici pubblici nonché per consentire, tramite l'iscrizione stessa, la contestuale revoca di tutti i consensi precedentemente prestati ai titolari del trattamento per la ricezione di chiamate promozionali.

12.2. Telemarketing

Le attività di *telemarketing* hanno determinato il concentrarsi presso l'Autorità del maggior numero di segnalazioni e reclami relativi ai contatti indesiderati per finalità commerciali o promozionali. Ciò in ragione del fatto che tali attività sono diffusamente impiegate da grandi compagnie del settore telefonico ed energetico in grado di sviluppare, attraverso le loro reti di agenzie, una grande quantità di chiamate pubblicitarie.

Il complessivo fenomeno del *telemarketing* selvaggio ha caratteristiche ricorrenti e facilmente riconoscibili, la prima delle quali è indubbiamente rappresentata dalla circostanza che le telefonate indesiderate vengono effettuate in gran parte da numerazioni non censite presso il Registro degli operatori di comunicazione (Roc), al quale devono invece obbligatoriamente iscriversi tutti gli operatori economici esercenti l'attività di *call center.* Tali numerazioni sono spesso disconosciute dalla rete di vendita delle compagnie committenti e le chiamate che partono da tali numerazioni realizzano quello che il Garante, in numerosi provvedimenti, ha definito un "sottobosco" illecito, che realizza un rilevantissimo volume di affari attraverso attività in gran parte illegittime.

12

In tale direzione il Garante ha adottato un provvedimento nei confronti di una importante compagnia telefonica con riferimento al complesso dei trattamenti finalizzati alla promozione di propri servizi o offerte e all'acquisizione di nuovi clienti. Il provvedimento, nel solco dei precedenti, ha accertato che la compagnia non ha posto in essere adeguati controlli della filiera di raccolta dei dati personali utilizzati per il primo contatto di potenziali clienti, rendendo quindi possibile il realizzarsi di condotte illecite di trattamenti di dati con finalità promozionali, in violazione del principio di responsabilizzazione stabilito dall'art. 5, par. 2, del RGPD. Tali condotte sono emerse con evidenza in ragione dell'importante numero di segnalazioni e reclami pervenuti al Garante e della circostanza che gran parte dei contatti illeciti (circa il 70%) sono stati effettuati da numerazioni telefoniche non incardinate nella rete di vendita del titolare e non censite nel Roc. Nel provvedimento è stato osservato che il fenomeno può essere arginato da parte del titolare del trattamento "configurando i propri sistemi in modo da poter bloccare le procedure di attivazione di offerte o servizi laddove la Società non sia in grado di garantire che l'attività promozionale si sia svolta nel rispetto delle norme e dei diritti degli interessati, fin dal momento del primo contatto. In tal senso, per ogni attivazione, i sistemi della Società, oltre a richiedere l'indicazione della lista di contatto utilizzata (con i vincoli di validità temporale coerenti con la data del primo contatto), dovrebbero richiedere ulteriori elementi necessari per determinare la correttezza dello svolgimento del contatto promozionale (ad es. indicazione del *partner* che ha operato il primo e i successivi contatti; indicazione delle numerazioni telefoniche chiamanti - debitamente censite nel Roc, registro degli operatori di comunicazione; *script* di chiamata e informativa letti dall'operatore di *call-center*). Le conseguenze connesse alla mancata valorizzazione di tali informazioni dovrebbero in ogni caso poter prevedere, in ragione della potenziale illiceità dei trattamenti, anche l'inutilizzabilità dei dati (ex art. 2-*decies* del Codice) ovvero il "blocco" dell'attivazione di contratti che non rispettino determinati requisiti".

Sono emerse anche criticità relative alle modalità di acquisizione delle liste di anagrafiche utilizzate dalla rete di vendita della compagnia telefonica per il contatto dei potenziali clienti: tale acquisizione avveniva attraverso plurimi passaggi fra diversi titolari del trattamento senza che ciascuno di essi avesse acquisito dagli interessati il consenso alla comunicazione dei propri dati, oppure in *partnership* con altre aziende, operazione che non garantiva la lecita comunicazione dei dati personali fra titolari. Il Garante ha pertanto disposto il divieto dei trattamenti effettuato con l'utilizzo delle liste di anagrafiche così acquisite e ha applicato alla compagnia telefonica una sanzione amministrativa pecuniaria di euro 4.501.868,00 (provv. 25 marzo 2021, n. 112, doc. web n. 9570997).

L'Autorità ha inoltre adottato un provvedimento nei confronti di un'azienda che offre contenuti televisivi mediante una piattaforma a pagamento, a seguito di una complessa istruttoria avviata in relazione alla ricezione di diverse decine di segnalazioni e reclami inviati da interessati che lamentavano continui contatti telefonici indesiderati effettuati dalla rete di vendita della società. In questo caso le contestazioni del Garante si sono concentrate principalmente sui mancati controlli del titolare sulle liste di contattabilità acquisite da soggetti terzi, cosicché, in talune circostanze, venivano raggiunti da comunicazioni promozionali anche soggetti che avevano espresso la propria opposizione ai trattamenti per finalità pubblicitarie ovvero soggetti che non avevano espresso alcun consenso ai trattamenti. L'intervento correttivo e sanzionatorio dell'Autorità ha avuto come elemento centrale il ripristino del pieno controllo dei dati personali da parte degli interessati, poiché le diverse acquisizioni di banche di dati da soggetti esterni, unitamente alle scarse indicazioni fornite dalla

12

società in sede di informativa, avevano reso estremamente complicato per gli interessati stessi risalire all'originario titolare del trattamento dei dati e alle modalità con le quali, a suo tempo, il consenso era stato rilasciato. Inoltre, sono state accertate carenze e criticità nella distribuzione delle responsabilità fra i diversi *partner* commerciali nell'ambito del trattamento. Il Garante ha pertanto imposto all'azienda il divieto di ogni ulteriore trattamento con finalità promozionali e commerciali effettuato mediante liste acquisite da soggetti terzi in assenza di efficaci verifiche sulla liceità della comunicazione dei dati nonché in carenza di un'idonea informativa e un legittimo consenso; ha prescritto alla società di adeguare i trattamenti in materia di *telemarketing* al fine di prevedere che i contatti promozionali svolti mediante i *partner*/fornitori siano preceduti dalla designazione degli stessi quali responsabili di tutte le fasi del trattamento; ha quindi applicato una sanzione amministrativa pecuniaria di euro 3.296.326,00 (provv. 16 settembre 2021, n. 332, doc. web n. 9706389).

L'attività di contrasto al *telemarketing* selvaggio è stata condotta anche attraverso l'osservazione degli esiti dei provvedimenti adottati negli anni precedenti e lo sviluppo delle linee istruttorie evidenziate in tali provvedimenti.

Nell'ambito della complessa istruttoria che aveva condotto all'adozione del provvedimento 15 gennaio 2020, con il quale il Garante aveva disposto nei confronti di una nota compagnia telefonica numerose misure correttive, sono stati predisposti provvedimenti correttivi e sanzionatori nei confronti di tre società di *call center,* incaricate dalla medesima compagnia dell'effettuazione delle campagne promozionali, tramite contatti telefonici. I provvedimenti hanno evidenziato differenti livelli di gravità delle medesime violazioni riscontrate (attinenti, in particolare, alla disciplina del consenso e del principio di liceità del trattamento), in termini sia quantitativi (numero delle utenze contattate in assenza di idonea base giuridica), sia qualitativi. In particolare in uno dei tre provvedimenti sono emerse violazioni dei principi di correttezza e del diritto di opposizione degli interessati (contattati anche 155 volte in un solo mese): in tale provvedimento è stato ingiunto al titolare di adottare misure organizzative e tecniche per la corretta gestione del fenomeno delle chiamate rivolte ad utenze cd. fuori lista; all'inserimento in *black-list* dei dati degli interessati che in qualunque modo si oppongano al trattamento. Con tali misure si è inteso garantire la legittimità dei trattamenti e l'introduzione di modalità corrette e non invasive nello svolgimento delle telefonate promozionali e nell'eventuale utilizzo di altri mezzi al medesimo fine, a tutela effettiva dei vari diritti connessi alla protezione dei dati, come quello alla tranquillità individuale (provv.ti 11 marzo 2021, n. 98, doc. web n. 9577371; n. 99, doc. web n. 9577065 e n. 100, doc. web n. 9577042).

L'Autorità ha avviato numerose istruttorie relative alle attività promozionali tramite *telemarketing* poste in essere da agenzie immobiliari. In tali istruttorie sono emersi elementi di criticità riconducibili ad una non corretta raccolta dei dati, anche tramite internet, e un utilizzo degli stessi che talvolta non ha tenuto conto della necessaria separazione fra attività connesse alla gestione del mandato conferito dal cliente, la cui base di liceità deriva dal rapporto contrattuale in essere, e attività promozionale, che dovrebbe invece essere realizzata solo previo consenso.

A seguito di una segnalazione con la quale veniva lamentata la ricezione di numerose telefonate indesiderate su un'utenza iscritta nel Registro pubblico delle opposizioni per conto di una società operante nel settore delle agenzie immobiliari, l'Autorità ha condotto accertamenti riguardo ai trattamenti di dati posti in essere dalla medesima, anche con riferimento al sito web, in particolare, ai testi dell'informativa *privacy* e dell'informativa relativa alla *newsletter.* Al completamento dell'istruttoria, il Garante ha adottato un provvedimento correttivo e sanzionatorio nei confronti della società. Dagli elementi complessivamente raccolti è emersa, oltre ad un'evidente incoerenza

tra i trattamenti descritti nelle informative ed i trattamenti effettivamente svolti, anche la mancata acquisizione di un consenso adeguatamente informato, libero e specifico per ciascuna delle finalità indicate nelle menzionate informative. Inoltre la carenza di alcune informazioni nei testi delle citate informative, ricavabili invece dal *form* di raccolta dati, non può ritenersi superata dal fatto che i dati possano essere conosciuti *aliunde,* né può considerarsi idoneo, e quindi legittimo, un meccanismo che costringa l'interessato ad effettuare ricerche nel sito web per poter acquisire tutte le informazioni obbligatoriamente previste dall'art. 13 del RGPD, contravvenendo, così, anche al requisito di facile accessibilità e fruibilità delle informazioni previsto dall'art. 12 del RGPD, nel più ampio contesto del basilare principio di trasparenza. Si è pertanto disposto nei confronti della società il divieto del trattamento dei dati personali degli interessati, per i quali la medesima non avesse acquisito un consenso adeguatamente informato, libero e specifico per ciascuna delle finalità menzionate nelle citate informative, nonché l'implementazione di misure tecniche ed organizzative tali da assicurare che vengano trattati solo i dati personali per i quali si disponga di un consenso informato, libero e specifico oppure di un'altra idonea e documentata base giuridica (provv. 27 maggio 2021, n. 217, doc. web n. 9689375).

In un altro provvedimento nei confronti di un'agenzia immobiliare, il Garante si è occupato in particolare delle modalità con le quali il titolare dei trattamenti svolti per finalità promozionali nell'ambito di attività di *telemarketing* ha reso possibile l'esercizio dei diritti di accesso e di opposizione previsti dagli artt. 15 e 21 del RGPD. Dall'istruttoria, avviata a seguito di reclamo, è emerso che l'agenzia aveva ripetutamente contattato telefonicamente un interessato per proporre i propri servizi, reiterando la condotta nonostante quest'ultimo avesse più volte richiesto di interrompere i contatti; l'agente, per promuovere i propri servizi, aveva inoltre utilizzato indebitamente anche il recapito del padre del reclamante mettendolo così a conoscenza della vendita dell'immobile. Nel corso dell'istruttoria il titolare non è stato in grado di documentare la fonte da cui aveva acquisito i dati del padre del reclamante ma ha assicurato di aver provveduto a recepire l'opposizione dell'interessato. Il Garante pertanto ha rivolto un ammonimento alla società e le ha ordinato di cancellare i dati del reclamante (provv. 25 marzo 2021, n. 114, doc. web n. 9584572).

Un elemento ricorrente nell'ambito del *telemarketing* selvaggio è quello delle numerose segnalazioni relative a telefonate promozionali provenienti da soggetti, o effettuate per conto di committenti, non individuati, o nelle quali non sono state indicate le numerazioni chiamanti o altri elementi (come la data e l'ora dei contatti indesiderati) essenziali ai fini di un'efficace attività di controllo dell'Autorità. Molto spesso la carenza di informazioni non dipende dalla completezza delle segnalazioni ma da un approccio da parte dell'operatore che effettua il contatto promozionale, volutamente confuso e privo di elementi chiari in ordine alla riconducibilità delle campagne pubblicitarie e ai termini delle offerte, approccio che caratterizza coloro che si muovono nel sottobosco delle attività di *marketing.*

Con riguardo a tali segnalazioni l'Ufficio – oltre ad aver rilevato numerosi casi di *spoofing* (utilizzo di numerazioni Voip non riconducibili a specifiche e reali intestazioni con conseguente occultamento della reale linea telefonica) – ha sistematicamente ricercato le numerazioni chiamanti, indicate dagli interessati, sul Registro degli operatori di comunicazione pubblicato nel sito web dell'Agcom, comunicando l'esito delle verifiche svolte nelle note di chiarimenti destinate ai segnalanti e censendo le società rilevate in un *dossier* appositamente predisposto per monitorare il fenomeno del *marketing* indesiderato da parte di tali operatori telefonici, nella prospettiva di promuovere l'esame organico delle doglianze avanzate nei confronti del

12

Utilizzo di *call center* ubicati fuori dall'Unione europea

medesimo titolare. Nella gestione delle variegate istanze, spesso è emerso il problema dell'irreperibilità di vari titolari collocati al di fuori del territorio dell'Unione europea che, pur avendo l'obbligo di nomina di un rappresentante stabilito nell'UE, non vi ottemperano.

Anche nel corso del 2021, 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,* decreto legge 22 giugno 2012, n. 83, come sostituito dall'art. 1, comma 243, legge 11 dicembre 2016, n. 232.

12.2.1. Il telemarketing *nel settore energetico*

Il Garante ha verificato come il *telemarketing* selvaggio nel settore energetico, con l'approssimarsi della scadenza per il passaggio dal mercato tutelato dell'energia elettrica e del gas al mercato libero, abbia registrato un netto e preoccupante incremento.

Nelle istruttorie condotte dall'Autorità è emerso un cronico, intenso e sempre più invasivo fenomeno di telefonate promozionali indesiderate, in assenza del necessario consenso, verso utenze riservate o iscritte al Registro delle opposizioni, oltre al tardivo o mancato riscontro a istanze di esercizio dei diritti di accesso ai dati personali o di opposizione al trattamento per finalità di *marketing.*

Il fenomeno è risultato avere connotati di maggiore pervasività rispetto alle altre forme di *telemarketing,* anche in considerazione della circostanza che le offerte commerciali sono state spesso veicolate con modalità di scarsa trasparenza con riferimento sia alle condizioni economiche sia alle compagnie energetiche che le propongono.

Una compagnia energetica di primaria importanza in campo nazionale è stata raggiunta da una sanzione per il trattamento illecito dei dati personali degli utenti a fini di *telemarketing.* Oltre al pagamento della multa, l'Autorità ha prescritto alla compagnia di adottare una serie di misure correttive per adeguare il trattamento al quadro normativo vigente. Il provvedimento è giunto al termine di una complessa attività avviata dall'Autorità a seguito di centinaia di segnalazioni e reclami di utenti che lamentavano la ricezione, in nome e per conto della compagnia energetica, di telefonate promozionali indesiderate, e evidenziavano la difficoltà di esercitare i propri diritti in tema di protezione dei dati personali e, più in generale, problemi derivanti dalla gestione dei dati nell'ambito dei servizi di fornitura energetica, ivi compresi i trattamenti svolti tramite l'area riservata del sito della società e la *app* di gestione dei consumi (provv. 16 dicembre 2021, n. 443, doc. web n. 9735672).

Nel provvedimento, l'Autorità ha rilevato come, in base al principio di responsabilizzazione previsto dal RGPD, non fosse più sufficiente per la compagnia dichiarare la propria estraneità alla maggior parte delle telefonate indesiderate. Infatti i principi di *accountability* e *privacy by design* richiedono un'ottica proattiva e un approccio non meramente formalistico da parte del titolare del trattamento, imponendogli un'opera di costante vigilanza e monitoraggio sull'intera filiera e l'adozione di specifiche misure idonee a contrastare il fenomeno del *telemarketing* selvaggio. Le misure delineate riguardano principalmente il sistema di controlli per documentare l'origine dei dati delle persone contattate; i meccanismi di verifica del rispetto della normativa *privacy* da parte di tutti i soggetti coinvolti nella filiera dei trattamenti; le scelte societarie e organizzative per impedire l'attivazione di offerte o servizi in caso di dubbi sulla provenienza dei dati o sul rispetto delle norme a tutela degli utenti. Una assenza di misure, nel sistema ufficiale di registrazione dei contratti può favorire la creazione di una porta d'accesso per eventuali "procacciatori non ufficiali" di contratti in grado di "catturare" gli utenti destinatari delle lamentate telefonate promozionali.

Il Garante ha inoltre rilevato che la compagnia, fino a giugno 2021, presentava

nell'area riservata del proprio sito web una informativa priva delle necessarie indicazioni sui destinatari dei dati raccolti sia nell'ambito del proprio gruppo di imprese, sia con riferimento ai *partner* commerciali. Il Garante ha anche accertato che la compagnia raccoglieva un consenso unico alla comunicazione dei dati per finalità promozionali anche da parte di società del gruppo, società controllanti, controllate e collegate e *partner* commerciali. Tale tipologia di consenso non può considerarsi né specifico né libero e non costituisce una idonea base giuridica per i trattamenti. L'Autorità ha ingiunto alla compagnia di adeguare ogni trattamento di dati svolto dalla rete di vendita a modalità e misure idonee a comprovare che l'attivazione di offerte e servizi e l'attivazione di contratti avvenga solo a seguito di contatti promozionali su numerazioni telefoniche censite e iscritte al Registro degli operatori della comunicazione (Roc), nonché di introdurre ulteriori misure tecniche e organizzative per gestire le istanze di esercizio dei diritti degli interessati, in particolare il diritto di opposizione alle finalità promozionali, in modo da dare riscontro agli interessati non oltre 30 giorni dalla richiesta.

Il Garante ha comminato una sanzione ad un'altra società operante nel settore energetico, per non aver verificato che tutti i passaggi dei dati dei destinatari delle promozioni fossero autorizzati da consenso. A seguito di diversi reclami e segnalazioni è emerso che la società aveva trattato dati personali per attività di *telemarketing,* che non aveva raccolto direttamente, ma aveva acquisito da altre fonti. La compagnia energetica infatti aveva ottenuto liste di anagrafiche da una società, che, a sua volta, le aveva acquisite, in veste di autonomo titolare del trattamento, da altre due aziende. Queste ultime avevano ottenuto il consenso dei potenziali clienti per il *telemarketing* effettuato sia da loro che da parte di terzi, ma tale consenso non costituiva una legittima base giuridica per il passaggio dei dati dei clienti dalla prima società alla compagnia energetica (provv. 13 maggio 2021, n. 192, doc. web n. 9670025).

Nei due provvedimenti sopra richiamati il Garante ha infine evidenziato che le compagnie avevano fornito una rappresentazione ed una documentazione probatoria incompleta ed inidonea durante l'istruttoria oltre che un'insufficiente collaborazione nelle diverse fasi del procedimento. Tale aspetto può costituire un forte ostacolo al completamento degli accertamenti in particolare nei casi in cui i titolari del trattamento sono organizzati in strutture molto complesse e ha rappresentato un elemento di grande difficoltà nel periodo dell'emergenza pandemica, in ragione della necessaria limitazione delle attività ispettive dell'Autorità.

12.2.2. Le attività di marketing *tramite strumenti elettronici*

L'Autorità ha preso in esame numerosi reclami e segnalazioni relativi alle attività di *marketing* veicolate tramite la posta elettronica e gli sms. Tali segnalazioni, quantitativamente meno rilevanti di quelle in ambito telefonico, hanno evidenziato una molteplicità di elementi critici, in gran parte legate alla non corretta gestione delle richieste degli interessati di esercizio dei diritti garantiti dal Regolamento, in particolare il diritto di opposizione di cui all'art. 21, par. 2, del RGPD. In base a tale disposizione, infatti, è facoltà dell'interessato opporsi ai trattamenti aventi finalità promozionali senza fornire alcuna specifica motivazione: a fronte di tale opposizione, pertanto, la condotta degli operatori di *marketing* che reiterano l'invio dei messaggi promozionali, non solo realizza un trattamento illecito di dati personali, ma contrasta con il generale dovere del titolare di agevolare l'esercizio dei diritti e di dare all'interessato le informazioni relative alle azioni intraprese per rendere effettivo tale esercizio.

In tale ambito, il Garante, a seguito di due atti di reclamo, è intervenuto nei confronti di una società che inviava *e-mail* promozionali indesiderate senza dare

12

riscontro alle richieste di opposizione degli interessati e le ha ingiunto di adottare le misure organizzative necessarie per fornire una risposta immediata a chi si oppone al *direct marketing*. L'attività istruttoria è stata peraltro aggravata dalla scarsa cooperazione del titolare: in mancanza di riscontro alle reiterate richieste di informazioni, si è infatti resa necessaria un'attività ispettiva che ha accertato l'impossibilità, da parte della società, di documentare l'origine dei dati utilizzati per le campagne di *marketing* e ha confermato i mancati riscontri alle richieste di esercizio dei diritti, dovuti, in base alle risultanze ispettive, a problemi organizzativi e di funzionamento dei sistemi. Il Garante ha quindi adottato nei confronti della società un provvedimento inibitorio e sanzionatorio, vietando il trattamento dei dati senza consenso e, applicando una sanzione amministrativa per non aver fornito la dovuta collaborazione e per le violazioni accertate (provv. 25 marzo 2021, n. 113, doc. web n. 9577323).

A seguito di reclamo, il Garante è intervenuto nei confronti di una società che inviava *e-mail* con offerte di collaborazione a professionisti senza alcuna possibilità per i riceventi di opporsi o di richiedere l'accesso ai dati personali, stante l'assoluta mancanza di indicazioni in merito al reale mittente. La stessa mancanza di trasparenza ha reso necessaria l'effettuazione di indagini straordinarie per individuare il titolare del trattamento, con l'acquisizione di informazioni da un soggetto terzo, fornitore della piattaforma di invio dei messaggi, individuato tramite analisi informatiche delle *e-mail*. La condotta della società è stata valutata come gravemente lesiva sia dei diritti degli interessati che del corretto svolgimento dall'attività istruttoria del Garante dal momento che l'Ufficio, come detto, ha dovuto attivare modalità supplementari di indagine, in luogo dell'ordinaria attività amministrativa che, con la cooperazione dei titolari del trattamento, solitamente consente una più semplice definizione dei procedimenti. L'Autorità ha pertanto adottato un provvedimento di carattere sanzionatorio nei confronti della società (provv. 24 giugno 2021, n. 257, doc. web n. 9689637).

In tema di esercizio dei diritti degli interessati e di distribuzione delle responsabilità nell'ambito delle attività promozionali effettuate mediante l'invio di sms, il Garante ha adottato un provvedimento inibitorio e sanzionatorio nei confronti di una società (provv. 2 dicembre 2021, n. 424, doc. web n. 9731682), segnalata da numerosi interessati in ragione degli inadeguati riscontri alle istanze di accesso ai dati e di opposizione al trattamento. In sede istruttoria, il titolare si è limitato a rispondere al Garante di non avere alcun ruolo nel trattamento e di aver incaricato al riguardo un proprio fornitore di servizi. Quest'ultimo ha rappresentato di non poter documentare l'acquisizione di idonei consensi al trattamento per finalità promozionali. Allo stesso modo, nessuna documentazione è stata fornita dalle due società con riferimento ai rapporti contrattuali fra loro, alla distribuzione delle responsabilità nel trattamento, all'origine dei dati e alle attività di vigilanza che il titolare avrebbe svolto in ordine alle attività del *partner*. All'esito dell'istruttoria il Garante ha adottato un provvedimento sanzionatorio anche nei confronti della società *partner* (provv. 2 dicembre 2021, n. 425, doc. web n. 9731664).

Con due diversi reclami è stato richiesto al Garante di intervenire per arginare la ricezione di sms promozionali per un noto marchio commerciale. Attraverso l'istruttoria, l'Autorità ha potuto accertare le modalità di realizzazione della campagna promozionale che, oltre al committente e al suo fornitore di servizi, ha visto coinvolti altri soggetti con una prospettazione dei ruoli, in concreto, molto diversa da quella che si erano riconosciute formalmente le parti.

Inoltre, le verifiche documentali e gli accertamenti d'ufficio, hanno permesso di acquisire elementi in merito alla prassi, molto diffusa nella realizzazione di campagne *marketing*, di avvalersi di catene di subappalti fino ad arrivare a *list provider*

stabiliti al di fuori del territorio dell'Unione europea che non offrono sufficienti garanzie in merito alla liceità della raccolta dei dati. Nel caso in esame, in particolare, sono stati acquisiti elementi sull'origine delle banche dati da ricondursi ad un soggetto con sede in Florida e ad un altro con sede in Svizzera nei confronti dei quali erano pervenute anche ulteriori segnalazioni. In questi casi, la delocalizzazione e la mancanza di un rappresentante in UE (ai sensi dell'art. 27 del RGPD) hanno ostacolato l'esercizio dei diritti da parte degli interessati e reso maggiormente gravosa l'istruttoria svolta dall'Autorità.

Il Garante pertanto è intervenuto con tre distinti provvedimenti nei confronti del committente titolare del trattamento, del responsabile che acquisiva le banche dati per conto del titolare, e di una società terza che, nel corso dell'istruttoria ha omesso di fornire riscontro alle richieste di informazioni formulate dall'Autorità. Con i provvedimenti di carattere correttivo e sanzionatorio l'Autorità ha ricordato che l'ordinato svolgimento delle attività di *marketing,* con l'utilizzo di dati raccolti lecitamente e aggiornati, oltre ad evitare pericolose derive (quali *phishing* e truffe), giova al mercato stesso tutelando gli operatori virtuosi e rafforzando la fiducia degli interessati. È pertanto necessario adottare la massima diligenza nella selezione delle banche dati. Il Garante ha altresì evidenziato che le condotte del titolare e del responsabile sono state connotate da grave negligenza dal momento che, pur essendovi palesi elementi di non conformità delle banche dati formate da soggetti stabiliti fuori dall'Unione europea e privi di rappresentante in ambito eurounitario, le due società le hanno ugualmente utilizzate per realizzare, per la durata di due anni, campagne promozionali destinate a milioni di interessati (provv.ti 25 novembre 2021, n. 412, doc. web n. 9736961; n. 413, doc. web n. 9737185; n. 414, doc. web n. 9738356).

12.2.3. Altre forme di marketing

Il Garante, a seguito di reclamo, è intervenuto nei confronti di un titolare che, dopo aver mandato un messaggio promozionale tramite posta cartacea, non aveva dato alcun riscontro alla richiesta di esercizio dei diritti dell'interessato. La società non ha risposto neanche alle due richieste di informazioni inviate dall'Ufficio ed è stato necessario richiedere un approfondimento istruttorio da parte della Guardia di finanza nel corso del quale il titolare ha fornito risposte sommarie, dichiarandosi estraneo al trattamento poiché questo era stato affidato ad un terzo, nominato responsabile. Dall'esame degli atti è emerso che tale responsabile aveva affidato a sua volta il trattamento ad un sub-responsabile all'insaputa del titolare, che comunque non aveva effettuato alcun controllo. Il soggetto che materialmente ha provveduto a realizzare la campagna promozionale ha dichiarato di aver utilizzato per errore una lista non aggiornata ma non ha fornito alcun chiarimento in merito all'origine di tale lista.

Ciò che è stato considerato maggiormente meritevole di attenzione non è stato solo l'invio del messaggio promozionale, privo di base giuridica, ma soprattutto la generale mancanza di adeguate misure organizzative, venuta in rilievo proprio grazie al reclamo originato da tale invio.

Pertanto è stato ribadito in linea generale che assume la veste giuridica del titolare il soggetto che stabilisce finalità e modalità del trattamento e, nel caso specifico, è stata dichiarata l'illiceità della condotta del titolare individuato nel reclamo con riguardo all'invio di comunicazioni promozionali senza consenso, al mancato rispetto degli obblighi di trasparenza informativa, al mancato riscontro alle richieste dell'Autorità e alla mancanza di misure organizzative adeguate a garantire la liceità dei trattamenti effettuati dal responsabile. Di conseguenza sono state impartite al medesimo specifiche prescrizioni per adeguare le proprie attività di trattamento alla

12

vigente normativa ed è stato imposto il divieto di utilizzare dati personali di soggetti per i quali non si sia in grado di dimostrare l'acquisizione di un idoneo consenso.

Inoltre, considerate le violazioni accertate e l'insufficiente adeguamento delle misure, si è ritenuto necessario imporre anche una sanzione amministrativa pecuniaria, (provv. 16 dicembre 2021, n. 444, doc. web n. 9742704).

13 Internet e servizi di comunicazione elettronica

13.1. *La libertà del consenso nei servizi fungibili*

La prassi, sempre più frequente, di vincolare l'utilizzo di un bene o di un servizio digitale al consenso per il trattamento dei dati personali dell'interessato anche per finalità promozionali e per la creazione di profili di consumatore o di utente, è stata presa in esame dal Garante anche per le possibili ricadute che tale prassi può determinare sulla rimodulazione del concetto stesso di dato personale, da nucleo centrale di un diritto inalienabile della persona a veicolo di prestazioni economiche che ancora oggi appaiono largamente incompatibili con l'impianto generale della protezione dei dati personali.

A seguito di un reclamo il Garante ha impartito misure correttive e sanzionatorie ad una società di *e-commerce* che vincolava il perfezionamento del processo di acquisto al consenso a ricevere messaggi promozionali, giustificando la propria scelta imprenditoriale con il fatto che il servizio offerto era da considerarsi fungibile. Oltre a provvedere in merito alla liceità delle basi giuridiche scelte dal titolare del trattamento, il Garante è stato dunque chiamato ad esprimersi sulle condizioni di validità del consenso e sulla possibilità di condizionarlo nel caso in cui il titolare offra servizi fungibili – cioè facilmente rinunciabili o sostituibili senza grande pregiudizio per l'interessato – richiamando le differenziate posizioni già espresse sul punto dalla Corte di cassazione, con sentenza n. 17278/2018, e dall'EDPB con le linee guida sul consenso 5/2020. Se infatti, entrambe le posizioni ammettono una condizionalità del consenso a fronte di una valida alternativa per l'interessato (al fine di ridurne il pregiudizio), la Cassazione consente la ricerca del servizio fungibile nell'intero mercato mentre l'EDPB ritiene inapplicabile, e di conseguenza illecita, tale prospettiva ammettendo una condizionalità solo nel caso in cui il servizio alternativo sia fornito dallo stesso titolare del trattamento.

In tale contesto, l'Autorità ha ritenuto che il consenso acquisito non poteva essere considerato libero dal momento che non poteva neanche definirsi necessario per l'esecuzione del contratto cui si pretendeva di subordinarlo, in contrasto con il disposto dell'art. 7, par. 4, del RGPD. Ciò in quanto il servizio offerto dal titolare consisteva nella vendita di prodotti per l'attività odontoiatrica; vendita a fronte della quale l'acquirente pagava una somma di denaro perfezionando così il rapporto a prestazioni corrispettive. Il conferimento di un consenso per le finalità di *marketing,* dunque, è apparso del tutto estraneo al rapporto sinallagmatico in questione dal momento che il pagamento del prezzo di vendita era condizione sufficiente a concludere il contratto a fronte, invece, della natura del tutto autonoma del trattamento per finalità promozionali (provv. 27 gennaio 2021, n. 119, doc. web n. 9711630).

Il Garante ha avviato ulteriori istruttorie riguardanti iniziative imprenditoriali che si incentrano su possibili forme di valorizzazione, arricchimento e scambio dei dati personali nell'ambito di un rapporto contrattuale, istruttorie che hanno preso in esame i modelli di *business* presenti nel mercato, anche con riferimento ai programmi di fidelizzazione, in particolare sviluppati in forma aggregata e integrata, e di *cashback.* Le istruttorie, in corso di svolgimento, hanno evidenziato la necessità di mettere in correlazione gli elementi acquisiti con le informazioni ricavabili dagli

13

approfondimenti sul tema dei *data analytics* e dei processi di profilazione, poiché appare sempre più evidente che il tema centrale della libertà del consenso e dello sfruttamento del valore informativo del dato personale deve essere posto in collegamento funzionale con la profondità delle analisi che proprio sul dato personale possono essere effettuate, analisi idonee a sviluppare profili personali distanti dalla percezione e dal controllo dell'interessato.

13.2. *Conservazione e accesso ai dati di traffico telematico e telefonico*

Nel 2021, un particolare impegno ha richiesto, anche in ragione delle significative modifiche normative introdotte con il d.l. 30 settembre 2021 n. 132, la trattazione di più doglianze in materia di *data retention,* e in particolare, di mancato o tardivo riscontro ad istanze di accesso ai tabulati per finalità giudiziarie.

In particolare, con tre provvedimenti nei confronti della medesima compagnia telefonica è stata accertata la legittimità di alcune istanze di accesso ai dati di traffico presentate da legali di imputati per finalità di indagini difensive ed è altresì risultato violato il diritto di accesso ex artt. 15 del RGPD e 132 del Codice. I provvedimenti hanno formato oggetto d'impugnazione presso il Giudice ordinario da parte della suindicata società (provv.ti 27 maggio 2021, n. 216, doc. web n. 9689324; 8 luglio 2021, n. 272, doc. web n. 9693464; 11 novembre 2021, n. 401, doc. web n. 9722894).

Con il primo provvedimento si è ingiunto alla compagnia di fornire senza ritardo all'interessato i dati in questione, ribadendo che il diritto ad ottenerli si cristallizza all'atto della presentazione di una tempestiva e corretta richiesta di accesso e che il tempo assorbito dalle procedure (in questo caso anche non pienamente conformi alla vigente normativa) non può andare a detrimento del diritto dell'interessato, determinando uno slittamento in avanti dei termini di conservazione dei dati e la conseguente perdita del patrimonio informativo richiesto. In tal senso è stata evidenziata l'opportunità di procedere ad una sorta di "congelamento" dei dati richiesti all'atto della presentazione dell'istanza, al fine di evitare il rischio che parte di essi, nel corso della procedura, superino i termini di conservazione previsti e siano pertanto non più ostensibili, ribadendo in ogni caso, a prescindere dalle modalità operative adottate, l'obbligo in capo alla compagnia di consegnare i dati ricompresi nell'arco temporale individuato nell'istanza.

In generale, i provvedimenti hanno confermato l'obbligo della compagnia telefonica di adottare soluzioni tecniche idonee al recupero dei tabulati che, nel caso di decorrenza del termine di 24 mesi dalla generazione del traffico, sono conservati unicamente nei *database* riservati alle richieste dell'Autorità giudiziaria nelle attività di contrasto a particolari gravi reati (perlopiù connessi alla criminalità organizzata).

13.3. *Raccolta di dati* online

L'Autorità ha completato l'istruttoria avviata a seguito di un reclamo concernente vari trattamenti, non assistiti da un adeguato consenso informato o da altre idonee basi giuridiche, con specifico riferimento all'invio di comunicazioni promozionali ai promotori finanziari i cui dati di contatto erano stati tratti dall'albo pubblico *online* di tali professionisti. Considerati in particolare il livello tenue della violazione, l'assenza di precedenti specifici nonché il modesto importo del fatturato, si è ritenuto di adottare, nei confronti della società, titolare del sito, un provvedimento di

ammonimento sulla necessità di acquisire previamente un consenso libero e specifico, oltre che informato, degli interessati per l'invio di comunicazioni promozionali. Si è ritenuto altresì di non ingiungere, nel caso di specie, la limitazione definitiva del trattamento o l'adozione di apposite misure organizzative e tecniche, tenuto conto della dichiarata interruzione dell'attività promozionale in rilievo e dell'avvenuta presa di consapevolezza delle suesposte criticità da parte della società, come emergente dalla complessiva interlocuzione con l'Autorità (provv. 22 luglio 2021, n. 283, doc. web n. 9696708).

In tema di utilizzo, per l'invio di messaggi promozionali, di banche dati accessibili al pubblico, il Garante ha avviato un'istruttoria sulla base di numerose segnalazioni pervenute da parte di avvocati che lamentavano la ricezione di *e-mail* promozionali da parte di una società che aveva reperito i dati di contatto utilizzando gli indirizzi presenti in un registro pubblico. All'esito dell'istruttoria, che ha confermato le circostanze riportate dai segnalanti, il Garante ha dichiarato l'illiceità del trattamento, ne ha vietato la continuazione e ha ordinato alla società di cancellare i dati già acquisiti con le modalità contestate. Nel provvedimento si è osservato che la finalità pubblicistica del registro non può ricomprendere anche l'attività di contatto promozionale: "a tal riguardo si richiama quanto disposto dall'art. 130 del Codice in base al quale l'invio di comunicazioni con modalità automatizzate è consentito solo con il consenso del contraente o utente potendosi ammettere una deroga unicamente nel caso in cui l'indirizzo *e-mail* sia stato rilasciato dall'interessato nel contesto di una vendita di beni o servizi analoghi" (provv. 15 aprile 2021, n. 149, doc. web n. 9680996).

L'utilizzo di banche dati pubbliche ha formato oggetto di valutazione nell'ambito di un provvedimento adottato dal Garante nei confronti di un'agenzia che aveva inviato un contatto tramite un servizio web di rete sociale, finalizzato a proporre servizi immobiliari in riferimento ad uno specifico immobile di proprietà di un soggetto che aveva poi sporto reclamo innanzi al Garante. Nel corso dell'istruttoria svolta dall'Autorità è emerso che l'agenzia aveva acquisito informazioni in ordine alle proprietà del reclamante dai pubblici registri immobiliari e aveva quindi utilizzato il contatto presente nella rete sociale per accertare se l'interessato avesse intenzione di vendere l'immobile. Il Garante ha dichiarato l'illiceità del trattamento e ha ingiunto all'agenzia di adottare adeguate misure operative per conformare i trattamenti alla normativa vigente. Con il provvedimento l'Autorità ha osservato che l'utilizzo di dati per finalità diverse e incompatibili da quelle per cui sono stati originariamente raccolti, non può essere considerato lecito. Nel caso di specie, si è chiarito che le finalità per cui viene creato un profilo all'interno di una rete sociale da parte di un utente, anche se aperto alla ricezione di messaggi da parte di tutti gli iscritti, devono essere ricondotte a quanto riportato nelle condizioni contrattuali del servizio che non contemplano la possibilità di utilizzi per finalità promozionali. Analoghe considerazioni sono state fatte per i dati contenuti nei registri immobiliari il cui regime di pubblicità non ne autorizza l'uso per finalità diverse da quelle per le quali sono stati costituiti (provv. 16 settembre 2021, n. 316, doc. web n. 9705632).

13.4. *Violazioni di dati nelle reti sociali*

Con riferimento al grave *data breach* subito da Facebook nell'aprile 2021, che ha coinvolto i dati di circa 36 milioni di utenti italiani, compresi in molti casi numeri telefonici e indirizzi *e-mail,* disponibili *online* a seguito di una violazione dei sistemi della nota piattaforma di *social networking,* il Garante ha chiesto alla società di mettere a disposizione un servizio per consentire a tutti gli utenti italiani di verificare se

13

la propria numerazione telefonica o il proprio indirizzo *e-mail* fossero stati interessati dalla violazione. Inoltre, con un provvedimento a carattere generale il Garante ha avvertito chiunque fosse entrato in possesso dei dati personali provenienti da tale violazione, che il loro eventuale utilizzo sarebbe stato in contrasto con la normativa in materia di *privacy,* essendo tali informazioni frutto di un trattamento illecito. Il Garante ha, inoltre, invitato tutti gli utenti Facebook interessati dalla violazione a prestare particolare attenzione a eventuali anomalie connesse al funzionamento della propria utenza telefonica e, in tali ipotesi, a contattare immediatamente il *call center* del proprio operatore telefonico per verificare le ragioni del problema e, in particolare, per verificare che terzi non avessero chiesto e ottenuto un trasferimento della numerazione su un'altra SIM (provv. 6 aprile 2021, n. 130, doc. web n. 9574600).

In data 8 aprile 2021, a seguito della notizia di un altro rilevante *data breach* nei confronti dei sistemi di Linkedin che ha determinato la diffusione di dati di utenti, compresi Id, nominativi completi, indirizzi *e-mail,* numeri di telefono, collegamenti ad altri profili Linkedin e a quelli di altri *social media,* titoli professionali e altre informazioni lavorative inserite nei propri profili dagli utenti, il Garante ha adottato un analogo provvedimento di avvertimento generale. Anche in questo caso l'Autorità ha avvertito che l'eventuale utilizzo dei dati personali provenienti dalla menzionata violazione sarebbe stato in contrasto con la normativa in materia di protezione dei dati personali (essendo tali informazioni frutto di un trattamento illecito) e avrebbe potuto avere conseguenze anche di carattere sanzionatorio. Contestualmente, tenuto conto del fatto che l'Italia è uno dei Paesi europei con il numero maggiore di iscritti alla piattaforma, il Garante ha invitato tutti gli utenti interessati dalla violazione a prestare particolare attenzione a eventuali anomalie connesse al funzionamento della propria utenza telefonica e del proprio *account* (provv. 8 aprile 2021, n. 131, doc. web n. 9574917).

13.5. *Linee guida sui* cookie

Nell'ambito dei compiti istituzionali di sorveglianza sull'evoluzione delle nuove tecnologie dell'informazione e della comunicazione che incidono sulla protezione dei dati personali (art. 57, par.1, lett. *i*), del RGPD), l'Autorità ha curato nel 2021 la predisposizione del *draft* di linee guida in materia di *cookie* e altri strumenti di tracciamento che, nel rispetto di una logica il più possibile partecipativa, è stato sottoposto ad una specifica consultazione pubblica.

Nell'ambito di tale consultazione sono pervenuti al Garante circa 50 contributi provenienti da settori diversi, dal mondo dell'accademia a quello delle imprese, dalle associazioni di consumatori ai singoli sviluppatori o consulenti, ma anche da cittadini che hanno potuto, in tal modo, esprimersi direttamente su un argomento che interessa le quotidiane attività della navigazione *online.*

L'attività svolta ha condotto infine all'adozione delle linee guida in materia di *cookie* e altri strumenti di tracciamento (provv. 10 giugno 2021, n. 231, doc. web n. 9677876, in G.U. 9 luglio 2021, n. 163).

In tale documento, oltre alla ricostruzione della disciplina applicabile alla fattispecie, è stato previsto il termine di sei mesi dalla pubblicazione in G.U. per consentire ai soggetti tenuti agli adempimenti di conformare la propria condotta alle misure e agli obblighi vigenti.

In particolare il provvedimento ha riguardato: le modalità di acquisizione del consenso *online* sulla base dei nuovi criteri di *accountability* e di *privacy by design* e *by default* e l'obbligo, per i titolari del trattamento, di documentare ed eventualmente

aggiornare le scelte effettuate dagli utenti; è stata sottolineata la necessità di rendere una informativa più estesa rispetto al passato, anche su più canali e con diverse modalità. Sono stati chiariti i concetti di *scrolling* e di *cookie wall* con identificazione della disciplina applicabile, nonché le regole per la reiterazione nella presentazione del *banner* che, diversamente dal pregresso, non potrà più essere riproposto indefinitamente a ogni nuovo accesso dell'utente allo stesso sito, ma potrà essere nuovamente presentato solo al ricorrere di specifiche condizioni, tra cui il decorso di almeno sei mesi ovvero quando mutino significativamente le condizioni del trattamento.

L'Autorità ha inoltre chiarito le regole per la revoca del consenso e per il corretto ricorso ai *cookie analytics* di terze parti ed ha richiamato i soggetti coinvolti all'adozione di un sistema universalmente accettato di codifica semantica dei *cookie* e degli altri strumenti di tracciamento, che consenta di distinguere anche i *cookie* tecnici da quelli di profilazione.

A beneficio sia di coloro che sono tenuti agli adempimenti in questione, sia degli interessati, sono state inoltre predisposte e pubblicate nel sito istituzionale dell'Autorità le FAQ e la relativa scheda infografica sul tema.

13.6. *Procedure IMI relative a trattamenti di dati effettuati da fornitori di servizi della società dell'informazione*

Le procedure di cooperazione europea, che originano da trattamenti transfrontalieri di dati personali, assumono grande rilevanza nell'ambito dei servizi della società dell'informazione – per definizione non circoscrivibili in ambiti territoriali nazionali – e rappresentano ormai una parte fondamentale dell'attività svolta dall'Autorità (cfr. parte IV, tab. 10-12).

Nell'anno 2021 è stata registrata una significativa crescita, quantitativa e qualitativa, delle procedure di cooperazione attraverso cui sono state veicolate tematiche di primario interesse, in particolare con riferimento alla pubblicità *online*.

L'attività di cooperazione tra le autorità di controllo è stata anticipata e rafforzata sin dalla fase istruttoria al fine di perseguire la ricerca di un consenso condiviso come previsto dall'art. 60, par. 1, del RGPD.

In particolare sono giunti a decisione importanti procedimenti avviati nei confronti di grandi titolari internazionali stabiliti nell'Unione europea che hanno evidenziato la vitalità del meccanismo dello sportello unico introdotto dal RGPD. Il sistema amministrativo europeo che si basa sui due principi complementari di cooperazione (tra autorità di controllo) e di coerenza (tra autorità, EDPB e Commissione) è unico nel suo genere (i regolamenti successivi, ad es. il regolamento (UE) 2017/2394 in materia di tutela dei consumatori, non hanno introdotto meccanismi analoghi) e trova giustificazione nella necessità di garantire la massima tutela possibile al diritto alla protezione dei dati personali che rappresenta la cartina di tornasole della moderna ICT *society*.

L'attività svolta nel 2021 nell'ambito della cooperazione europea ha evidenziato l'importanza delle procedure di assistenza reciproca tra autorità di controllo e del sistema decisorio compartecipato di cui al Capo VII del RGPD per garantire un'applicazione coerente ed omogenea del diritto alla protezione dei dati personali in tutta l'Unione.

Tra le numerose decisioni finali cui il Garante ha cooperato in qualità di autorità interessata, secondo la definizione di cui all'art. 4, n. 22, del RGPD, se ne sono registrate alcune di particolare interesse.

In data 2 settembre 2021 l'Autorità irlandese, nella sua veste di autorità di

13

controllo capofila, ha adottato una decisione finale nei confronti di WhatsApp per violazione del principio di trasparenza e degli obblighi informativi di cui agli artt. 12, 13 e 14 del RGPD, comminando contestualmente una sanzione amministrativa pari a 225 milioni di euro ed un ordine di conformare il trattamento adottando una serie di specifiche misure correttive.

L'*iter* della procedura di cooperazione ha formalmente avuto inizio nel dicembre 2020 con la trasmissione, da parte della *Data Protection Commissioner* irlandese, di un progetto di decisione a tutte le autorità di controllo interessate, ai sensi dell'art. 60, par. 3, del RGPD. Nei confronti di tale progetto, otto autorità, tra cui il Garante, hanno sollevato obiezioni "motivate e pertinenti" a seguito delle quali, all'esito di un'ulteriore infruttuosa attività di cooperazione, l'Autorità irlandese ha avviato la procedura di risoluzione delle controversie avanti al Comitato europeo ai sensi dell'art. 65, par. 1, lett. *a*), del RGPD.

Il 28 luglio 2021 il Comitato europeo, in parziale accoglimento delle numerose obiezioni presentate avverso il progetto irlandese, ha adottato una decisione vincolante, alla cui stesura il Garante ha fattivamente contribuito, contenente una serie di principi che l'Autorità irlandese ha recepito nella sua decisione finale ai sensi dell'art. 65, par. 6, del RGPD.

Il 15 luglio 2021 la *Commission nationale pour la protection des données* del Granducato del Lussemburgo, in veste di autorità capofila, ha adottato una decisione finale nei confronti di Amazon Europe Core S.à r.l nell'ambito di una procedura di cooperazione europea che ha visto coinvolte numerose autorità interessate, tra cui il Garante. Tale decisione, la cui notizia è stata diffusa dallo stesso titolare, non è ancora stata pubblicata in quanto la legge nazionale lussemburghese sulla protezione dei dati personali subordina la pubblicazione del provvedimento, qualificata come sanzione accessoria, al passaggio in giudicato dello stesso, passaggio in giudicato non perfezionato per l'avvenuta impugnazione da parte del titolare.

Con tale decisione, adottata ai sensi dell'art. 60, par. 7, del RGPD, l'Autorità lussemburghese ha comminato una sanzione di 746 milioni di euro nei confronti della società per alcuni accertati severi profili di illiceità in relazione al trattamento di dati personali degli utenti per finalità di pubblicità comportamentale (OBA, *Online Behavioural Advertising*).

La gestione della procedura è stata all'insegna della cooperazione con le autorità interessate sin dalla fase istruttoria in tal modo agevolando un'interazione che ha permesso di incorporare nel progetto di decisione le osservazioni delle altre autorità, tra cui quelle del Garante, in merito alla qualificazione giuridica dei fatti ed all'esercizio dei poteri correttivi e scongiurando l'apertura di una controversia avanti l'EDPB attraverso l'attivazione del meccanismo di coerenza ai sensi dell'art. 65, par. 1, lett. *a*), del RGPD.

Sempre con riferimento ai sistemi per la gestione della pubblicità *online,* si segnala un'altra rilevante decisione, assunta nell'ambito della procedura di cooperazione di cui al Capo VII del RGPD, alla quale il Garante ha partecipato in qualità di autorità interessata, adottata dall'Autorità di controllo capofila belga nei confronti di *Interactive Advertising Bureau Europe* (IAB Europe).

L'Autorité de protection des données belga (APD) ha, infatti, accertato che il cd. *Transparency and Consent Framework* (TCF), una piattaforma implementata da IAB per la gestione per conto terzi delle preferenze degli utenti per la ricezione di pubblicità personalizzata *online* attraverso il sistema di *Real Time Bidding* (RTB), aveva violato diverse disposizioni del RGPD, tra cui il principio di liceità, non essendo stata determinata una valida base giuridica per il trattamento delle cd. TC *String* (stringhe di caratteri codificate che contengono tutte le informazioni rilevanti sul consenso

dell'utente) e l'ulteriore trattamento da parte di fornitori di tecnologie pubblicitarie, essendo venuti meno i principi di trasparenza (in ragione della natura eccessivamente generica delle informazioni fornite agli utenti), *accountability,* sicurezza, *privacy by design* e *by default,* ed essendo stata rilevata la mancanza del registro di cui all'art. 30, di idonee misure tecniche e organizzative, di cui all'art. 32, della valutazione d'impatto di cui all'art. 35 e della nomina di un Rpd, ai sensi dell'art. 37 del RGPD.

Per tali violazioni l'Autorità di controllo belga ha inflitto a IAB Europe una sanzione amministrativa di 250.000 euro ed ordinato la messa in conformità del TCF mediante un piano d'azione da concordare con l'Autorità.

Come per la decisione lussemburghese nei confronti di Amazon, anche la procedura di cooperazione condotta dall'Autorità belga ha comportato una proficua applicazione del meccanismo dello sportello unico: a seguito di una serie di commenti, tra cui le osservazioni proposte dal Garante e due obiezioni sollevate rispetto ad un primo progetto di decisione, l'APD ha sottoposto un progetto di decisione riveduto, ai sensi dell'art. 60, par. 4, del RGPD in cui ha recepito tutte le proposte delle autorità intervenute e sul quale è stato successivamente raggiunto un consenso condiviso che ha consentito l'adozione delle decisione finale ai sensi dell'art. 60, par. 7, del RGPD.

14 La protezione dei dati personali nel rapporto di lavoro privato e pubblico

14.1. *La protezione dei dati nell'ambito del rapporto di lavoro privato. I trattamenti effettuati per finalità di prevenzione dal contagio da Covid-19*

Nel periodo di riferimento, ancora caratterizzato dalla continua evoluzione normativa derivante dall'emergenza sanitaria in atto, anche nel settore lavoristico sono state trattate numerose istanze pervenute a titolo sia di reclamo ex art. 77 del RGPD sia di segnalazione e sono pervenuti verbali di accertamento di presunte violazioni della disciplina in materia di protezione dei dati personali da parte di diversi organi accertatori. Sono stati altresì forniti chiarimenti e, in alcuni casi, assistenza ai soggetti destinatari delle disposizioni in materia di protezione dei dati (titolari, interessati, associazioni di categoria e rappresentative di interessati), anche attraverso risposte a quesiti di particolare rilevanza o con profili di novità rispetto a questioni già affrontate dal Garante.

Per quanto riguarda le condizioni di liceità dei trattamenti effettuati mediante dispositivi tecnologici, sia quelli tradizionalmente utilizzati come i sistemi di videosorveglianza e di posta elettronica, sia quelli caratterizzati da profili di novità in quanto ricollegati all'operatività di piattaforme digitali che funzionano tramite algoritmi, sono stati adottati due provvedimenti nei confronti di società del settore del cd. *food delivery* aventi ad oggetto i trattamenti, anche automatizzati, dei dati dei cd. *rider* nell'ambito dell'attività di consegna di cibo e altri beni (provv.ti 10 giugno 2021, n. 234, doc. web n. 9675440; 22 luglio 2021, n. 285, doc. web n. 9685994).

Il Garante si è inoltre occupato del trattamento di categorie particolari di dati personali di cui all'art. 9 del RGPD (in particolare dati relativi alla salute) e dei dati personali relativi a condanne penali e reati ex art. 10 del RGPD.

In più occasioni è stato ribadito che pure in ambito lavorativo l'esercizio dei diritti riconosciuti all'interessato (v. artt. 12-22 del RGPD) deve essere quanto più possibile agevolato dal titolare, conformemente a quanto stabilito in proposito dalla disciplina di derivazione eurounitaria. È stata, in particolare, rammentata la necessità di fornire ai sensi dell'art. 12, par. 4, del RGPD, nel caso di diniego dell'istanza di esercizio dei diritti, gli specifici motivi dell'inottemperanza e l'indicazione della possibilità di proporre reclamo all'autorità di controllo o di proporre ricorso giurisdizionale.

Trattamenti di dati personali nell'ambito della pandemia da Covid-19

Come già nel 2020 oggetto dell'attività sono stati altresì numerosi e diversificati trattamenti di dati connessi all'emergenza sanitaria da Covid-19, con riguardo sia all'ambito lavorativo sia alle attività produttive, economiche e commerciali, tra le quali, palestre, piscine, attività di ristorazione e strutture ricettive, anche alla luce delle linee guida per la ripresa delle attività economiche e sociali adottate ai sensi dell'art. 1, comma 14, d.l. n. 33/2020 in conformità alle disposizioni del d.l. n. 52/2021 e s.m.i. e del d.l. n. 65/2021.

Sotto il profilo normativo e delle regole al riguardo applicabili merita di essere menzionato tra l'altro, l'aggiornamento, in data 6 aprile 2021, del Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro sottoscritto fra il Governo e le parti sociali ed adottato in base a quanto previsto dall'art. 1, n. 7, lett. *d*), d.P.C.M. 11 marzo 2020 (il cui contenuto è stato successivamente richiamato dall'art. 29-*bis,*

14

d.l. n. 23/2020, inserito con legge di conversione 5 giugno 2020, n. 40), concernente specifiche misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro e nell'ambito di rapporti di lavoro. Sono stati, inoltre, adottati il d.l. 22 aprile 2021, n. 52, convertito con modificazioni dalla legge 17 giugno 2021, n. 87, nonché il d.P.C.M. 17 giugno 2021, adottato a seguito del parere del Garante reso con provvedimento 9 giugno 2021, n. 229 (doc. web n. 9668064), modificato da ultimo dal d.P.C.M. 17 dicembre 2021, anch'esso adottato a seguito del parere favorevole del Garante il 13 dicembre 2021, n. 420 (doc. web n. 972720), che ha previsto all'art. 13 le modalità di verifica del possesso del *green pass.*

Il decreto legge 1° aprile 2021, n. 44 (artt. 4 e ss.), per la prevenzione dell'infezione da Sars-CoV-2 – modificato, tra l'altro, dal d.l. 26 novembre 2021, n. 172 non ancora convertito, alla data di riferimento di questo testo – ha previsto l'obbligo vaccinale, dapprima per gli esercenti le professioni sanitarie e successivamente anche per altre categorie di lavoratori tassativamente indicate (impiegati in strutture residenziali, socio-assistenziali e socio-sanitarie, personale della scuola, del comparto difesa, sicurezza e soccorso pubblico, della polizia locale, degli organismi di cui alla l. 3 agosto 2007, n. 124, delle strutture di cui all'art. 8-*ter,* d.lgs. 30 dicembre 1992, n. 502, degli istituti penitenziari, delle università, delle istituzioni di alta formazione artistica, musicale e coreutica e degli istituti tecnici superiori).

Visto l'ampio novero di attività e contesti in relazione ai quali specifiche disposizioni normative hanno via via subordinato l'accesso ai luoghi di lavoro al possesso del *green pass* o al completamento del ciclo vaccinale previsto per la prevenzione dell'infezione da Sars-CoV-2, l'attività del Garante è stata volta ad arginare, nel rispetto del principio di minimizzazione dei dati (art. 5, par. 1, lett. *a*), del RGPD), forme di indiscriminato trattamento di dati comunque ricollegati alle certificazioni verdi Covid-19 e, più in generale, all'infezione da Covid-19.

Verifica del possesso della certificazione verde Covid-19 in capo ai possessori di *skipass*

Tra gli altri è stato esaminato il progetto presentato da un Consorzio di impianti sciistici sulle modalità di controllo della certificazione verde Covid-19 dei possessori di *skipass* funzionale all'accesso agli impianti di risalita con cd. veicoli chiusi presenti all'interno del relativo comprensorio sciistico, in conformità all'art. 9-*quater,* comma 1, lett. *e*) (Impiego delle certificazioni verdi Covid-19 nei mezzi di trasporto), d.l. 22 aprile 2021, n. 52.

All'esito di valutazioni anche tecniche, considerata in particolare l'esigenza di approntare procedure di verifica rapide a fronte di una grande quantità di utenti anche al fine di evitare code ed assembramenti, si sono ritenute le modalità delineate compatibili con l'attuale quadro normativo in quanto utilizzano l'apposito SDK (*Software Development Kit*) messo a disposizione dal Ministero della salute, previsto dall'art. 13, comma 10, lett. *a*), del d.P.C.M. 17 giugno 2021. In particolare, è stato rilevato che la verifica della validità del *green pass* è istantanea rispetto all'esibizione (da remoto) del *green pass* stesso, non comportando alcuna conservazione di dati. Inoltre, è previsto che l'estrazione del contenuto del QR *code* sia effettuata sul terminale dell'utente (es. *smartphone* o *personal computer*) e che la sua trasmissione ai *server* della Federazione avvenga attraverso un canale di comunicazione sicuro. Ciò considerato, l'Autorità ha ritenuto che il progetto potesse essere valutato in linea con lo specifico quadro normativo vigente, ma, tenuto conto dei rischi elevati per i diritti e le libertà degli interessati derivanti dall'utilizzo di un sistema così complesso basato sul trattamento di dati particolari, su larga scala, si è invitata la Federazione ad effettuare (e tenere costantemente aggiornata), prima dell'avvio del trattamento, un'idonea valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD volta a individuare le misure necessarie per affrontare i possibili rischi (nota 10 novembre 2021).

Progetto di *screening* e di prevenzione per la diffusione del virus Covid-19 nei luoghi di lavoro

È stato anche esaminato un progetto di *screening* e di prevenzione per la diffusione del virus Covid-19 nei luoghi di lavoro, presentato da alcune società di un gruppo multinazionale dichiaratamente preordinato alla individuazione di soggetti asintomatici (sia dipendenti che soggetti terzi) nelle sedi aziendali presenti sul territorio nazionale attraverso sottoposizione a tampone autosomministrato dagli stessi interessati. In particolare, in base a quanto rappresentato dalle società, ciascun lavoratore avrebbe acceduto all'area di effettuazione dei test mediante il proprio *badge* aziendale e, dopo essere stato identificato attraverso alcuni ulteriori dati personali (quali nome e cognome, indirizzo, numero telefonico ed *e-mail* personale), si sarebbe effettuato autonomamente il test e il campione, contraddistinto da un codice di identificazione univoco, sarebbe stato inviato in un laboratorio situato nel Regno Unito e lì analizzato sulla base di metodologie che sarebbero state validate dalle autorità sanitarie inglesi. La società, inoltre, avrebbe attivato presso le autorità sanitarie italiane un procedimento per ottenere la validazione della metodologia utilizzata nel laboratorio situato nel Regno Unito. L'esito del test sarebbe stato comunicato all'interessato dal laboratorio utilizzando un applicativo scaricato sul telefono cellulare oppure attraverso sms o *e-mail*. Il risultato sarebbe stato altresì messo a disposizione dell'interessato attraverso un portale web dedicato. Secondo la società gli interessati in Italia sarebbero stati più di 16.000.

In esito a valutazioni ufficiose da parte dell'Autorità, anche alla luce della normativa in tema di emergenza epidemiologica da Covid-19, le società hanno comunicato l'intenzione di non procedere all'implementazione del progetto in Italia. In particolare il trattamento avrebbe sollevato problemi di compatibilità con la disciplina di protezione dei dati con riferimento, tra l'altro: alle condizioni di liceità del trattamento considerata l'assenza di base giuridica per il trattamento dei campioni biologici del lavoratore da parte del datore di lavoro; al principio di minimizzazione in quanto sarebbero stati trattati, oltre ai dati necessari per realizzare la finalità propria del progetto, anche dati non necessari e non pertinenti rispetto allo stesso; all'assenza dei requisiti previsti dall'ordinamento per l'effettuazione di *screening* come misura di contenimento della diffusione del virus Covid-19 negli ambienti di lavoro; alla non chiara assegnazione e ripartizione dei ruoli (titolare e responsabile del trattamento), anche in relazione al laboratorio sito in Gran Bretagna; ai principi di *privacy by design* e *by default* considerata la molteplicità di *database* nei quali vengono raccolti i dati relativi al progetto; al principio di limitazione della conservazione avuto riguardo alla finalità del progetto individuata nell'implementazione delle condizioni di sicurezza per individuare i lavoratori positivi al Covid-19 (note 2 marzo, 2 maggio e 24 giugno 2021).

Applicativi per la verifica della certificazione verde Covid-19

A seguito di notizie di stampa, l'Autorità ha avviato un'istruttoria, ancora in corso di definizione, sull'utilizzo di un'applicazione mobile volta a generare un QR *code* che attesta il cd. *status* Covid-*free* degli utenti registrati al fine di accedere ad eventi, manifestazioni, luoghi aperti al pubblico (es. lezioni universitarie in presenza, discoteche, ecc.); *status* che viene verificato in base all'evidenza temporanea del tampone negativo, all'autodichiarazione in ordine all'avvenuta vaccinazione ovvero alla guarigione da Covid-19.

Vista la necessità di intervenire in via d'urgenza per tutelare i diritti e le libertà degli interessati, anche in ragione del possibile utilizzo della suddetta applicazione in occasione di ulteriori eventi e manifestazioni, in data 3 giugno 2021, è stato adottato un provvedimento di limitazione provvisoria del trattamento dei dati personali in questione posto in essere per il tramite della suddetta applicazione (n. 224, doc. web n. 9592298). Al riguardo è stata infatti sottolineata la mancanza di una valida base giuridica per il trattamento di dati, anche particolarmente delicati come

14

quelli di natura sanitaria, effettuato mediante l'applicazione e finalizzato ad accertare la situazione Covid-*free* di quanti partecipino ad avvenimenti sportivi nonché ad altre manifestazioni pubbliche o accedano a locali aperti al pubblico. Il blocco è stato predisposto per il tempo necessario a consentire all'Autorità la definizione dell'istruttoria.

Modalità di verifica del possesso della certificazione verde Covid-19

Alcune istanze hanno riguardato i controlli – tanto in modalità base che rafforzata – dei *green pass,* sul presupposto che la continua (e, a tratti, convulsa) evoluzione normativa potesse aver creato difficoltà e/o discriminazioni nell'applicazione dello strumento. Al riguardo, è stato più volte precisato che il trattamento di dati personali connesso all'utilizzo del *green pass* è consentito, tanto nella versione base che in quella rafforzata, nei soli casi previsti dalla normativa vigente e nei limiti da questa stabiliti (nota 23 dicembre 2021). Non è pertanto ipotizzabile, ad esempio, un eventuale uso della certificazione verde Covid-19 per l'accesso a beni, servizi o luoghi che, pur tenendo conto del progressivo ampliamento degli scenari di utilizzo, non siano però contemplati nelle misure di volta in volta adottate dal Governo per il contrasto della pandemia.

14.2. *I trattamenti dei dati effettuati mediante piattaforme digitali nel settore del cd.* food delivery

Il Garante, anche a seguito di pronunce dell'Autorità giudiziaria e di proposte di iniziativa legislativa (successivamente adottate), nel 2019 aveva avviato d'ufficio, per i profili di competenza un'attività di controllo sui trattamenti di dati personali riferiti al personale (cd. *rider*) incaricato della consegna di cibo – o altri beni – effettuati attraverso l'intermediazione di piattaforme digitali. Allo stato, all'esito di tale attività ispettiva, sono stati adottati due provvedimenti nei confronti di società che operano nel settore.

La procedura di cooperazione in relazione a trattamenti transfrontalieri

Trattandosi di società che sono parte di gruppi societari, poiché nel corso delle attività ispettive sono emersi possibili trattamenti transfrontalieri ai sensi dell'art. 4(23) del RGPD, il Garante ha avviato un procedimento attraverso la piattaforma IMI per individuare, in concreto, l'autorità di controllo capofila che assume il ruolo di *Lead Authority* (v. art. 56, par. 1, del RGPD).

Il Regolamento prevede che, pure nel caso di trattamenti transfrontalieri, l'autorità nazionale dello stabilimento rimanga competente nel caso in cui la stessa riceva un reclamo o nel caso di eventuali violazioni del RGPD se l'oggetto riguarda unicamente uno stabilimento nel suo Stato membro o incide in modo sostanziale sugli interessati unicamente nel suo Stato membro (art. 56, par. 2, del RGPD). In relazione ad entrambi i casi oggetto di accertamento l'Autorità è stata ritenuta competente a procedere per i trattamenti aventi impatto solo locale ai sensi dell'art. 56, par. 2, del RGPD ed ha altresì proceduto, ai sensi dell'art. 55 e del cons. 122 del RGPD, la valutazione della liceità dei trattamenti effettuati unicamente su interessati che operano sul territorio nazionale adottando i provvedimenti in commento (provv.ti 10 giugno 2021, n. 234, doc. web n. 9675440 e 22 luglio 2021, n. 285, doc. web n. 9685994).

In relazione ad uno dei due casi, l'autorità capofila ha iniziato il procedimento nei confronti della società capogruppo ai sensi dell'art. 60 del RGPD, avviando con le autorità interessate (tra cui quella italiana), la procedura di cooperazione allo stato non conclusa, in vista dell'adozione di una decisione concordata e vincolante (v. art. 60, par. 6, del RGPD).

La peculiarità dei trattamenti effettuati mediante piattaforme digitali

Il Garante ha in primo luogo accertato che le società che operano in Italia ed effettuano trattamenti dei dati dei *rider,* anche attraverso piattaforme digitali la cui proprietà è in capo alla capogruppo, agiscono in qualità di titolari del trattamento, in quanto ne determinano finalità e mezzi. Ciò è emerso dall'accesso diretto ai sistemi utilizzati dalle società e dall'esame della copiosa documentazione acquisita in atti.

I trattamenti effettuati, preordinati alla gestione di una prestazione lavorativa consistente nella consegna di beni, si caratterizzano per il carattere innovativo della tecnologia utilizzata che si avvale del funzionamento di una piattaforma digitale e degli algoritmi che ne determinano l'operatività (il cui meccanismo di funzionamento è stato solo parzialmente reso noto nel corso del procedimento, sia per quanto riguarda l'accesso alle prenotazioni delle fasce orarie sia per ciò che riguarda l'assegnazione degli ordini da consegnare). La raccolta di una notevole quantità di informazioni, attraverso strumenti diversi (applicativo installato sul dispositivo mobile del *rider,* contatti con il *rider* attraverso *chat, e-mail,* telefonate), riferite ad un numero rilevante di interessati, comporta l'effettuazione di trattamenti automatizzati, compresa la profilazione, che incidono in modo significativo sugli interessati, escludendo, in particolare, una parte dei *rider* dalle occasioni di lavoro (v. art. 4, n. 4), del RGPD, cons. 71).

I trattamenti effettuati dalle società oggetto di accertamento, pur differenziandosi per taluni aspetti anche significativi di cui si dà conto nei rispettivi provvedimenti, sono stati ritenuti tali da determinare, dal punto di vista della disciplina di protezione dei dati, "un rischio elevato per in diritti e le libertà delle persone fisiche" (v. art. 35, del RGPD), con conseguente obbligo per il titolare di effettuare, prima di procedere al trattamento, una valutazione di impatto dei trattamenti previsti.

Entrambi tali significativi aspetti sono stati, insieme ad altri, oggetto di contestazione alle società, con conseguente ingiunzione di conformarsi a quanto in proposito stabilito dal Regolamento. Il Garante ha anche, per la prima volta, individuato specifiche misure correttive riferite all'operatività di algoritmi e meccanismi di *feedback,* ed ingiunto alle società di adottare "misure appropriate volte alla verifica periodica della correttezza e accuratezza dei risultati dei sistemi algoritmici, anche al fine di garantire che sia minimizzato il rischio di errori e di conformarsi a quanto stabilito dall'art. 47-*quinquies,* d.lgs. n. 81/2015 in materia di divieto di discriminazione, accesso alla piattaforma e esclusione dalla piattaforma" nonché di adottare "misure appropriate volte ad introdurre strumenti per evitare usi impropri e discriminatori dei meccanismi reputazionali basati su *feedback".*

La peculiarità dei trattamenti oggetto di accertamento, effettuati dalle società nell'ambito di un rapporto di lavoro che intercorre con i *rider,* è costituita anche dalla applicabilità di specifiche discipline di settore la cui osservanza costituisce condizione di liceità dei trattamenti stessi (v. artt. 5, par. 1, lett. *a*) e 88 del RGPD; art. 114 del Codice). Ciò con riguardo sia alle discipline applicabili in caso di trattamenti di dati personali effettuati nel contesto lavorativo attraverso dispositivi tecnologici che consentono attività di controllo a distanza, sia alle disposizioni di recente introduzione nel nostro ordinamento riguardanti attività lavorative caratterizzate dall'operatività di sistemi tecnologici complessi (v. l. n. 128/2019, di conversione del d.l. n. 101/2019, che ha inserito il capo V-*bis* nel d.lgs. n. 81/2015, "Tutela del lavoro tramite piattaforme digitali", nonché il nuovo periodo nell'art. 2, comma 1, d.lgs. n. 81/2015, che fa riferimento alle "modalità di esecuzione della prestazione […] organizzate mediante piattaforme anche digitali").

Pur considerato che le società hanno adottato modalità di trattamento che si differenziano, per taluni aspetti, in entrambi i casi si è ritenuto in concreto applicabile l'art. 2, d.lgs. n. 81/2015 laddove stabilisce che "ai rapporti di collaborazione che si

concretano in prestazioni di lavoro prevalentemente personali, continuative e le cui modalità di esecuzione sono organizzate dal committente […] anche qualora le modalità di esecuzione della prestazione siano organizzate mediante piattaforme anche digitali" si applica "la disciplina del rapporto di lavoro subordinato". Tale valutazione tiene anche conto delle indicazioni fornite in proposito dalla Corte di cassazione, sentenza 24 gennaio 2020, n. 1663, più ampiamente richiamata nei provvedimenti.

Nell'ambito delle tutele che costituiscono la "disciplina della subordinazione" nonché di quelle poste "a tutela della libertà e dignità del lavoratore" rientra la specifica disciplina richiamata dall'art. 114 del Codice come condizione di liceità del trattamento (ossia il più volte richiamato art. 4, l. n. 300/1970).

Il Garante ha pertanto rilevato che entrambe le società, attraverso una pluralità di strumenti tecnologici (individuati nella piattaforma digitale, l'*app* e i canali utilizzati per contattare i *rider*), effettuano trattamenti di dati che consentono una minuziosa attività di controllo della prestazione lavorativa svolta dai *rider,* senza conformarsi a quanto in proposito stabilito dall'art. 4, comma 1, l. n. 300/1970.

Il Garante ha pertanto ingiunto alle società di conformare i propri trattamenti alle discipline risultate applicabili a seguito della valutazione e dell'accertamento delle concrete caratteristiche delle attività di trattamento effettuate nel contesto del cd. *food delivery.*

L'Autorità ha altresì accertato una pluralità di violazioni delle disposizioni del Regolamento, ingiunto alle società di conformarsi all'ordinamento vigente attraverso l'adozione di specifiche misure nonché applicato sanzioni amministrative pecuniarie commisurate alle peculiarità del caso concreto.

Attribuzione di un punteggio al *rider*

In uno dei casi oggetto di accertamenti ispettivi, riguardante una società che all'epoca aveva dichiarato di effettuare trattamenti relativi a più di 18 mila *rider,* è emerso un quadro di assai scarsa trasparenza nei confronti degli interessati, tra l'altro per quanto riguarda la geolocalizzazione continua dei dispositivi, la raccolta di dati relativi alle comunicazioni intraprese via *chat, e-mail* e telefono con il *call center,* le valutazioni espresse sul *rider* da parte degli esercenti e dei clienti (*feedback*), i tempi di conservazione dei dati, l'effettuazione di trattamenti automatizzati (compresa l'attività di profilazione) preordinati all'assegnazione di un punteggio al *rider.* La società inoltre non ha definito i termini di conservazione dei dati personali riferiti ai *rider* in relazione alle distinte tipologie di trattamento e le relative finalità, e si è limitata per lo più a individuare un unico – e ampio – termine di conservazione, pari a quattro anni dopo la cessazione del rapporto di lavoro, in relazione ad una pluralità di trattamenti effettuati per scopi diversi nonché in relazione a distinte tipologie di dati, in alcuni casi riferiti al contenuto di comunicazioni in sé protette da particolari garanzie da parte dell'ordinamento (via *chat, e-mail* e telefono). Per questi ed altri profili i sistemi sono stati ritenuti in violazione dell'art. 5, par. 1, lett. *c*), del RGPD (principio di minimizzazione dei dati) e dell'art. 25 del RGPD (principio di *privacy by design* e *by default*). È stata altresì riscontrata la violazione dell'obbligo di adottare adeguate misure di sicurezza (art. 32 del RGPD) posto che i sistemi sono risultati configurati in modo che la pagina di presentazione consentiva l'accesso ai dati di tutti i *rider* che operano sia in territorio UE che extra UE, in assenza di alcun criterio di selezione all'accesso. Successivamente alla contestazione effettuata dall'Autorità la società ha tuttavia provveduto a modificare il sistema di accesso con l'introduzione di un meccanismo (cd. *city permission*) che consente agli operatori di accedere ai dati dei *rider* solo su base territoriale.

Come già osservato nella sezione introduttiva, è stata riscontrata l'omessa effettuazione di una valutazione di impatto pur in presenza di trattamenti che presentano, per le loro caratteristiche, rischi elevati per i diritti e le libertà degli interessati.

14

Sistema di prenotazione dei turni in base alle statistiche e algoritmo di assegnazione degli ordini

In base a quanto accertato dall'Autorità, attraverso il sistema di punteggio, la società ha valutato l'operato del *rider* con un effetto significativo sulla sua persona proponendo o negando l'accesso alle fasce orarie e la relativa possibilità di effettuare la prestazione oggetto del contratto. In relazione a tali complessi trattamenti, come sopra accennato, il Garante ha ingiunto l'adozione di misure correttive specifiche (provv. 10 giugno 2021, n. 234, doc. web n. 9675440).

Anche all'esito degli accertamenti effettuati nei confronti di diversa società che opera nel settore del cd. *food delivery,* è emerso un quadro di scarsa trasparenza nei confronti degli interessati rispetto alle concrete caratteristiche dei trattamenti effettuati con riguardo in particolare alla sistematica raccolta dei dati relativi alla geolocalizzazione (ogni 12 secondi) effettuata dalla società attraverso l'applicazione installata sul dispositivo ed ai tempi di conservazione dei dati raccolti, peraltro non conformi al principio di limitazione della conservazione (v. art. 5, par. 1, lett. *e*), del RGPD). La concreta configurazione dei sistemi, inoltre, tale da consentire la raccolta e la memorizzazione di tutti i dati relativi alla gestione dell'ordine è stata ritenuta in violazione degli artt. 5, par. 1, lett. *c*), del RGPD (principio di minimizzazione dei dati) e 25 del RGPD, relativo alla protezione dei dati fin dalla progettazione e per impostazione predefinita (*privacy by design* e *by default*). Anche in questo caso è emerso che tutti i sistemi (sia quelli sviluppati dalla società che quelli sviluppati da terze parti), almeno fino alla data del 10 luglio 2020, consentivano agli operatori l'accesso ai dati di tutti i *rider* che operano sia in territorio UE che extra UE. Successivamente alla effettuazione dell'attività di accertamento da parte dell'Autorità i sistemi sono stati riconfigurati in base al principio di "segregazione per singola giurisdizione, con eccezioni per un numero limitato di *supervisor*". L'omessa attivazione di un criterio di accesso selettivo al sistema, con conseguente possibilità per gli operatori di accedere ai dati dei *rider* trattati da tutte le società del gruppo, è stata ritenuta in violazione di quanto stabilito dall'art. 32 del RGPD.

Differente è risultata, invece, la modalità di effettuazione dei trattamenti automatizzati compresa la profilazione.

Il sistema di prenotazione fondato sulla applicazione di una formula matematica e abbandonato dalla società nel corso del procedimento davanti all'autorità di controllo in base a quanto accertato dal Garante, penalizza direttamente il *rider* che non effettua il *login* dopo l'avvio del turno nonché i *rider* che non si presentano *online* nella sessione prenotata e che non partecipano (o partecipano meno) alle sessioni di super picco. Attraverso il punteggio derivante dalle statistiche la società valuta l'operato del *rider* producendo, in tal modo, un effetto significativo sulla sua persona. Con riguardo all'algoritmo di assegnazione dell'ordine, l'Autorità ha registrato una scarsa trasparenza dei relativi meccanismi di funzionamento, posto che la società non ne ha chiarito il funzionamento e in particolare i criteri di priorità elaborati in base ai dati raccolti. Considerato, inoltre, che la società continua a raccogliere una grande quantità e varietà di dati personali attraverso i diversi sistemi di gestione degli ordini e che non è stata fornita alcuna informazione sui trattamenti effettuati dei dati già raccolti dal sistema di elaborazione delle statistiche e sulle nuove modalità di assegnazione, il Garante ha ritenuto che la modifica del sistema di prenotazione, attiva dal 3 novembre 2020, riguarda al massimo i criteri di accesso al turno di lavoro, ma non la modalità con la quale all'interno del turno è assegnato l'ordine. In relazione ai trattamenti automatizzati, compresa la profilazione, così individuati, la società non ha attivato le misure a tutela dei diritti e delle libertà degli interessati previste dall'art. 22, par. 3, del RGPD.

Come già segnalato nella parte introduttiva l'Autorità ha ritenuto che l'attività di trattamento svolta dalla società rientra tra quelle che presentano "un rischio elevato

per i diritti e le libertà delle persone fisiche" con conseguente necessità di effettuare, prima dell'inizio del trattamento stesso, una valutazione di impatto ai sensi dell'art. 35 del RGPD, tenuto conto che il trattamento viene effettuato anche attraverso l'utilizzo innovativo di una piattaforma digitale dalla società italiana in qualità di titolare nei confronti di un numero considerevole di interessati.

In relazione a tali complessi trattamenti, anche in questo caso il Garante ha ingiunto l'adozione di misure correttive specifiche (provv. 22 luglio 2021, n. 285, doc. web n. 9685994).

14.3. *I trattamenti dei dati effettuati mediante dispositivi tecnologici*

Oggetto delle attività di accertamento sono stati sia dispositivi tradizionalmente utilizzati nel contesto lavorativo (in particolare i sistemi di videosorveglianza e la posta elettronica) sia sistemi più complessi (*Work Force Management*). Conformemente ad una posizione ormai consolidata, il Garante ha ribadito che la protezione della vita privata si estende anche all'ambito lavorativo, come più volte stabilito dalla Corte EDU che ritiene applicabile l'art. 8 della Convenzione europea dei diritti dell'uomo senza distinguere tra sfera privata e sfera professionale (v. tra le altre Niemietz c. Allemagne, 16.12.1992, ric. n. 13710/88, par. 29, Bărbulescu v. Romania [GC], 5 settembre 2017, ric. n. 61496/08, parr. 70-73 Antović and Mirković v. Montenegro, 28 novembre 2017, ric. n. 70838/13, parr. 41-42).

I provvedimenti dell'Autorità in materia tengono conto della necessità di applicare il vigente quadro normativo caratterizzato da reciproci rinvii operati dal legislatore – anche di recente, in sede di adeguamento dell'ordinamento nazionale alle norme del RGPD – tra la disciplina in materia di protezione dei dati personali (artt. 113, 114 e 171 del Codice e 88 del RGPD) e le norme di settore sui controlli a distanza (l. n. 300/1970).

Trattamenti mediante utilizzo di sistemi di *Work Force Management*

È stato ritenuto illecito il trattamento effettuato da una società mediante un sistema di WFM (*Work Force Management*) senza informare i lavoratori che la tipologia dei dati e le modalità utilizzate dal sistema erano tali da consentirne la riconducibilità ai singoli interessati identificabili, attraverso l'utilizzo di ulteriori informazioni nella disponibilità del titolare. In proposito, il Garante ha ribadito che la conservazione di dati personali su sistemi diversi non incide sulla unitarietà del trattamento effettuato dal titolare. All'esito dell'istruttoria è altresì emerso che il sistema trattava una pluralità di dati, anche organizzati in registri, non menzionati nell'informativa resa ai dipendenti. L'informativa è inoltre risultata priva di riferimenti ai tempi di conservazione dei dati trattati, in violazione dei principi di trasparenza e correttezza del trattamento (artt. 13 e 5, par. 1, lett. *a*), del RGPD).

Un ulteriore e specifico profilo di violazione dell'obbligo di fornire una compiuta informativa ai dipendenti è stato accertato in relazione all'indicazione di una pluralità di finalità (tra loro eterogenee) che la società ha dichiarato di perseguire nelle attività di trattamento dei dati raccolti attraverso il sistema WFM senza tuttavia indicare contestualmente la specifica e distinta base giuridica del trattamento. Il Garante ha altresì dichiarato illecito il trattamento dei dati raccolti con il sistema WFM in ragione dell'avvenuto successivo utilizzo da parte della società al fine di verificare la veridicità di quanto affermato da un dipendente nel corso di un procedimento disciplinare avviato a suo carico. Ciò contravvenendo sia a quanto espressamente indicato nell'informativa relativa al funzionamento del sistema sia alla specifica condizione contenuta nell'autorizzazione rilasciata dall'Ispettorato del lavoro competente ai sensi dell'art. 4, l. n. 300/1970. Sotto tale ultimo profilo il Garante ha ribadito

14

che in base all'art. 114 del Codice l'osservanza del richiamato art 4, l. n. 300/1970 – che prevede il rilascio della autorizzazione da parte dell'Ispettorato del lavoro in caso di mancato accordo con le rappresentanze dei dipendenti come condizione indefettibile in caso di installazione di "strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori" – costituisce condizione di liceità dei trattamenti di dati personali. La norma di settore costituisce una delle disposizioni del diritto nazionale "più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro" (art. 88 del RGPD). Inoltre, tra le misure correttive impartite, è stata disposta la limitazione definitiva dei trattamenti effettuati con il sistema, limitatamente alle operazioni di conservazione dei dati ed è stata applicata una sanzione amministrativa pecuniaria (provv. 15 aprile 2021, n. 136, doc. web n. 9586936).

Trattamenti di dati contenuti in dispositivi aziendali attraverso strumenti di indagine forense

A seguito di due distinti reclami nei confronti di una medesima società, l'Autorità ha dichiarato illecito il trattamento effettuato attraverso l'analisi dei dati contenuti nei dispositivi aziendali affidati ai reclamanti nell'ambito di un rapporto di lavoro. L'illiceità è stata accertata, in primo luogo, per l'assenza di una previa informativa idonea a rappresentare con chiarezza agli interessati la possibilità per il datore di lavoro di effettuare controlli sui dispositivi aziendali del tipo di quelli attivati nel caso concreto (indagini sui contenuti memorizzati sui dispositivi aziendali – pc e *smart phone* – previa sottoposizione ad *imaging* degli stessi), con conseguente violazione degli artt. 13 e 5, par. 1, lett. *a*), del RGPD (principi di trasparenza e correttezza; in proposito v. già linee guida per posta elettronica e internet, provv. 1° marzo 2007, n. 13, in G.U. 10 marzo 2007, n. 58). L'Autorità ha nell'occasione sottolineato che l'adempimento degli obblighi informativi nei confronti del dipendente (consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli") costituisce altresì specifica condizione per il lecito utilizzo di tutti i dati raccolti nel corso del rapporto di lavoro, attraverso strumenti tecnologici e/o strumenti di lavoro, per tutti i fini connessi al relativo rapporto, ivi compresi i rilievi disciplinari, unitamente al rispetto della disciplina in materia di protezione dei dati personali (v. art. 4, comma 3, l. n. 300/1970, come sostituito dall'art. 23, comma 1, d.lgs. 14 settembre 2015, n. 151).

L'Autorità ha inoltre ritenuto non conformi alle disposizioni poste in materia di protezione dei dati attività di controllo caratterizzate dalla sistematica osservazione (monitoraggio) del flusso della navigazione in internet e della posta elettronica, anche di natura privata, con possibilità per la società di "scavalcare" le *password* e di accedere al contenuto di qualsiasi comunicazione effettuata dal dipendente (tramite telefono, *e-mail* o documenti redatti) in presenza di non specificati legittimi interessi della società. Tali trattamenti sono stati ritenuti non conformi ai principi di minimizzazione e di proporzionalità (v. art. 5, par. 1, lett. *c*), del RGPD e art. 52 CDFUE), considerata anche l'assenza di misure preventive (ad es. redazione di *black list* di siti internet non consentiti) e accertamenti graduali, ad esempio, su base aggregata, al fine di non consentire controlli prolungati, costanti o indiscriminati. Non risulta, in definitiva, conforme al richiamato principio generale di proporzionalità l'annullamento di ogni aspettativa di riservatezza qualora il dipendente sia connesso alla rete aziendale o utilizzi una risorsa aziendale anche attraverso dispositivi personali (v. sul punto Corte EDU, Bărbulescu v. Romania (GC), 5 settembre 2017 (ric. n. 61496/08), par. 80).

Inoltre le attività di controllo che la società si è riservata di effettuare nei termini previsti dai regolamenti aziendali sono state ritenute non conformi all'art. 114 del Codice (laddove richiama l'osservanza dell'art. 4, l. n. 300/1970 come condizione di liceità del trattamento) e all'art. 113 del Codice (laddove richiama come condizione

di liceità del trattamento l'osservanza dell'art. 8, l. n. 300/1970 e dell'art. 10, d.lgs. 10 settembre 2003, n. 276). Per le medesime ragioni le attività di indagine interna, effettuate dalla società anche attraverso il ricorso ad una società di investigazioni forensi, hanno comportato il trattamento di dati personali dei reclamanti in violazione del principio di minimizzazione e di proporzionalità (v. art. 5, par. 1, lett. *c*), del RGPD e art. 52 CDFUE) nonché dei richiamati artt. 113 e 114 del Codice.

Il Garante ha inoltre ritenuto la comunicazione di dati personali dei reclamanti alla capogruppo (soggetto giuridico distinto con sede legale nel Regno Unito) priva di una base giuridica idonea (v. art. 6 del RGPD), considerato che il legittimo interesse della controllante (genericamente indicato dalla società nella necessità di difendere e far valere i propri diritti) non è stato ritenuto sussistente nel caso concreto (v. art. 6, par. 1, lett. *f*), del RGPD; v. Gruppo Art. 29, WP217, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*) alla luce dei chiarimenti forniti dall'Autorità sulla condivisione di informazioni tra società appartenenti ad un medesimo gruppo di imprese (v. 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 privati, provv. 23 novembre 2006, n. 53; spec. par. 32).

È stato altresì ingiunto alla società di adeguare i propri regolamenti interni e la disciplina delle comunicazioni di dati personali dei dipendenti alla capogruppo alle disposizioni vigenti in materia di protezione dei dati ed è stata irrogata una sanzione amministrativa pecuniaria (provv. 15 aprile 2021, n. 137, doc. web n. 9670738).

Trattamento di dati attraverso sistemi di videosorveglianza

Il Garante nell'anno di riferimento ha rammentato ai titolari del trattamento l'obbligo di rispettare quanto previsto dall'art. 114 del Codice (che, come già precisato, rinvia all'art. 4 della l. n. 300/1970) – anche nel caso in cui le telecamere riprendano aree in cui transitano o sostano i dipendenti per lo svolgimento dell'attività lavorativa –, l'obbligo di fornire un'adeguata informativa agli interessati prima che entrino nel campo di azione delle telecamere nonché la necessità di effettuare il trattamento solo in presenza di una specifica condizione di liceità del trattamento. In proposito è stato ribadito che il consenso eventualmente prestato dai singoli lavoratori all'installazione di impianti non può essere considerato idonea base giuridica in quanto non è equivalente alla necessaria attivazione della procedura con le rappresentanze dei dipendenti o, in mancanza, sotto il controllo dell'autorità pubblica.

Il Garante, a seguito della presentazione di un'annotazione relativa all'accesso ispettivo effettuato dal Comando dei Carabinieri per la tutela del lavoro - Nucleo Carabinieri Ispettorato del lavoro, ha applicato una sanzione amministrativa pecuniaria nei confronti di una società che aveva attivato presso la propria sede operativa, in assenza di autorizzazione rilasciata dall'Ispettorato del lavoro o di un accordo con le rappresentanze sindacali, un sistema di videosorveglianza che riprendeva anche le zone in cui transitano i dipendenti per lo svolgimento dell'attività lavorativa (ingressi, cortili prospicienti l'officina, parcheggio) o per recarsi all'interno o presso aree a loro dedicate (spogliatoi, area ristoro, area fumatori).

Il trattamento è stato ritenuto illecito, fino all'avvenuta stipulazione dell'accordo ai sensi dell'art. 4 della l. n. 300/1970, per violazione degli artt. 5, par. 1, lett. *a*); 88 del RGPD e 114 del Codice.

Né è stata ritenuta idonea a far venir meno l'obbligo di conformarsi alla richiamata disciplina la circostanza che i rappresentanti sindacali aziendali e il rappresentante dei lavoratori per la sicurezza fossero stati informati della presenza dell'impianto e, secondo quanto dichiarato dalla società, ne condividessero la necessità in relazione alle finalità perseguite. Il consenso, infatti, non può ritenersi idonea base giuridica

14

per il trattamento dei dati personali dei dipendenti (provv. 16 settembre 2021, n. 331, doc. web n. 9719768).

In un altro caso, in seguito ad un'annotazione dei Carabinieri, è stata irrogata una sanzione amministrativa pecuniaria per un sistema di videosorveglianza installato presso strutture socio-assistenziali non conforme a quanto prescritto nell'autorizzazione rilasciata dall'Ispettorato del lavoro né, più in generale, alla disciplina in materia di protezione dei dati personali.

In particolare le telecamere del sistema di videosorveglianza erano state posizionate in modo differente rispetto a quanto autorizzato dall'Ispettorato e non era stato correttamente adempiuto l'obbligo di informativa nei confronti degli interessati (tra i quali anche lavoratori). Inoltre era prevista la registrazione dell'audio, sebbene all'interno dell'autorizzazione rilasciata dall'Ispettorato del lavoro fosse stato precisato che "non sono consentite intercettazioni e/o registrazioni audio". A seguito del sequestro effettuato dai Carabinieri, il trattamento è cessato.

Ai fini della quantificazione della sanzione l'Autorità ha considerato, tra l'altro, che il legale rappresentante della società titolare del trattamento, all'esito del procedimento avviato in sede penale, in base all'art. 171 del Codice, aveva già provveduto a pagare per la violazione di cui all'art. 4, comma 2, l. n. 300/1970 in relazione all'art. 114 del Codice, una somma pari al quarto del massimo dell'ammenda stabilita (provv. 16 settembre 2021, n. 330, doc. web n. 971890).

Trattamenti di dati relativi ad *account* di posta elettronica aziendale

Una parte significativa dei reclami e delle segnalazioni presentati all'Autorità continua a riguardare il trattamento dei dati relativi ad *account* di posta elettronica aziendale contenente il nome e/o il cognome del dipendente e, in particolare, il persistente utilizzo da parte del datore di lavoro degli *account* stessi anche dopo che il rapporto di lavoro si è interrotto.

L'Autorità ha ritenuto non conforme alla disciplina di protezione dei dati il trattamento posto in essere da una società che, dopo la cessazione del rapporto di lavoro con il segnalante, ha mantenuto attivi i due *account* di posta elettronica aziendale assegnatigli ed ha conservato, tramite *server,* i messaggi di posta elettronica relativi a uno dei due *account* disponendone la conservazione per dieci anni dalla cessazione del rapporto. La società ha inoltre conservato i messaggi in entrata e in uscita relativi al secondo *account* fino alla loro cancellazione. L'Autorità ha anche accertato che la società non aveva fornito, né prima dell'operazione di fusione né successivamente alla stessa, un'adeguata informativa al segnalante in merito al trattamento dei dati con riferimento all'utilizzo dell'*account* di posta elettronica aziendale e ai possibili controlli esercitati su quest'ultimo dal datore di lavoro.

Il Garante, nel rammentare quanto previsto dall'art. 2504-*bis* del c.c., ha ritenuto violati gli artt. 5, par. 1, lett. *a*), 12 e 13 del RGPD.

In merito alla persistente attività degli *account* di posta elettronica aziendale a seguito della cessazione del rapporto di lavoro, poi, è stata accertata la violazione dell'art. 5, par. 1, lett. *c*), del RGPD, in quanto, considerato che lo scambio di corrispondenza elettronica estranea o meno all'attività lavorativa su un *account* aziendale di tipo individualizzato configura un'operazione che consente di conoscere alcune informazioni personali relative all'interessato, in conformità ai principi in materia di protezione dei dati personali, dopo la cessazione del rapporto di lavoro il titolare del trattamento deve provvedere alla rimozione dell'*account,* previa disattivazione dello stesso e contestuale adozione di sistemi automatici volti ad informarne i terzi e a fornire a questi ultimi indirizzi *e-mail* alternativi riferiti alla sua attività professionale.

La conservazione, tramite *server,* delle comunicazioni relative agli *account* di posta elettronica aziendale per asserite ragioni di tutela in giudizio è risultata non conforme ai principi di minimizzazione dei dati (art. 5, par. 1, lett. *c*), del RGPD) e di

limitazione della conservazione (art. 5, par. 1, lett. *e*), del RGPD) in quanto "il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti".

Il Garante ha inoltre ribadito che la conservazione di documentazione necessaria per l'ordinario svolgimento e la continuità dell'attività aziendale, è assicurata, in primo luogo, dalla predisposizione di sistemi di gestione documentale idonei ad individuare i documenti archiviabili nel corso dell'attività lavorativa con modalità idonee a garantire le prescritte caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità. I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche.

Sempre con riferimento alla conservazione tramite *server* delle comunicazioni relative agli *account* di posta elettronica aziendale, in relazione alla quale è stata accertata la possibilità della società di accedere sia ai dati esterni sia al contenuto della casella *e-mail* in costanza di rapporto di lavoro, il Garante ha accertato la violazione degli artt. 113 (che rinvia all'art. 8, l. n. 300/1970) e 114 del Codice (che rinvia all'art. 4, l. n. 300/1970). Ciò in quanto "la conservazione preventiva e sistematica dei dati esterni e del contenuto delle *e-mail* inviate e ricevute in occasione dello svolgimento dell'attività lavorativa è idonea a consentire di ricostruire l'attività del dipendente e di effettuare un controllo sulla stessa, anche indirettamente, al di là delle finalità tassativamente ammesse dall'art. 4, l. n. 300/1970 e comunque in assenza delle garanzie procedurali ivi previste" nonché in quanto, attraverso la sistematica conservazione delle *e-mail,* la società può, inoltre, conoscere informazioni relative alla vita privata del lavoratore non rilevanti ai fini della valutazione dell'attitudine professionale dello stesso.

È stata pertanto ravvisata una violazione del principio di liceità del trattamento (art. 5, par. 1, lett. *a*), del RGPD in relazione agli artt. 113 e 114 del Codice) nonché dell'art. 88 del RGPD in quanto gli artt. 113 e 114 costituiscono norme del diritto nazionale "più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro" individuate dall'art. 88 del RGPD. La società è stata quindi condannata al pagamento di una sanzione amministrativa pecuniaria ed è stato vietato l'ulteriore trattamento dei dati estratti dall'*account* di posta elettronica aziendale riferito al segnalante in relazione al quale la società ha dichiarato di continuare a conservare le *e-mail,* fatta salva la loro conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria, per il tempo necessario a tale scopo, tenuto conto di quanto previsto dall'art. 160-*bis* del Codice (provv. 29 settembre 2021, n. 353, doc. web n. 9719914).

Account di posta elettronica aziendale successiva alla cessazione del rapporto di lavoro

Sempre con riferimento al trattamento dei dati relativi ad *account* di posta elettronica aziendale da parte di una società, dopo la cessazione del rapporto di lavoro con il reclamante, il Garante ha ritenuto violati i principi di minimizzazione e limitazione della conservazione di cui all'art. 5, par. 1, lett. *c*) ed *e*), del RGPD, nonché la violazione delle disposizioni relative all'informativa artt. 5, par. 1, lett. *a*) e 13 del RGPD.

Considerato, inoltre, che la società ha fornito riscontro alle richieste dell'Autorità ai sensi dell'art. 157 del Codice solo a seguito dell'effettuazione di un accertamento ispettivo delegato al Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza, il Garante ha condannato la società al pagamento di una sanzione amministrativa pecuniaria (provv. 16 dicembre 2021, n. 440, doc. web n. 9739653).

14

14.4. *I trattamenti dei dati giudiziari e dei dati particolari*

A seguito di un reclamo, l'Autorità ha accertato che alcuni dati relativi alla salute dell'interessato erano stati comunicati via *e-mail* dal titolare (società datore di lavoro del reclamante) a un soggetto esterno alla società, in un contesto caratterizzato dall'assenza di misure relative alla disciplina della raccolta e della circolazione dei dati personali relativi alla salute dei dipendenti che avrebbero dovuto essere predisposte in relazione agli specifici livelli di rischio dell'attività svolta in concreto dalla società. Ciò è stato ritenuto in violazione dei principi di liceità e minimizzazione dei dati (v. art. 5, par. 1, lett. *a*) e *c*), del RGPD) e delle condizioni di liceità dei trattamenti di dati particolari nel contesto del rapporto di lavoro (v. art. 9, par. 2, lett. *b*), del RGPD). È risultato inoltre essere stato violato l'art. 32 del RGPD in base al quale il titolare è tenuto a predisporre misure tecniche ed organizzative adeguate a garantire un livello di sicurezza riferito agli specifici profili di rischio del trattamento effettuato.

Il Garante ha ritenuto altresì illecito il trattamento consistente nell'acquisizione, da parte della società, del certificato del casellario giudiziale mediante consegna da parte dell'interessato al titolare nella fase preassuntiva, alla luce della specifica disciplina vigente all'epoca del fatto oggetto di reclamo, antecedente alla definitiva applicazione del RGPD nel nostro ordinamento. È stata quindi applicata una sanzione amministrativa pecuniaria (provv. 11 febbraio 2021, n. 47, doc. web n. 9562814).

L'Autorità ha altresì ribadito la necessità che il trattamento dei dati giudiziari avvenga previa scrupolosa osservanza delle norme di protezione dei dati e delle discipline di settore applicabili.

Estrazione del certificato del casellario giudiziale e disciplina sui contratti pubblici

Ha in particolare adottato un provvedimento nei confronti di una società che, in qualità di stazione appaltante che gestisce un proprio albo dei fornitori, aveva estratto il certificato giudiziale del reclamante e lo aveva trasmesso in copia alla società presso la quale egli ricopriva il ruolo di sindaco supplente. Sebbene il trattamento oggetto di reclamo fosse avvenuto in epoca antecedente all'attuazione del RGPD nell'ordinamento nazionale, la decisione ha applicato norme e principi che trovano in buona parte corrispondenza nella disciplina vigente (art. 10 del RGPD; art. 2-*octies* del Codice). In particolare il Garante ha chiarito che la stazione appaltante avrebbe dovuto, in primo luogo, predisporre in termini chiari e univoci la modulistica relativa all'iscrizione al proprio albo speciale, tenuto conto della interpretazione letterale e sistematica delle norme di settore in materia di contratti pubblici e della sussistenza di interpretazioni non univoche in giurisprudenza. In applicazione, inoltre, dei principi di necessità, pertinenza e non eccedenza (espressione del principio generale di proporzionalità, che costituisce parametro generale di legittimità delle limitazioni del diritto alla protezione dei dati personali ex art. 52 della CDFUE), stabiliti al tempo dei fatti oggetto di reclamo dagli artt. 3 e 11 del Codice previgente e dalla autorizzazione generale n. 6/2016, la società avrebbe dovuto valutare con attenzione la necessità e la pertinenza del trattamento che si accingeva ad effettuare, prima di procedere alla estrazione dei dati dal casellario verificando se il sindaco supplente avesse ricoperto (o meno) incarichi effettivi e, in ogni caso, prima di effettuare la comunicazione del certificato alla società presso la quale ricopriva l'incarico, anche in considerazione dei possibili effetti di tale ulteriore attività di trattamento sull'interessato – effetti che si sono in concreto verificati con le dimissioni rassegnate da quest'ultimo dagli incarichi ricoperti.

In conclusione l'Autorità ha stabilito che il trattamento dei dati giudiziari effettuato dalla società, sia in fase di estrazione del certificato, sia in occasione della comunicazione della copia del certificato ad altro soggetto, ha comportato una

irragionevole compressione del diritto alla riservatezza dell'interessato. Alla luce della particolarità e della novità del caso concreto unitamente al provvedimento *de quo* è stato adottato un provvedimento di ammonimento nei confronti della società (provv. 16 dicembre 2021, n. 441, doc. web n. 9742485).

14.5. *Esercizio dei diritti*

Il Garante, nell'esaminare alcuni reclami in materia di esercizio dei diritti riconosciuti dal RGPD agli interessati, ha rammentato ai titolari del trattamento l'obbligo di agevolare l'esercizio dei diritti riconosciuti agli interessati ai sensi dell'art. 12 del RGPD, fornendo un chiaro ed adeguato riscontro agli stessi nel rispetto dei termini individuati dall'ordinamento. È stato precisato, inoltre, che grava sul titolare del trattamento l'obbligo di manifestare il diniego con la chiara indicazione dei motivi sottostanti, indicando, altresì, la possibilità di presentare reclamo al Garante o, in alternativa, ricorso giurisdizionale.

Diritto di accesso ai dati

Nell'anno di riferimento, il Garante, dopo avere esaminato una pluralità di reclami aventi ad oggetto l'esercizio del diritto di accesso degli interessati ai dati personali trattati nel corso del rapporto di lavoro, ha adottato un provvedimento nei confronti di una società cooperativa che, in qualità di datore di lavoro, non aveva riscontrato le istanze degli interessati per accedere ai propri dati personali contenuti nei tabulati delle timbrature.

Considerato che, solo a seguito della presentazione dei reclami, nel corso del procedimento instaurato dall'Autorità, la società ha provveduto ad inviare agli interessati i dati oggetto delle istanze di accesso, il Garante ha ritenuto illecita la menzionata condotta in relazione all'art. 12, parr. 2 e 3 con riferimento all'art. 15 del RGPD.

L'Autorità ha altresì ribadito che, in base alla costante giurisprudenza di legittimità, il diritto di accesso ai propri dati personali, anche nell'ambito del rapporto di lavoro, "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 […] 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" (provv. 25 marzo 2021, n. 104, doc. web n. 9583835).

Il Garante ha adottato un ulteriore provvedimento nei confronti di una società a seguito della presentazione di un reclamo nel quale era stata lamentata l'impossibilità di esercitare il diritto di cui all'art. 15 del RGPD relativamente al fascicolo personale del lavoratore e, in particolare, agli attestati di formazione ivi contenuti.

In base alle risultanze dell'istruttoria è emerso che la società aveva dato all'interessato, in un primo momento, un riscontro insufficiente all'istanza di accesso agli attestati di formazione richiesti, dichiarando esclusivamente di non potere dare seguito alla stessa, ed omettendo, quindi, di precisare i motivi dell'inottemperanza; successivamente la società, a seguito di una ulteriore istanza di accesso presentata sempre dal reclamante, si era limitata a dichiarare di avere già consegnato la documentazione relativa allo stesso in suo possesso e di mettere a sua disposizione la cartella sanitaria.

È altresì emerso che la società aveva consegnato, anche in data antecedente rispetto all'intervento del Garante, a ridosso della cessazione del rapporto di lavoro con il reclamante, tutti gli attestati di formazione relativi allo stesso dei quali era in possesso. La società aveva inoltre trasmesso nuovamente tali attestati in seguito all'apertura dell'istruttoria da parte dell'Autorità, precisando, per quanto riguarda quelli

14

non in suo possesso, di non essere in grado di soddisfare la richiesta in quanto due attestati erano stati rilasciati esclusivamente al lavoratore e di un terzo non era stata rilasciata copia alcuna.

Il Garante ha, quindi, dichiarato illecita la condotta della società in quanto non conforme all'art. 12, par. 4, con riferimento all'art. 15 del RGPD in ragione della mancata precisa indicazione all'interessato dei motivi di diniego del diritto di accesso ai dati contenuti nei tre attestati di formazione e per l'assenza dell'indicazione della possibilità di proporre reclamo a un'autorità di controllo o ricorso giurisdizionale ed ha ammonito il titolare del trattamento sulla necessità di conformarsi alla menzionata disposizione (provv. 11 febbraio 2021, n. 63, doc. web n. 9567218).

14.6. *La protezione dei dati nell'ambito del rapporto di lavoro pubblico. I trattamenti effettuati per finalità di prevenzione dal contagio da Covid-19*

Nel 2021, l'Autorità ha affrontato numerose questioni relative ai trattamenti di dati personali effettuati da soggetti pubblici o da soggetti privati che svolgono compiti di interesse pubblico, con riguardo, in particolare, ai trattamenti: volti ad assicurare la salute e la sicurezza sui luoghi di lavoro (anche nel contesto dell'emergenza epidemiologica da Sars-CoV-2); connessi all'impiego di strumenti tecnologici; finalizzati alla gestione del rapporto di lavoro nelle sue varie fasi (inclusa quella del reclutamento mediante procedure concorsuali); effettuati in occasione dell'assolvimento degli obblighi derivanti da specifiche normative di settore applicabili specialmente all'ambito pubblico, come la disciplina in materia di trasparenza dell'azione amministrativa e quella relativa alla tutela della riservatezza del dipendente che segnala illeciti (cd. *whistleblowing*).

Nel periodo di riferimento, l'Autorità ha continuato a fornire indicazioni e chiarimenti, ai sensi dell'art. 57, par. 1, lett. *b*) e *d*), del RGPD, agli interessati e ai titolari a vario titolo coinvolti nei trattamenti di dati personali nel contesto lavorativo (datori di lavoro, medici competenti, ordini professionali e altri soggetti istituzionali) nel quadro dell'emergenza epidemiologica da Sars-CoV-2, avviando campagne di informazione e adottando specifici documenti di indirizzo volti, in particolare, a prevenire autonome decisioni o iniziative dei datori di lavoro non previste dalla legge, con possibili effetti discriminatori per gli interessati.

L'Autorità in molteplici occasioni ha fornito il proprio parere, ai sensi dell'art. 58, par. 3, lett. *b*), del RGPD, sulle disposizioni attuative di un quadro normativo in costante aggiornamento, concernenti in modo particolare il settore del lavoro, ed ha avviato specifiche istruttorie, anche sulla base dei numerosi reclami e segnalazioni pervenuti.

La sicurezza dei luoghi di lavoro, la vaccinazione anti Covid-19 dei lavoratori e il ruolo del medico competente

A seguito di notizie di stampa e richieste di chiarimenti, è stata portata all'attenzione dell'Autorità la questione della possibilità, per il datore di lavoro, di richiedere la vaccinazione dei propri dipendenti o di altro personale prospettando, in taluni casi, anche l'irrogazione di sanzioni disciplinari in caso di rifiuto da parte del lavoratore. Al riguardo, l'Autorità, con specifiche FAQ (Vaccinazione dei dipendenti: le FAQ del Garante *privacy.* Principi generali e *focus* sugli operatori sanitari del 17 febbraio 2021, doc. web n. 9543615), ha chiarito che il datore di lavoro non può acquisire, neanche con il consenso del dipendente o tramite il medico compente, i nominativi del personale vaccinato o la copia delle certificazioni vaccinali. Ciò anche per l'impossibilità di considerare il consenso dei dipendenti una valida condizione di liceità per il trattamento dei dati personali in ambito lavorativo, specie quando il datore di lavoro sia un'autorità pubblica (cons. 43 del RGPD), e per le disposi-

zioni nazionali che vietano al datore di lavoro di trattare dati non pertinenti e non attinenti alla valutazione dell'attitudine professionale del lavoratore (cfr. art. 113 del Codice, che rinvia agli artt. 8 della l. n. 300/1970, e 10, d.lgs. n. 276/2003).

In tale quadro, il datore di lavoro può venire a conoscenza del solo giudizio di idoneità alla mansione specifica e delle eventuali prescrizioni fissate dal medico competente come condizioni di lavoro, e deve limitarsi ad attuare tali prescrizioni. In presenza di un giudizio di inidoneità da parte del medico competente, il datore deve adibire il lavoratore, ove possibile, a mansioni equivalenti o inferiori, garantendo, altresì, il trattamento corrispondente alle mansioni di provenienza (art. 42, d.lgs. n. 81/2008; v. FAQ nn. 1 e 2).

Nei casi di esposizione diretta ad agenti biologici durante il lavoro, come, ad esempio, nel contesto sanitario, l'Autorità, auspicando un intervento del legislatore nazionale concernente l'eventuale introduzione della vaccinazione quale requisito per lo svolgimento di determinate professioni o mansioni, ha precisato che trovano applicazione le misure speciali di protezione di cui all'art. 279, d.lgs. n. 81/2008 ed ha ricordato che, anche in tale quadro, solo il medico competente può trattare i dati personali relativi alla vaccinazione dei dipendenti e, se del caso, tenerne conto in sede di valutazione dell'idoneità alla mansione specifica. Il datore di lavoro deve invece limitarsi ad attuare le misure indicate dal medico competente nei casi di giudizio di parziale o temporanea inidoneità alla mansione cui è adibito il lavoratore (art. 279, 41 e 42, d.lgs. n. 81/2008; v. FAQ n. 3).

Successivamente l'articolo 4 del d.l. 1° aprile 2021, n. 44, ha previsto che, al fine di tutelare la salute pubblica e mantenere adeguate condizioni di sicurezza del lavoro nell'erogazione delle prestazioni di cura e assistenza, la vaccinazione anti Sars-CoV-2 costituisce per gli esercenti le professioni sanitarie e gli operatori di interesse sanitario un "requisito essenziale per l'esercizio della professione e per lo svolgimento delle prestazioni lavorative".

Con successivi decreti legge tale obbligo vaccinale è stato esteso ad altre categorie professionali, quali tutti i soggetti, anche esterni, che svolgono, a qualsiasi titolo, la propria attività lavorativa nelle strutture residenziali, socio-assistenziali e socio-sanitarie (d.l. n. 111/2021), nonché, in particolare, il personale della scuola, del comparto difesa, sicurezza e soccorso pubblico, della polizia locale e degli istituti penitenziari (d.l. n. 172/2021).

In successivi provvedimenti di carattere generale e documenti di indirizzo, nonché in decisioni su singoli casi, l'Autorità ha precisato che, anche nel periodo emergenziale, sulla base dello stato della regolazione in vigore e stante la libertà di scelta da parte delle persone in ambito vaccinale, fatta eccezione per le predette categorie di lavoratori, il datore di lavoro non è legittimato a trattare i dati personali relativi alla vaccinazione anti Sars-CoV-2 dei dipendenti, né è consentito far derivare alcuna conseguenza, positiva o negativa, in ragione della scelta del lavoratore in ordine all'adesione o meno alla campagna vaccinale.

Al riguardo, uno specifico documento di indirizzo, in risposta alle numerose richieste di chiarimenti pervenute nel corso del tempo, ha fornito indicazioni generali sul ruolo del medico competente in materia di igiene e sicurezza sul luogo di lavoro, anche alla luce del quadro normativo emergenziale (14 maggio 2021, doc. web n. 9585367).

In particolare, è stato chiarito che la disciplina in materia di tutela della salute e della sicurezza nei luoghi di lavoro (d.lgs. n. 81/2008) individua la funzione del medico competente come autonoma rispetto a quella del datore di lavoro, prevedendo specifici e distinti obblighi, nonché le diverse responsabilità di ciascuno (v. artt. 18 e 25) e delineando, sotto il profilo della protezione dei dati, l'ambito del rispettivo

14

trattamento. Il medico non è, infatti, tenuto a seguire le istruzioni del datore di lavoro, dovendo, invece, operare con autonomia e terzietà rispetto allo stesso. Conseguentemente, nell'ambito dell'attività di sorveglianza sanitaria e di tenuta delle cartelle sanitarie e di rischio dei singoli lavoratori, il medico competente è, per legge, l'unico legittimato a trattare i dati personali di natura sanitaria, non potendo informazioni relative, ad esempio, alla diagnosi o all'anamnesi familiare del lavoratore, essere in alcun modo trattate dal datore di lavoro, se non nella misura del mero giudizio di idoneità alla mansione specifica e delle eventuali prescrizioni che il professionista fissa come condizioni di lavoro. Il datore di lavoro non può, peraltro, avere accesso ai dati contenuti nella documentazione sanitaria del lavoratore nemmeno in caso di cessazione della propria attività o del rapporto di lavoro con l'interessato.

Sulla base di tali considerazioni, il Garante, confermando un orientamento già espresso in passato, ha chiarito che il medico, non trattando i dati per conto del datore di lavoro, agisce in qualità di titolare del trattamento (artt. 4, n. 7 e 24 del RGPD).

L'Autorità ha, inoltre, fornito specifici chiarimenti con riguardo ai casi in cui il servizio di medicina del lavoro è fornito da strutture sanitarie pubbliche e al diverso caso dell'individuazione del medico competente tra i dipendenti della struttura.

Nel documento di indirizzo sono stati altresì individuati i principali adempimenti del medico competente in materia di protezione dei dati personali, indicando, ove possibile, modalità semplificate per assicurarne l'assolvimento (istituzione del registro delle attività di trattamento; informativa agli interessati; sicurezza dei dati personali; nomina del Rpd; cfr. artt. 14, 30, 32-34, 37-39 del RGPD).

Con riguardo al ruolo del medico competente nell'ambito dell'emergenza epidemiologica, tenendo conto anche delle indicazioni del Ministero della salute, si è evidenziato che lo stesso è chiamato a collaborare con il datore di lavoro e con il servizio di prevenzione e protezione nella valutazione dei rischi, nell'individuazione, attuazione e perfezionamento delle misure e nell'osservanza dei protocolli anti-contagio, nell'informazione e formazione dei lavoratori sul rischio di contagio (art. 25 del citato d.lgs. n. 81/2008 e s.m.i.), nell'esame dei rischi riguardanti gruppi di lavoratori maggiormente esposti al contagio (es. operatori sanitari, Forze dell'ordine) o in particolari situazioni di fragilità legata a fattori quali l'età anagrafica o a situazioni di pregressa morbilità. Il medico competente, inoltre, prosegue e intensifica l'attività di sorveglianza sanitaria e le connesse visite mediche nei casi previsti dalla disciplina di settore (art. 41 del medesimo decreto), anche venendo coinvolto nella precoce identificazione dei contatti in ambito lavorativo (cd. *contact tracing*) e nel loro isolamento.

In tale quadro, le principali attività di trattamento dei dati – raccolta delle adesioni, somministrazione, registrazione nei sistemi regionali dell'avvenuta vaccinazione – devono essere effettuate dal medico competente o da altro personale sanitario, restando preclusa al datore di lavoro l'acquisizione di informazioni in merito alla vaccinazione o alla vita privata del dipendente (cfr. artt. 5, 6, 9, 88 del RGPD e 113 del Codice). Più nel dettaglio, con uno specifico documento di indirizzo dedicato alla vaccinazione nei luoghi di lavoro (Protocollo condiviso di aggiornamento delle misure per il contrasto e il contenimento della diffusione del virus Sars-CoV-2/Covid-19 negli ambienti di lavoro del 6 aprile 2021), è stato chiarito che la realizzazione dei piani vaccinali per l'attivazione di punti straordinari di vaccinazione nei luoghi di lavoro costituisce un'iniziativa di sanità pubblica. Pertanto, la responsabilità generale e la supervisione dell'intero processo rimangono in capo al Servizio sanitario regionale. In tale quadro, un ruolo centrale spetta al medico competente, o ad altro personale sanitario appositamente individuato, trovando, invece, applicazione, rispetto al datore di lavoro, i limiti sopra richiamati, sicché egli non può far derivare alcuna conseguenza, né positiva né negativa, dall'adesione o meno alla campagna

vaccinale (documento di indirizzo 13 maggio 2021, doc. web n. 9585300; cfr. comunicato stampa 14 maggio 2021, doc. web n. 9585263).

Tali temi, sono stati, altresì, oggetto di uno specifico provvedimento adottato nei confronti della Regione siciliana, a fronte di un'iniziativa (ordinanza 7 luglio 2021, n. 75 del Presidente della Regione) volta a introdurre a livello regionale requisiti professionali e conseguenti trattamenti di dati personali, connessi allo stato vaccinale dei dipendenti degli enti pubblici regionali, non previsti dalla normativa nazionale.

Al riguardo, il Garante, ha precisato che la materia della sanità pubblica è soggetta a riserva di legge statale e che il trattamento dei dati personali, anche relativi alla vaccinazione dei dipendenti, può certamente essere effettuato dal solo medico competente, stante gli specifici limiti per il trattamento di tali dati da parte del datore di lavoro, ma pur sempre nei limiti e alle condizioni stabilite dalla disciplina di settore in materia di sicurezza sul lavoro, che perimetra l'ambito del trattamento consentito anche al medico competente.

Nell'ambito della verifica dell'idoneità alla "mansione specifica" del dipendente, infatti, il medico può, "in funzione della valutazione del rischio" concreto e delle "condizioni di salute" del singolo lavoratore, ovvero su richiesta dello stesso in presenza di proprie specifiche o sopravvenute condizioni di salute, stabilire caso per caso se ricorrano i presupposti e la necessità di sottoporre i lavoratori a ulteriori visite straordinarie e/o a indagini diagnostiche (art. 41, commi 2 e 4, d.lgs. n. 81/2008). Ciò in quanto il medico, anche nel periodo emergenziale, non tratta i dati per conto o in base alle istruzioni e indicazioni di altri soggetti (enti pubblici, autorità sanitarie, datori di lavoro) ma in qualità di titolare del trattamento.

Per tali ragioni, la previsione contenuta nell'ordinanza presidenziale di dar corso a una ricognizione generalizzata del numero di dipendenti non vaccinati e l'indiscriminata effettuazione di visite straordinarie in favore di tutti i dipendenti è stata ritenuta dall'Autorità non conforme al quadro normativo in materia di salute e sicurezza sui luoghi di lavoro.

Di conseguenza, anche alla luce delle successive precisazioni contenute in alcuni documenti interpretativi della regione, il Garante ha ritenuto che "l'assegnazione del lavoratore ad altra mansione per effetto dell'accertata inidoneità siccome discendente dall'omessa effettuazione del vaccino" introducesse, in realtà, su base regionale un requisito per lo svolgimento di determinate mansioni (quelle che implicano "il contatto diretto del lavoratore con l'utenza esterna"), generando una disparità di trattamento rispetto al personale che svolge le medesime mansioni sull'intero territorio nazionale.

Per tali ragioni, il Garante ha emanato un provvedimento di avvertimento nei confronti della Regione siciliana e di tutti gli altri soggetti pubblici e privati coinvolti (aziende sanitarie provinciali, datori di lavoro, medici competenti), ai sensi dell'art. 58, par 2, lett. *a*), del RGPD, ritenendo che i trattamenti previsti dall'ordinanza avrebbero potuto verosimilmente violare le disposizioni in materia di protezione dei dati personali di cui agli artt. 5, 6, 9, 25, 32 e 88 del RGPD e 2-*ter,* 2-*sexies* e 113 del Codice in riferimento all'art. 8 della l. 20 maggio 1970, n. 300 e all'art. 10, d.lgs. 10 settembre 2003, n. 276 (provv. 22 luglio 2021, n. 273, doc. web n. 9683814; cfr. comunicato stampa 23 luglio 2021, doc. web n. 9683768).

Le certificazioni verdi per accedere ai luoghi di lavoro e gli obblighi vaccinali anti Covid-19 per specifiche categorie di lavoratori

Alla luce del regolamento (EU) 2021/953 – che disciplina il rilascio, la verifica e l'accettazione di certificati interoperabili di vaccinazione, di test e di guarigione in relazione alla Covid-19 (certificato Covid digitale dell'UE) per agevolare la libera circolazione delle persone durante la pandemia di Covid-19 (cons. nn. 36, 37 e 48) – e dei consolidati orientamenti della giurisprudenza costituzionale in merito alla riserva di legge statale sulla protezione dati (cfr. Corte cost., sent. n. 271/2005; Corte cost., sent. n. 37/21; Corte cost., ord. n. 4/21), l'Autorità ha ribadito, in numerose

14

occasioni, le garanzie che le disposizioni nazionali devono prevedere in merito ai trattamenti funzionali alle verifiche del cd. *green pass,* al fine di prevenire discriminazioni nei diversi contesti di utilizzo (v. audizione del Presidente del Garante sulle tematiche relative alla certificazione verde Covid-19 del 6 maggio 2021, doc. web n. 9583365).

Con riguardo all'ordinamento italiano, il d.l. 22 aprile 2021, n. 52, (conv. con mod. dalla l. 17 giugno 2021, n. 87, e succ. mod.), quale misura urgente per contenere e contrastare l'emergenza epidemiologica, ha introdotto l'utilizzo della certificazione verde ai fini degli spostamenti sul territorio nazionale e, con interventi normativi successivi, per l'accesso a specifiche attività, servizi e eventi (cfr. in particolare, d.l. 18 maggio 2021, n. 65; d.l. 23 luglio 2021, n. 105; d.l. 6 agosto 2021, n. 111; d.l. 10 settembre 2021, n. 122; d.l. 21 settembre 2021, n. 127).

Successivamente, dapprima con riguardo al contesto scolastico e universitario (cfr. d.l. 6 agosto 2021, n. 111) e poi con riferimento all'ambito lavorativo pubblico e privato (cfr. d.l. 21 settembre 2021, n. 127), è stato previsto che, al fine di tutelare la salute pubblica e mantenere adeguate condizioni di sicurezza, sia nell'erogazione in presenza del servizio essenziale di istruzione che, in generale, ai fini dell'accesso ai luoghi di lavoro, il personale debba possedere ed esibire la certificazione verde in corso di validità.

In particolare, i controlli relativi al possesso delle certificazioni verdi in corso di validità, nei vari contesti lavorativi, devono essere effettuati da parte dei datori di lavoro o altro personale da questi autorizzato, con le modalità indicate dal d.P.C.M. 17 giugno 2021 e dai successivi decreti che lo hanno integrato e modificato, su cui il Garante ha reso il dovuto parere ai sensi del RGPD.

In occasione dei pareri resi su tali disposizioni attuative, l'Autorità ha richiamato l'attenzione sulla circostanza che, fatta eccezione per il personale dei settori per i quali la vaccinazione (obbligatoria) costituisce specifico requisito professionale, in tutti i restanti contesti lavorativi pubblici e privati, il datore di lavoro non è legittimato a trattare i dati personali relativi alla vaccinazione dei dipendenti.

Al riguardo, l'Autorità ha reso in via d'urgenza, stante la rappresentata esigenza di consentire la ripresa in sicurezza delle attività didattiche in presenza, il proprio parere sullo schema di d.P.C.M. che introduce modalità semplificate per la verifica del possesso delle certificazioni verdi del personale scolastico. Tali modalità, alternative a quelle ordinarie (che prevedono l'uso dell'*app* VerificaC19, comunque utilizzabile), consistono nella possibilità di utilizzare un'apposita funzionalità della Piattaforma nazionale-DGC che, attraverso il Sistema informativo dell'istruzione-Sidi, consente agli uffici scolastici regionali e alle scuole statali del sistema nazionale di istruzione la verifica quotidiana del possesso delle certificazioni verdi in corso di validità ma non permette di visualizzare le ulteriori informazioni trattate nell'ambito della Piattaforma nazionale-DGC, quali gli specifici presupposti che hanno determinato il rilascio della certificazione verde al personale, essendo consentita, in caso di mancato possesso di una valida certificazione, la raccolta dei soli dati strettamente necessari nell'ambito del rapporto di lavoro (es. sospensione, mancata corresponsione della retribuzione), che rilevano anche sul piano sanzionatorio.

Tale quadro normativo contiene specifiche misure a tutela dei diritti degli interessati, prevedendo, in particolare, che le istituzioni scolastiche, in qualità di datori di lavoro, si limitino a verificare il mero possesso della certificazione verde da parte del personale; che la verifica quotidiana sia effettuata esclusivamente con riguardo al personale per cui è prevista l'effettiva presenza in servizio nel giorno della verifica, escludendo comunque il personale assente per specifiche causali (ad es. ferie, permessi, malattia, ecc.); che il personale della scuola interessato dal processo di verifica

sia opportunamente informato dall'istituzione scolastica di appartenenza in merito al trattamento dei dati attraverso una specifica informativa, anche mediante comunicazione resa alla generalità del personale; che i soggetti tenuti ai controlli possano accedere, in modo selettivo, ai soli dati del personale in servizio presso le istituzioni scolastiche di propria competenza (individuate mediante il codice meccanografico), resi disponibili dalla banca dati del Sidi; che le operazioni di verifica del possesso delle certificazioni verdi da parte dei soggetti tenuti ai controlli siano oggetto di registrazione in appositi *log* (conservati per dodici mesi), che non contengono l'esito delle verifiche; che l'aggiornamento della valutazione d'impatto sulla protezione dei dati relativa ai trattamenti connessi alle certificazioni verdi sia effettuato tenendo conto degli specifici rischi connessi al trattamento, su larga scala e concernente dati sulla salute di interessati vulnerabili (dipendenti), avendo particolare attenzione alle possibili conseguenze discriminatorie, anche indirette, nel contesto lavorativo (artt. 35 e 88 del RGPD).

L'Autorità, anche a seguito delle interlocuzioni con i rappresentanti del Ministero dell'istruzione e del Ministero della salute, ha ritenuto appropriato il complesso delle misure di garanzia adottate per tutelare i diritti fondamentali e gli interessi delle persone fisiche, e ha quindi espresso parere favorevole sullo schema di decreto (provv. 31 agosto 2021, n. 306, doc. web n. 9694010; v. anche comunicato stampa 31 agosto 2021, doc.web n. 9693841).

Anche il parere sullo schema di d.P.C.M., che ha disciplinato le modalità di verifica automatizzate in tutti gli altri contesti lavorativi, mediante sistemi informativi già esistenti e accessibili da parte dei singoli datori di lavoro, si è fondato sulla necessità di garantire i diritti e le libertà dei lavoratori, nonché la sicurezza, l'esattezza e l'aggiornamento dei dati in base ai quali è generata la certificazione verde, individuando al contempo modalità semplificate da utilizzare per le verifiche.

Alla luce del confronto con l'Autorità analoghe garanzie per la verifica delle certificazioni in parola sono state introdotte nelle disposizioni che hanno integrato e modificato il d.P.C.M. 17 giugno 2021. In particolare, tale quadro ha previsto che l'attività di verifica del possesso delle certificazioni verdi possa essere effettuata anche attraverso modalità alternative all'*app* VerificaC19, quali l'impiego di un pacchetto di sviluppo per applicazioni (SDK), rilasciato dal Ministero con licenza *open source,* da integrare nei sistemi di controllo degli accessi ovvero, per i datori di lavoro pubblici e privati, mediante l'utilizzo di una specifica funzionalità della Piattaforma NoiPA o del portale istituzionale Inps, nonché, esclusivamente con riguardo alle amministrazioni pubbliche con più di mille dipendenti, attraverso un servizio di interoperabilità applicativa con la Piattaforma nazionale-DGC. Il Garante ha pertanto espresso in via d'urgenza parere favorevole sullo schema di decreto, sottolineando la necessità di dare piena operatività all'istituto della revoca delle certificazioni verdi, al fine di garantire la reale efficacia della misura di sanità pubblica connessa all'introduzione della stessa per l'accesso ai luoghi di lavoro e, in pari tempo, il trattamento di dati esatti e aggiornati (es. nei casi di sopraggiunta positività del lavoratore vaccinato). Considerati i maggiori rischi per gli interessati nel contesto lavorativo, è stata, altresì, rappresentata l'urgenza di completare il quadro giuridico di riferimento mediante individuazione delle specifiche tecniche per trattare in modalità digitale le certificazioni di esenzione alla vaccinazione e consentirne la verifica digitale, assicurando contestualmente la protezione dei dati personali in esse contenuti (provv. 11 ottobre 2021, n. 363, doc. web n. 9707561; v. anche comunicato stampa 12 ottobre 2021, doc. web n. 9707561).

A seguito delle disposizioni normative (d.l. 26 novembre 2021, n. 172) che hanno istituito l'obbligo vaccinale anche per altre categorie di lavoratori (v. *supra*) e

14

hanno introdotto un nuovo procedimento di verifica di tale obbligo per gli operatori sanitari (che, diversamente dal passato, prevede il diretto coinvolgimento degli ordini professionali, per il tramite delle rispettive federazioni nazionali), il Garante ha reso il parere sul decreto che ha modificato, in merito, il richiamato d.P.C.M. 17 giugno 2021 concernente, tra gli altri numerosi aspetti, anche le modalità automatizzate di verifica dell'adempimento del predetto obbligo da parte dei datori di lavoro o dei responsabili delle istituzioni presso cui tali categorie di interessati prestano servizio (cfr. par. 5.1.2).

Con specifico riguardo alle modalità automatizzate di verifica, come evidenziato nel predetto parere, i trattamenti effettuati per la verifica dell'obbligo vaccinale, nei casi previsti dalla legge, devono essere tenuti separati da quelli effettuati per la verifica quotidiana del possesso della certificazione verde per l'accesso fisico alle sedi di lavoro.

La diversa finalità delle verifiche incide, in particolare, sia sulla periodicità delle stesse in quanto le verifiche circa il rispetto dell'obbligo vaccinale devono essere effettuate con una cadenza più ampia (anche *una tantum*), non potendo ritenersi giustificata – diversamente da quelle relative al possesso di una valida certificazione verde – l'esecuzione di verifiche relative all'assolvimento dell'obbligo vaccinale con cadenza ravvicinata (quotidiana o, comunque, frequente).

Con riguardo alle modalità di annotazione nell'albo professionale *online* dell'intervenuta sospensione in conseguenza della mancata vaccinazione da parte dell'esercente la professione sanitaria, le norme in esame, recependo le indicazioni dell'Autorità, hanno, tra l'altro, stabilito che al fine di evitare la diffusione, anche *online,* di informazioni particolarmente delicate, l'annotazione in questione, sia effettuata senza ulteriori specificazioni dalle quali sia possibile desumere il mancato rispetto dell'obbligo vaccinale.

Alla luce della piena attuazione dell'istituto della revoca delle certificazioni verdi, è stato, altresì, previsto, come auspicato dall'Autorità in coerenza con il principio di esattezza dei dati, che nei casi in cui il lavoratore si avvalga della facoltà prevista dalla legge di consegna della certificazione verde al proprio datore di lavoro, questo sia comunque tenuto a effettuare il regolare controllo sulla perdurante validità della certificazione del lavoratore effettivamente in servizio con le modalità previste dalla disciplina di settore (mediante lettura del QR *code* della copia in possesso del datore di lavoro attraverso l'*app* VerificaC19, ovvero mediante le previste modalità automatizzate; cfr. segnalazione al Parlamento e al Governo sul disegno di legge di conversione d.l. n. 127/2021 (AS 2394), doc. web n. 9717878; memoria del Presidente del Garante 7 dicembre 2021 su AS 2463 – conversione in legge del decreto-legge; provv.ti 26 novembre 2021, n. 172, doc. web n. 9725434, 13 dicembre 2021, n. 430, doc. web n. 9727220 nonché comunicato stampa 14 dicembre 2021, doc. web n. 9727103).

14.7. *I trattamenti dei dati mediante strumenti tecnologici*

A conclusione di specifici procedimenti originati da reclami e segnalazioni, che hanno richiesto anche il ricorso ad attività ispettive *in loco,* l'Autorità è tornata sul tema dell'impiego degli strumenti tecnologici nei diversi contesti lavorativi, evidenziando il rapporto tra la disciplina di settore (l. n. 300/1970) e la disciplina di protezione dei dati, che, pur costituendo normative autonome, dotate ciascuna di un proprio apparato sanzionatorio, posto a tutela di beni giuridici distinti e complementari, sono comunque integrate attraverso richiami incrociati che regolano

le condotte del datore di lavoro (artt. 113, 114 e 171 del Codice; v. anche art. 4, comma 3, l. n. 300/1970).

Sul rispetto della vita privata nei luoghi di lavoro, richiamando la sentenza della Corte europea dei diritti dell'uomo, nel caso Antović e Mirković v. Montenegro (Application n. 70838/13 del 28 novembre 2017) nonché, la raccomandazione CM/Rec(2015)5 del Comitato dei ministri agli Stati membri sul trattamento di dati personali nel contesto occupazionale (spec. punto 3), è stato chiarito che il mancato rispetto della predetta disciplina può comportare l'applicazione di sanzioni amministrative pecuniarie (cfr. artt. 83, par. 5, lett. *d*) e 88 del RGPD, nonché 114 del Codice, in riferimento all'art. 4, l. n. 300/1970), nonché può integrare la fattispecie di reato prevista dall'art. 171 del Codice.

14.7.1. Sistemi di controllo e filtraggio della navigazione internet dei dipendenti

A seguito di uno specifico reclamo presentato da un dipendente comunale, l'Autorità ha accertato che un comune aveva trattato dati personali relativi alla navigazione in internet in assenza della dovuta informativa, in violazione degli artt. 5, par. 1, lett. *a*) e 13 del RGPD.

Sebbene il datore di lavoro avesse stipulato uno specifico accordo con le organizzazioni sindacali, come richiesto dalla disciplina di settore, è emerso che le caratteristiche originarie del sistema di filtraggio del traffico di rete e le conseguenti operazioni di trattamento (raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web dei singoli dipendenti, memorizzazione per trenta giorni e possibilità di estrazione di reportistica relativa alla loro navigazione) non fossero necessarie e proporzionate rispetto alla finalità di protezione e sicurezza della rete interna invocata dal comune (cfr. cons. 49 e art. 6, par.1, lett. *e*), del RGPD), avendo riguardato, peraltro, dati non "adeguati, pertinenti e limitati" a quanto necessario a garantire la sicurezza della rete. Sotto tale profilo, il sistema impiegato dall'ente consentiva di registrare dati di dettaglio in ordine alla risorsa internet visitata (Url), che proprio in ragione del collegamento univoco con il nominativo del dipendente dava luogo alla raccolta sistematica di numerosi dati personali, anche non attinenti allo svolgimento della prestazione lavorativa, e informazioni potenzialmente relative alla vita privata dell'interessato, in contrasto con il divieto per il datore di lavoro di trattare dati "non attinenti alla valutazione dell'attitudine professionale del lavoratore" (art. 113 del Codice, in riferimento agli artt. 8, l. n. 300/1970 e 10, d.lgs. n. 276/2003).

Sono stati accertati, tra gli altri profili, la violazione del principio di limitazione della finalità e il mancato rispetto delle condizioni previste dalla disciplina di settore con riguardo all'utilizzo dei dati raccolti per altri fini connessi alla gestione del rapporto di lavoro. Al riguardo, è stato evidenziato che solo dal 2015 il quadro normativo vigente consente che i dati raccolti ai sensi dell'art. 4, commi 1 e 2, della l. n. 300/1970 possano essere utilizzati dal datore di lavoro "a tutti i fini connessi al rapporto di lavoro" a condizione che "sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n.196" (art. 4, comma 3, l. n. 300/1970). Diversamente, l'amministrazione effettuava fin dal 2000 tali trattamenti e i dati relativi alla navigazione web del reclamante, originariamente raccolti e trattati in maniera non conforme alla disciplina in materia di protezione dei dati (anche con riguardo all'obbligo di rendere l'informativa), sono stati successivamente impiegati per contestare addebiti disciplinari al personale, non rispettando quindi i presupposti e le condizioni previste dalla richiamata disciplina di settore all'art. 4, comma 3, l. n. 300/1970.

14

È stato, inoltre, verificato che il trattamento dei dati personali degli interessati è stato effettuato in assenza di una preliminare valutazione d'impatto sulla protezione dei dati, sulla base dell'erroneo presupposto che il trattamento non presentasse rischi specifici per gli stessi, in violazione dell'art. 35 del RGPD.

Sotto diverso profilo, è stato, altresì, verificato che il modulo originariamente in uso presso l'amministrazione, che il dipendente doveva compilare per richiedere al medico competente un accertamento straordinario sulle proprie condizioni di salute, nella parte in cui presupponeva la necessaria presa visione del direttore di ripartizione, non fosse conforme alle disposizioni nazionali in materia di salute e sicurezza dei luoghi di lavoro (d.lgs. 9 aprile 2008, n. 81), comportando – indipendentemente dall'espressa indicazione della patologia da parte del lavoratore – che soggetti delegati allo svolgimento delle funzioni datoriali all'interno dell'amministrazione venissero a conoscenza di dati personali relativi allo stato di salute, diversi e ulteriori rispetto a quelli consentiti dalla legge (in violazione degli artt. 5, 9, par. 2, lett. *b*) e 88 del RGPD).

In considerazione delle condotte accertate, il Garante ha comminato al titolare una sanzione pecuniaria e ha ingiunto allo stesso di adottare talune misure correttive (provv. 13 maggio 2021, n. 190, doc. web n. 9669974; v. anche *Newsletter* 22 giugno 2021, doc. web n. 9670319).

14.7.2. Sistema di gestione delle telefonate utilizzato per il servizio di assistenza all'utenza (call center inbound)

Con riguardo a una società privata, gestore del servizio di trasporto pubblico locale, l'Autorità ha accertato la violazione di numerose di disposizioni del RGPD e del Codice.

Nel corso dell'istruttoria, è emerso che il sistema per la gestione delle telefonate della clientela (*call center inbound*) da parte del personale addetto al *call center* rendeva possibili in particolare, la memorizzazione e il riascolto delle telefonate, nonché la raccolta di informazioni di dettaglio (meta informazioni: il nome dell'operatore, il numero chiamante, la data e l'ora della chiamata) associate in via diretta al dipendente che gestiva la telefonata con l'utente. Il Garante, nel solco di proprie precedenti decisioni su casi analoghi, nonché degli orientamenti della magistratura, del Ministero del lavoro e dell'Ispettorato nazionale del lavoro, ha ritenuto che tale sistema non potesse essere considerato tra gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (art. 4, comma 2, l. n. 300/1970). Il sistema, funzionale al perseguimento delle specifiche finalità (organizzative e produttive), poteva, invece, essere utilizzato solo nel rispetto delle garanzie procedurali prescritte dall'art. 4, comma, 1, ossia l'accordo sindacale o, in alternativa, l'autorizzazione pubblica. Tali garanzie, non erano, tuttavia, state adottate dal datore di lavoro, in violazione dell'art. 114 del Codice.

In questo quadro, la raccolta e memorizzazione per un arco temporale indefinito delle meta informazioni riferite direttamente ai dipendenti e alla loro attività lavorativa, non sono state ritenute conformi ai principi di minimizzazione e di limitazione della conservazione dei dati, nonché di protezione dei dati personali fin dalla progettazione e per impostazione predefinita, in violazione degli artt. 5, par. 1, lett. *c*) ed *e*) e 25 del RGPD. L'Autorità ha pertanto comminato una sanzione pecuniaria alla società, che, a seguito dell'accertamento ispettivo, aveva sospeso l'utilizzo del predetto sistema (provv. 28 ottobre 2021, n. 384, doc. web n. 9722661; v. anche *Newsletter* 3 dicembre 2021, doc. web n. 9722394).

14.7.3. Sistemi di videosorveglianza in contesti lavorativi

L'installazione di sistemi di videosorveglianza in contesti ove si svolge anche l'attività lavorativa richiede il necessario rispetto, non solo dei principi generali sul tratta-

mento dei dati (art. 5 del RGPD), ma anche della disciplina in materia di controlli a distanza, come requisito di liceità del trattamento (art. artt. 5, par. 1, lett. *a*), 6, lett. *c*) ed *e*), 88, del RGPD, nonché art. 114 del Codice). In particolare "gli impianti audiovisivi e gli altri 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 nel rispetto delle altre garanzie procedimentali ivi previste, ossia l'accordo con le rappresentanze sindacali o, in alternativa, l'autorizzazione pubblica (art. 4, comma 1, l. n. 300/1970, come modificato dal d.lgs. n. 151/2015).

In tale quadro è stato definito un reclamo proposto nei confronti di un ateneo, che aveva installato delle telecamere di videosorveglianza, a fini di tutela del proprio patrimonio e per ragioni di sicurezza, nei corridoi di un edificio o, in assenza di un previo accordo sindacale o di autorizzazione dell'Ispettorato nazionale del lavoro. Inoltre, per un considerevole arco temporale, non era stata resa agli interessati un'informativa completa sul trattamento dei dati effettuato mediante il predetto sistema di videosorveglianza ed erano stati affissi cartelli informativi carenti di taluni degli elementi richiesti dalla normativa in materia di protezione dei dati. Per tali motivi, è stata accertata la violazione degli artt. 5, par. 1, lett. *a*), 6, 13 e 88 del RGPD, nonché dell'art. 114 del Codice, in relazione all'art. 4, comma 1, l. n. 300/1970, comminando anche una sanzione pecuniaria (provv. 11 marzo 2021, n. 90, doc. web n. 9582791).

14.8. *Sistema di rilevazione delle presenze mediante trattamento di dati biometrici dei dipendenti*

Sempre con riguardo al contesto lavorativo, a seguito di notizie di stampa, l'Autorità ha avviato d'ufficio un'istruttoria nei confronti di un'azienda sanitaria, che aveva installato nelle proprie sedi un sistema che consentiva il trattamento dei dati biometrici dei dipendenti per la rilevazione delle presenze, soprattutto al fine di scoraggiare fenomeni di assenteismo. Nel provvedimento prescrittivo e sanzionatorio adottato all'esito dell'istruttoria, il Garante ha, anzitutto, chiarito che, ancorché l'azienda non conservasse i dati biometrici su una banca dati centralizzata, ma solo su dispositivi portatili dotati di adeguate capacità crittografiche (*badge* con funzionalità di *smart card*), affidati alla diretta ed esclusiva disponibilità di ciascun interessato, si concretizzava comunque un trattamento di dati biometrici, i quali transitavano, anche se per pochi istanti, nei sistemi impiegati dal datore di lavoro (ciò sia nella fase di registrazione, cd. *enrollment,* con l'acquisizione delle caratteristiche biometriche, ovvero le impronte digitali, dell'interessato, sia nella fase di riconoscimento biometrico, all'atto delle rilevazioni delle presenze).

Per quanto concerne i presupposti di liceità del trattamento, il Garante ha precisato che l'art. 2 della l. 19 giugno 2019, n. 56 (rispetto al quale il Garante ha in passato reso il proprio parere sia sullo schema di disegno di legge sia sul successivo schema di regolamento, cfr. provv.ti 11 ottobre 2018, n. 464, doc. web n. 9051774 e 19 settembre 2019, n. 167, doc. web n. 9147290) era rimasto comunque inattuato e, da ultimo, abrogato per effetto dell'art. 1, comma 958, l. 30 dicembre 2020, n. 178. Il Garante ha quindi chiarito che non si rinviene nell'ordinamento un'idonea base giuridica che possa soddisfare i requisiti richiesti dal RGPD e dal Codice per legittimare le amministrazioni pubbliche a porre in essere il trattamento dei dati biometrici per finalità di rilevazione delle presenze dei dipendenti ai sensi dell'art. 9, par. 2, lett. *b*), del RGPD.

14

Per quanto concerne il rispetto degli obblighi di trasparenza nei confronti degli interessati, l'Autorità ha rilevato che il titolare del trattamento non aveva rappresentato compiutamente il trattamento effettuato, prospettandolo, peraltro, come conforme al quadro normativo in materia di protezione dei dati, in maniera difforme dal principio di liceità, correttezza e trasparenza (art. 5, par. 1, lett. *a*), del RGPD).

Sulla base delle considerazioni che precedono, il Garante, oltre a comminare una sanzione pecuniaria, ha ingiunto all'azienda sanitaria la cancellazione dei modelli biometrici dei dipendenti memorizzati all'interno dei *badge* in uso agli stessi (provv. 14 gennaio 2021, n. 16, doc. web n. 9542071; v. anche *Newsletter* 19 febbraio 2021, doc. web n. 9544567).

14.9. *Il trattamento di dati personali nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti (cd.* whistleblowing*)*

L'Autorità è tornata ad occuparsi del tema dei trattamenti dei dati personali nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti da parte dei dipendenti e di soggetti terzi, come previsto dalla disciplina nazionale del cd. *whistleblowing* (l. n. 179/2017 e art. 54-*bis,* d.lgs. n. 165/2001), volta a proteggere la divulgazione dell'identità del segnalante e prevenire l'adozione di misure discriminatorie nei confronti dello stesso.

In tale quadro, nell'ambito di un ciclo di attività ispettive, avente a oggetto le principali funzionalità di alcuni tra gli applicativi per l'acquisizione e gestione delle segnalazioni di illeciti più diffusamente impiegati dai datori di lavoro pubblici e privati, sono stati effettuati specifici accertamenti nei confronti di una società di gestione di un aeroporto e dell'azienda fornitrice dell'applicativo utilizzato per l'acquisizione e gestione delle segnalazioni di illeciti dei dipendenti.

Il Garante ha rilevato che la società di gestione dell'aeroporto, titolare del trattamento, in difformità agli artt. 5, par. 1, lett. *f*), 25 e 32 del RGPD, non aveva utilizzato tecniche crittografiche per il trasporto e la conservazione dei dati, tenuto conto che l'accesso all'applicativo avveniva mediante il protocollo HTTP (*Hyper Text Transfer Protocol*), ossia un protocollo di rete che, anche in ragione della natura dei dati e degli elevati rischi derivanti dalla loro possibile acquisizione da parte di terzi, non garantiva l'integrità e la riservatezza dei dati scambiati tra il *browser* dell'utente e il *server* che ospitava l'applicativo.

Nel corso dell'istruttoria è, altresì, emerso che l'accesso all'applicativo da parte dei dipendenti della società con postazioni di lavoro o dispositivi personali connessi alla rete aziendale era mediato da apparati di *firewall* che memorizzavano per novanta giorni le operazioni di navigazione effettuate, ivi comprese le connessioni all'applicativo, includendo anche l'indirizzo Ip e il nome utente del soggetto che effettuava la connessione. Tale configurazione avrebbe potuto consentire la tracciabilità dei soggetti che utilizzavano l'applicativo, ivi inclusi i segnalanti, in maniera non conforme anche ai principi di "protezione dei dati fin dalla progettazione e per impostazione predefinita" (art. 25 del RGPD). Al riguardo, il Garante ha ricordato che il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve verificare, anche avvalendosi del supporto del responsabile della protezione dei dati ove nominato, la conformità del trattamento ai principi applicabili al trattamento dei dati, adottando, nel rispetto del principio di responsabilizzazione, le opportune misure tecniche e organizzative e impartendo le necessarie istruzioni al fornitore del servizio (cfr. artt. 5, par. 2; 24, 25 e 32 del RGPD). In tale prospettiva, il titolare del trattamento deve eseguire una valutazione

dei rischi e accertarsi che siano disattivate le funzioni che non hanno una base giuridica e non sono compatibili con le finalità del trattamento, ovvero si pongono in contrasto con specifiche norme di settore previste dall'ordinamento, in particolare quelle a tutela dei diritti degli interessati nel contesto lavorativo.

Inoltre, nonostante la particolare delicatezza delle informazioni trattate, gli elevati rischi, in termini di possibili effetti ritorsivi e discriminatori, anche indiretti, per il segnalante, la cui identità è protetta da uno specifico regime di garanzia e riservatezza previsto dalla normativa di settore, nonché la "vulnerabilità" degli interessati (soggetti segnalanti e segnalati) nel contesto lavorativo (cfr. artt. 35 e 88, par. 2, del RGPD), la società non aveva condotto una valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento (art. 35 del RGPD).

Per effetto delle condotte sopra descritte, il Garante ha comminato alla società di gestione aeroportuale una sanzione pecuniaria (provv. 10 giugno 2021, n. 235, doc. web n. 9685922).

Con riguardo, invece, al fornitore dell'applicativo, il Garante, con separato provvedimento, ha rilevato che lo stesso aveva fatto ricorso a sub-responsabili del trattamento senza aver previamente informato il titolare ed aver concesso allo stesso la possibilità di opporsi, omettendo anche di stipulare accordi per la protezione dei dati con i sub-responsabili, in violazione dell'art. 28, parr. 2 e 4, del RGPD.

Nel corso dell'istruttoria è poi stato accertato che, ancorché autorizzati al trattamento, due soggetti operanti sotto l'autorità del fornitore e di un sub-responsabile utilizzavano un'unica utenza non nominale, con profilo di amministratore di sistema, per l'accesso all'applicativo, in maniera non adeguata sotto il profilo della sicurezza. È, altresì, emerso che l'interfaccia di gestione amministrativa dell'applicativo era accessibile da rete pubblica, con una procedura di autenticazione informatica debole (a un solo fattore) e senza alcun meccanismo di blocco automatico della predetta utenza condivisa in caso di ripetuti tentativi di autenticazione (v. artt. 32 e 83, par. 4, del RGPD). Le modalità di accesso all'applicativo, con le caratteristiche sopra descritte, non sono state ritenute conformi all'art. 32 del RGPD.

In considerazione delle condotte sopra illustrate, il Garante ha comminato anche al fornitore dell'applicativo una sanzione pecuniaria e ha ingiunto allo stesso di adottare talune misure correttive (provv. 10 giugno 2021, n. 236, doc. web n. 9685947; cfr. *Newsletter* 2 agosto 2021, doc. web n. 9687860).

14.10. *Il trattamento di dati personali per finalità di gestione del rapporto di lavoro*

Anche con riguardo alla gestione del rapporto di lavoro, il Garante, sulla base di istruttorie avviate a seguito di reclami presentati da dipendenti pubblici o di 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 posti in essere in violazione della disciplina in materia di protezione dei dati.

14.10.1. Pubblicazione di documenti in bacheche e in aree ad accesso riservato di siti web

In uno dei casi esaminati, un dipendente di un'azienda concessionaria del servizio di trasporto pubblico locale aveva lamentato l'affissione, su una bacheca aziendale, di documentazione relativa a un provvedimento disciplinare, con il quale era stata disposta la sospensione dal servizio. Il Garante, sul presupposto che i dati personali dei dipendenti non possono essere messi a conoscenza di soggetti che non sono parte

del rapporto di lavoro, né comunque autorizzati ad accedervi (cfr. artt. 4, par. 10, 29, 32, par. 4, del RGPD), ha ritenuto che la pubblicazione fosse avvenuta in assenza di un'idonea base giuridica, avendo avuto luogo una "comunicazione" illecita di dati personali a "terzi" non autorizzati (cfr. art. 4, par.1, n. 10), del RGPD, nonché art. 2-*ter,* comma 4, lett. *a*), del Codice). L'azienda, avrebbe, invece, potuto, nel rispetto della disciplina di protezione dei dati e in modo parimenti efficace, affiggere in aree disponibili agli addetti al servizio il solo documento riepilogativo dei turni giornalieri (provv. 27 maggio 2021, n. 214, doc. web n. 9689234).

In un altro caso, è stata censurata la messa a disposizione in un'area del sito web di un istituto scolastico, ad accesso riservato, di un documento organizzativo denominato "piano annuale del personale Ata", in cui erano contenuti dati personali identificativi della reclamante, anche relativi alla salute (ovvero riferimenti alla circostanza che, in ragione di una terapia farmacologica effettuata dall'interessata, era stata richiesta una variazione dell'orario di servizio). Tale documento, era consultabile non solo dal personale di segreteria, ma anche da tutti i colleghi della reclamante appartenenti al personale Ata, dando luogo a una comunicazione illecita di dati personali a terzi, in assenza di un'idonea base giuridica. Il Garante ha, peraltro, ritenuto irrilevante la circostanza che i colleghi della reclamante fossero stati informati dalla stessa in merito alle vicende oggetto di pubblicazione da parte dell'istituto (provv. 16 settembre 2021, n. 322, doc. web n. 9711517).

Va menzionato, infine, il caso della pubblicazione, nella rete intranet di un'azienda ospedaliera, accessibile a tutti i dipendenti tramite *username* e *password,* di dati e informazioni personali contenuti nella graduatoria finale relativa all'attribuzione delle progressioni economiche orizzontali-area comparto riferiti a circa 750 dipendenti, nonché nelle relative schede di valutazione, le quali contenevano, oltre i dati identificativi, anche le informazioni relative all'anzianità di servizio, con relativa qualifica, e le esperienze professionali (titoli di studio, attività di docenza, corsi seguiti) con indicazione dei singoli punteggi. Anche in tale evenienza l'azienda è stata sanzionata per aver effettuato una comunicazione illecita di dati personali priva di un'idonea base giuridica (provv. 14 gennaio 2021, n. 22, doc. web n. 9543138, cit.).

14.10.2. Circolazione di informazioni personali nei contesti lavorativi, anche nei sistemi di protocollazione informatica degli atti

Il Garante si è, inoltre, pronunciato su un reclamo, con il quale un dipendente di un comune aveva lamentato la circostanza che il proprio superiore avesse inviato via *e-mail* a tutti i suoi colleghi una nota del comitato unico di garanzia per le pari opportunità concernente la valorizzazione del benessere di chi lavora e contro le discriminazioni recante, in allegato, una lettera anonima, con la quale colleghi non identificati del reclamante avevano espresso giudizi negativi circa il suo comportamento in ambito lavorativo.

All'*e-mail* in questione era, altresì, allegato un questionario, con il quale veniva chiesto ai destinatari se condividessero, o meno, i giudizi riportati in tale lettera anonima. Nel caso di specie, i colleghi del reclamante, destinatari della predetta *e-mail,* erano venuti a conoscenza dei dati personali dell'interessato, pur non potendo essere considerati persone autorizzate a conoscere tali dati in ragione del proprio specifico incarico. Ciò ha, pertanto, comportato una comunicazione di dati personali dal comune a terzi in assenza di un'idonea base giuridica. Il Garante ha, altresì, ritenuto che, nel rispetto del principio di minimizzazione dei dati (art. 5, par. 1, lett. *c*), del RGPD), la comunicazione dei dati del reclamante ai propri colleghi non fosse, in ogni caso, necessaria per il perseguimento delle finalità prospettate dal comune (provv. 14 gennaio 2021, n. 23, doc. web n. 9543161).

Sempre con riguardo alla circolazione di informazioni nel contesto lavorativo, a seguito di un reclamo presentato da un militare con riguardo alle modalità di protocollazione di documentazione contente propri dati personali, anche relativi alla salute, il Garante ha prescritto al titolare di conformare il sistema di protocollazione informatica, al tempo in uso, ai principi di protezione dei dati personali. Nel caso di specie, una nota contenente dati personali del reclamante era stata gestita nel protocollo informatico con visibilità a tutti i militari del comando stazione di appartenenza, a cui era stato attribuito indistintamente il ruolo di protocollista. Tale nota, menzionando un acronimo riconducibile ai procedimenti relativi alle cause di servizio e alla liquidazione dell'equo indennizzo, che presuppongono inevitabilmente uno stato patologico del dipendente, indipendentemente dagli esiti dei procedimenti, rendeva desumibili informazioni anche relative allo stato di salute dell'interessato. Il Garante ha accertato, quindi, che i dati del reclamante erano stati messi a disposizione di personale che non poteva considerarsi autorizzato al trattamento, comminando la conseguente sanzione amministrativa (provv. 11 febbraio 2021, n. 50, doc. web n. 9562866).

14.10.3. Il trattamento dei dati relativi alla salute del personale militare: il sistema del cd. doppio certificato

Il Ministro dell'economia e delle finanze ha chiesto al Garante un parere, ai sensi dell'art. 36, par. 4, del RGPD, con riguardo allo schema di decreto ministeriale predisposto ai sensi dell'art. 748, comma 2, d.P.R. 15 marzo 2010, n. 90, relativo al sistema del doppio certificato per il personale appartenente al Corpo della Guardia di finanza, utilizzato per finalità di gestione delle assenze per motivi di salute del personale militare. L'Autorità, anche all'esito delle interlocuzioni intercorse con il Ministero, nell'esprimere il proprio parere favorevole, ha evidenziato come lo schema di decreto in questione, recependo le indicazioni fornite nel tempo dal Garante con riguardo al trattamento dei dati personali sia, in generale, nel contesto lavorativo sia con specifico riguardo al personale militare (cfr. provv. 8 ottobre 2015, n. 521, doc. web n. 4487512), individuasse correttamente le necessarie garanzie, anche ai sensi dell'art. 2-*septies* del Codice, per le distinte finalità riconducibili alla gestione delle assenze per malattia (artt. 9, par. 2, lett. *b*) e 88 del RGPD), alla "medicina del lavoro" e alla "valutazione della capacità lavorativa del dipendente" (art. 9, parr. 2, lett. *h*) e 3, del RGPD). Ciò assicurando, in particolare, che i dati personali relativi alla salute contenuti nel certificato recante anche la diagnosi fossero accessibili ai soli organi sanitari competenti per la verifica della persistenza dell'idoneità psico-fisica del militare e che essi non siano in alcun modo trascritti nei documenti caratteristici o matricolari ovvero nel fascicolo personale del militare (provv. 27 gennaio 2021, n. 25, doc. web n. 9549211).

14.11. *Diffusione* online *di dati personali 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 che contengono dati personali di lavoratori (cfr. par. 4.4).

Con riguardo a tali fattispecie, il Garante, dichiarando l'illiceità del trattamento, in ragione dell'assenza di un'idonea base giuridica che potesse giustificare la diffusione dei dati personali di lavoratori, ha definito i seguenti numerosi reclami, concernenti la pubblicazione sul sito web istituzionale di:

14

- un comune, di una deliberazione della giunta comunale e di due determinazioni, riportanti dati personali di un dipendente, incluse informazioni relative a specifiche vicende connesse al rapporto di lavoro con particolare riguardo a un procedimento disciplinare e al contenzioso con l'amministrazione) (provv. 27 gennaio 2021, n. 34, doc. web n. 9549165);
- un comune, di una delibera di giunta e diverse determinazioni dirigenziali in cui erano riportati dati e informazioni riferiti ad agenti di polizia municipale (fra cui nome e cognome, indicazione della sede di lavoro e tipo di mansioni svolte) (provv. 25 marzo 2021, n. 108, doc. web n. 9670709);
- un'azienda socio-sanitaria territoriale, di un *curriculum vitae* di un candidato a ricoprire il ruolo di medico specialista, omettendo di oscurare preventivamente i dati afferenti alla sfera personale dello stesso (quali l'indirizzo di residenza, l'utenza cellulare privata, l'*e-mail* personale e la firma autografa), che non potevano ritenersi "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. *c*), del RGPD (provv. 29 aprile 2021, n. 171, doc. web n. 9682169);
- di un istituto professionale, di alcuni documenti contenenti dati personali del reclamante e dei suoi familiari, tra cui anche informazioni relative allo stato di salute (provv. 24 giugno 2021, n. 255, doc. web n. 9688099);
- un comune, di una deliberazione della giunta comunale, contenente dati personali e valutazioni sull'operato di un dipendente (provv. 24 giugno 2021, n. 256, doc. web n. 9689607);
- di un comune, di una determinazione dirigenziale, avente a oggetto la risoluzione del rapporto di lavoro e l'acquisizione del diritto alla pensione di inabilità, in cui erano riportati in chiaro dati personali di un dipendente inabile al lavoro e informazioni inerenti all'attività lavorativa e all'effettuazione della visita medica in violazione del divieto di diffusione di dati sulla salute (provv. 8 luglio 2021, n. 301, doc. web n. 9703112);
- un'accademia di belle arti, di un verbale del consiglio di amministrazione, contenente dati personali relativi al reclamante, inclusi riferimenti a un procedimento disciplinare avviato nei confronti dello stesso e ai contenuti di note inviate all'accademia dal reclamante per il tramite del suo avvocato (provv. 16 settembre 2021, n. 318, doc. web n. 9718134);
- un consorzio di bonifica, di una delibera, contenente dati personali di un lavoratore, relativi a un provvedimento disciplinare adottato nei propri confronti, nonché al suo stato di salute (provv. 16 settembre 2021, n. 319, doc. web n. 9704048);
- un'azienda sanitaria provinciale, di una deliberazione del commissario straordinario e della nota allegata, riguardanti le dimissioni dall'incarico di medicina generale del reclamante, con ulteriori riferimenti particolareggiati ai relativi problemi di salute e al rapporto di lavoro con l'azienda sanitaria, in violazione del divieto di diffusione di dati sulla salute (provv. 16 settembre 2021, n. 326, doc. web n. 9718175);
- un comune, di una determinazione relativa alla presa d'atto e accettazione delle dimissioni di un dipendente contenente informazioni personali relative al rapporto di lavoro (ivi comprese valutazioni sull'operato del reclamante e sul suo stato di salute) (provv. 25 febbraio 2021, n. 68, doc. web n. 9567429);
- un comune, relativa alla presa d'atto e accettazione delle dimissioni di un dipendente contenente informazioni personali relative al rapporto di lavoro (ivi comprese valutazioni sull'operato del reclamante e sul suo stato di salute (provv. 25 febbraio 2021, n. 69, doc. web n. 9565258);

- un convitto nazionale statale, di uno schema di contratto integrativo, contenente affermazioni in merito alla circostanza che il reclamante non avesse adempiuto ai propri doveri d'ufficio, pur essendo presente in servizio (provv. 25 marzo 2021, n. 105, doc. web n. 9565258);
- un ateneo, di un *curriculum vitae* di un docente, inviato ai meri fini di una procedura di selezione avviata dall'ateneo per l'assegnazione di un incarico di docente a contratto, diffondendo dati personali dello stesso (quali la residenza, il numero di telefono, l'indirizzo di posta elettronica, l'indirizzo di Pec e lo stato civile) ritenuti non "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. *c*), del RGPD) (provv. 16 dicembre 2021, n. 448, doc. web n. 9742923;
- un comune, di atti e documenti contenenti informazioni riguardanti il reclamante (con riguardo all'utilizzo da parte del medesimo comune di dispositivi video indossabili, cd. *body cam,* nel corso di una seduta consiliare, senza aver reso ai soggetti ripresi un'informativa sul trattamento dei dati personali, si rinvia al par. 4.5. relativo agli enti locali) (provv. 11 novembre 2021, n. 399, doc. web n. 9725891);
- un ufficio scolastico regionale - ambito territoriale, di una nota contenente informazioni personali anche relative alle esperienze professionali del reclamante, in assenza di un'idonea base giuridica (provv. 29 aprile 2021, n. 172, doc. web n. 9686899).

14.11.1. Pubblicazione di graduatorie e atti di procedure concorsuali

Alcuni reclami hanno riguardato la diffusione *online* di dati personali in relazione alla pubblicazione di graduatorie e atti di procedure concorsuali, su cui tradizionalmente il Garante ha fornito specifiche indicazioni alle p.a. 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, cit., 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).

L'Autorità ha, in particolare, censurato, adottando i conseguenti provvedimenti sanzionatori, il comportamento di tre istituti scolastici che avevano pubblicato sul proprio sito web istituzionale, e indicizzato sui motori di ricerca, graduatorie relative al personale docente e amministrativo, tecnico e ausiliario, contenenti informazioni eccedenti quali i recapiti e il codice fiscale degli interessati, nonché, in alcuni casi, tra i titoli di preferenza del personale scolastico, anche informazioni relative alle condizioni di salute. In proposito, è stato, infatti, ritenuto che l'associazione della lettera "S" (che, in base alla disciplina di settore, individua la categoria degli invalidi e mutilati civili; cfr. all. 6 al decreto del Ministero dell'istruzione università e ricerca 1° aprile 2014, n. 235) a taluni nominativi comportasse la diffusione di dati personali relativi alla salute, in violazione degli artt. 6 e 9 del RGPD e degli artt. 2-*ter* e 2-*septies,* comma 8, del Codice nonché dei principi di liceità e minimizzazione del trattamento (art. 5 del RGPD) (provv.ti 27 gennaio 2021, n. 28, doc. web n. 9576756; 11 febbraio 2021, n. 51, doc. web n. 9572226; 11 febbraio 2021, n. 60, doc. web n. 9574101).

A fronte della pubblicazione da parte di un ufficio scolastico regionale sul proprio sito web istituzionale di graduatorie relative al personale docente, contenenti, in particolare, la menzione del codice fiscale degli interessati, il Garante ha rilevato che la pubblicazione era stata effettuata in violazione dei principi di liceità, correttezza

14

e trasparenza e di minimizzazione dei dati, di cui all'art. 5, par. 1, lett. *a*) e *c*), del RGPD. Il Garante, oltre ad aver comminato una sanzione amministrativa, ha disposto la limitazione dei trattamenti in corso, vietando ogni ulteriore operazione di trattamento con riguardo ai dati personali dei docenti inseriti nelle graduatorie (provv. 21 aprile 2021, n. 153, doc. web n. 9685245).

In un altro caso, è stata comminata una sanzione amministrativa nei confronti di un istituto scolastico che aveva pubblicato, nella sezione "avvisi" del proprio sito web istituzionale, un *link,* accessibile a tutti, alle graduatorie provvisorie dei docenti perdenti posto, contenenti anche dati idonei a rivelare lo stato di salute degli stessi. Accanto al nominativo di alcuni docenti erano stati, infatti, apposti due asterischi con la specificazione "beneficiario della legge 104/92" (provv. 16 settembre 2021, n. 321, doc. web n. 9718196).

Il Garante ha, inoltre, censurato il comportamento di una regione, che aveva pubblicato *online* le griglie degli ammessi con riserva e le convocazioni per la preselezione ad alcune procedure concorsuali di numerosi candidati. Al riguardo, è stato ribadito che la normativa di settore, riguardante la pubblicità delle graduatorie, prevede che siano pubblicate le sole graduatorie definitive dei vincitori di concorso e non anche gli avvisi di convocazione dei candidati contenenti dati personali identificativi, come, nel caso di specie, il nome, il cognome, il giorno, l'ora e il luogo della convocazione dei partecipanti alla procedura (provv. 29 aprile 2021, n. 170, doc. web n. 9681778).

Il Garante ha poi affrontato il caso di un'azienda ospedaliera, che aveva pubblicato nella sezione Amministrazione trasparente del proprio sito web istituzionale numerosi atti e documenti contenenti dati personali (recapiti personali, codice fiscale, codice di partecipazione al concorso, numero di telefono, indirizzo di residenza, indirizzo Pec personale), anche relativi a categorie particolari, dei partecipanti a una procedura concorsuale. A tal riguardo, l'Autorità, ha ribadito che, in base al d.lgs. 14 marzo 2013, n. 33, le p.a. possono pubblicare le sole graduatorie finali di una procedura concorsuale e che le disposizioni concernenti la pubblicità degli esiti delle prove concorsuali e delle graduatorie di concorsi dispongono che siano pubblicate le sole graduatorie definitive dei vincitori di concorso e non anche, ad esempio, gli esiti delle prove intermedie o dei dati personali dei concorrenti non vincitori. Per tali ragioni, considerato anche il numero degli interessati coinvolti, nonché la natura dei dati oggetto di pubblicazione, è stata comminata una sanzione amministrativa (provv. 25 novembre 2021, n. 407, doc. web n. 9732406).

In un altro caso, l'Autorità è intervenuta nei confronti di una società partecipata di un comune, che aveva pubblicato sul proprio sito web istituzionale, e indicizzato sui motori di ricerca, la documentazione riguardante una selezione pubblica, contenente gli esiti delle valutazioni relative al reclamante e agli altri candidati, con riferimenti anche al titolo di studio e al giudizio in merito ai requisiti professionali (provv. 11 marzo 2021, n. 89, doc. web n. 9581028).

L'Autorità, a seguito di un reclamo, ha, altresì, sanzionato un comune, che aveva pubblicato su una pagina del proprio sito web istituzionale, indicizzata anche sui motori di ricerca, una determinazione contenente dati personali della reclamante e di altri partecipanti a una procedura di mobilità, tra cui la residenza anagrafica. L'Autorità ha altresì evidenziato che l'istituto dell'accesso civico è autonomo e indipendente dagli obblighi di pubblicazione, che rimangono, invece, circoscritti esclusivamente a quelli indicati dalla legge (provv. 25 marzo 2021, n. 106, doc. web n. 9584421).

15 Le attività economiche

15.1. *Il trattamento dei dati personali in ambito assicurativo*

In linea con gli andamenti registrati negli ultimi anni, anche il 2021 ha visto un significativo afflusso di istanze relative al settore assicurativo, perlopiù relative a tematiche già esaminate e definite in passato dal Garante (v. Relazione 2020, p. 179) rilevando l'incompetenza dell'Autorità a pronunciarsi sulle richieste volte a ottenere, come nei casi esaminati, l'accesso o la copia di atti o documenti detenuti dai titolari.

Sul fronte grandi banche dati sono proseguiti gli approfondimenti, anche d'intesa con Ivass e Agcm, sul progetto presentato da Ania – e di cui si è dato conto già nella Relazione 2020 – relativamente a un archivio antifrode nei segmenti di rischio diversi dalla responsabilità civile autoveicoli.

15.2. *Settore bancario-finanziario e sistemi di informazioni creditizie*

Anche nel 2021 sono stati numerosi i casi riguardanti il trattamento di dati personali effettuato da istituti di credito, società finanziarie, sistemi di informazione creditizia gestiti da soggetti privati, centrale dei rischi pubblica gestita da Banca d'Italia, Centrale di allarme interbancaria, anche su profili già approfonditi in passato dal Garante mediante l'adozione di provvedimenti collegiali (in specie, le linee guida adottate il 25 ottobre 2007: provv. 25 ottobre 2007, n. 53, doc. web n. 1457247), i cui princìpi sono stati ritenuti compatibili con il quadro regolatorio risultante dal RGPD e dal Codice novellato a seguito dell'entrata in vigore del d.lgs. n. 101/2018 (v. Relazione 2020, p. 181).

La differenza tra accesso ai dati e accesso ai documenti in ambito bancario

Con provvedimento 25 novembre 2021, n. 408 (doc. web n. 9731887) l'Autorità ha disposto la misura dell'ammonimento nei confronti di un importante gruppo bancario per la violazione degli artt. 12 e seguenti del RGPD in relazione al mancato tempestivo riscontro alla richiesta di accesso ai dati personali che era stata formulata da un cliente. Nel caso di specie l'istituto di credito aveva comunicato all'interessato i dati richiesti solo a seguito della presentazione del reclamo all'Autorità (seppure in una data antecedente all'avvio, da parte della stessa, del relativo procedimento), limitandosi peraltro, nella comunicazione medesima, a rappresentare che il ritardo era stato determinato da un disguido, senza fornire al riguardo ulteriori elementi di precisazione.

Considerato che nel corso del procedimento la banca aveva illustrato le circostanze dell'errore materiale che aveva determinato il ritardo e che si era prontamente attivata, da un lato, fornendo all'interessato le informazioni richieste e, dall'altro, prevedendo misure organizzative e formative nell'ambito della procedura interna per la gestione delle istanze relative all'esercizio dei diritti ex artt. 15-22 del RGPD, l'Autorità ha qualificato la fattispecie come violazione minore (cfr. art. 83, par. 2 e cons. 148 del RGPD) adottando nei confronti dell'istituto di credito la misura dell'ammonimento ai sensi dell'art. 58, par. 2, lett. *b*), del RGPD medesimo.

In linea con il consolidato orientamento dell'Autorità in materia, è stato ribadito che l'accesso ai dati personali è diverso dall'accesso ai documenti bancari disciplinato

15

dall'art. 119, d.lgs. 1° settembre 1993, n. 385 (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, né possono riguardare dati di terzi.

In un caso, nel quale l'interessata aveva paventato l'incompletezza di un riscontro ricevuto da un primario istituto di credito a un'istanza di esercizio del diritto di accesso ai propri dati personali – riferita, in particolare, a contratti della cui esistenza l'interessata aveva dichiarato di avere acquisito conoscenza solo in sede di produzione, nelle competenti sedi, della documentazione prescritta per ottenere l'attestazione Isee – e proposto reclamo al Garante, sono stati svolti approfondimenti, mirati soprattutto sul profilo dell'aggiornamento, da parte della banca, dei dati riferiti ai rapporti oggetto di reclamo nell'archivio dei rapporti finanziari istituito presso l'Agenzia delle entrate.

Le risultanze istruttorie hanno evidenziato non solo che i contestati rapporti di conto corrente erano stati correttamente conferiti nell'archivio, ma anche che l'istante aveva ricevuto dalla banca un riscontro all'istanza di esercizio del diritto di accesso ai dati in linea con il RGPD.

Acclarato, infatti, che, nel caso di specie, per ottenere le specifiche informazioni necessarie ai fini dichiarati, la reclamante avrebbe dovuto accedere ed eventualmente ricevere copia degli estratti conto o di altri documenti (elaborati e trasmessi ai propri clienti da ciascun istituto di credito ai sensi delle vigenti disposizioni del Tub in materia di trasparenza bancaria e comunicazioni alla clientela) contenenti le informazioni desiderate e che di tale circostanza l'interessata era stata già resa edotta dalla banca (la quale aveva altresì provveduto a trasmettere nuovamente, ai sensi dell'art. 119 del Tub e all'indirizzo noto per l'invio di comunicazioni fornito dalla reclamante, copia degli estratti conto di interesse già inviati al momento della relativa emissione), si è ritenuto di dover precisare che, in ambito bancario, tale risultato è legittimamente conseguibile ai sensi della vigente disciplina di settore (in particolare, proprio dell'art. 119, comma 4, del Tub), che consente, ai soggetti ivi legittimati e nei tempi prescritti (più dilatati rispetto a quelli accordati dal RGPD al titolare del trattamento per rispondere all'esercizio dei diritti di un interessato), di accedere a (e/o di ottenere copia di) tutta la documentazione di interesse (nel caso in esame, gli estratti conto, contenenti informazioni puntuali e analitiche, incluse quelle che la reclamante aveva mostrato interesse a ricevere nel caso di specie), senza oscuramento di dati (che, eventualmente, possono riferirsi anche a soggetti terzi).

Nel richiamare l'orientamento già espresso in precedenti pronunce, si è pertanto archiviato il reclamo ai sensi dell'art. 11 del regolamento interno n. 1/2019 (nota 16 dicembre 2021).

Antiriciclaggio e antiterrorismo: identificazione e adeguata verifica della clientela

Segnalazioni e quesiti hanno riguardato anche le operazioni di identificazione e di adeguata verifica della clientela prescritte dalla normativa vigente in materia di antiriciclaggio e antiterrorismo (esaminata diverse volte dal Garante, per i profili di propria competenza, da ultimo con il parere sul d.lgs. 4 ottobre 2019, n. 125, di attuazione alla cd. quinta direttiva – v. il provvedimento 24 luglio 2019, n. 150, doc. web n. 9126288 – v. Relazione 2019). Si è precisato ai richiedenti che, ai sensi della vigente normativa di riferimento, essi sono obbligati non solo a identificare l'interessato e effettuare le operazioni di adeguata verifica del medesimo, necessarie, caso per caso, prima di stipulare qualsiasi rapporto contrattuale o di effettuare operazioni occasionali, ma anche a effettuare il monitoraggio e il controllo continuativo dei contratti in essere. L'identificazione del cliente prevede la consegna di copia di un valido documento d'identità dell'interessato, mentre l'adeguata verifica richiede l'acquisizione

15

Sistemi di informazione creditizia

di dettagliate informazioni e di specifica documentazione (anche in merito all'attività lavorativa svolta e alla situazione economica e patrimoniale), variabile a seconda del tipo di verifica da svolgere nel caso specifico (semplificata, ordinaria o rafforzata).

Particolarmente intenso è stato il flusso di istanze in materia di trattamenti di dati personali censiti nei sistemi di informazioni creditizie gestiti da soggetti privati (cd. Sic). Alcune di queste hanno riguardato il preavviso da rendere all'interessato, al verificarsi di ritardi nel pagamento degli importi pattuiti, prima dell'inserimento dei dati nei Sic; altre i tempi di conservazione dei dati nei Sic (variabili a seconda che il rapporto censito sia stato stipulato o meno e, in caso affermativo abbia avuto un andamento regolare o irregolare). L'Ufficio ha richiamato i princìpi del RGPD e del Codice e le disposizioni del codice di condotta – strumento di autoregolamentazione ad adesione volontaria in grado di concorrere, nel settore, alla corretta applicazione della normativa in materia di protezione dei dati personali (art. 40) – invitando, qualora necessario, i partecipanti e i gestori dei Sic ad aderire spontaneamente alle richieste formulate dagli interessati. Si rileva al riguardo che il codice di condotta, approvato dal Garante il 12 settembre 2019 (n. 163, doc. web n. 9141941) non risulta ancora efficace in assenza del regolamento dell'organismo di monitoraggio, la cui adozione il Garante auspica possa avvenire nel corso del 2022.

In numerosi casi, in assenza di elementi rappresentativi di violazioni della normativa in materia di protezione dei dati personali, le istanze pervenute (basate soprattutto sull'esercizio dei diritti di rettifica o di cancellazione dei dati dai Sic) sono state dichiarate infondate.

In un caso specifico, in cui l'interessato chiedeva indicazioni per revocare il consenso al trattamento dei dati riferiti a suoi rapporti con andamento regolare dai Sic, si è fatto presente che, nel nuovo codice di condotta, il consenso dell'interessato non costituisce più la base giuridica per il trattamento dei dati riferiti a un rapporto contrattuale censito in uno o più Sic con andamento regolare (cd. dati positivi): tutti i dati personali (sia positivi che negativi) nell'ambito di un Sic sono ora trattati ai sensi dall'art. 6, comma 1, del codice di condotta, a norma del quale "[i]l trattamento dei dati personali da parte del gestore e dei partecipanti al Sic secondo i termini e le condizioni stabilite nel Codice di condotta risulta lecito ai sensi dell'art. 6 comma 1, lett. *f*), del Regolamento in quanto è necessario per il perseguimento di legittimi interessi dei partecipanti all'utilizzo del Sic per le finalità di cui al presente codice di condotta". Si è poi evidenziato che, le informative sul trattamento dei dati personali degli interessati rese dalle società che gestiscono i Sic e dai cd. partecipanti sui rispettivi siti istituzionali, ai sensi dell'art. 6 del codice di condotta, specificano espressamente tale base giuridica del trattamento (nota 9 dicembre 2021).

La Centrale di allarme interbancaria

In un caso l'interessato, segnalato da un istituto di credito nella Centrale di allarme interbancaria (cd. Cai) per utilizzo sopra soglia di una carta di credito, aveva chiesto il ripristino dell'operatività della carta e la cancellazione del proprio nominativo dalla Cai, avendo sanato, *medio tempore,* la propria posizione. Al riguardo si è dato conto che, il mutato assetto normativo – ovvero da un lato, il provvedimento di modifica del regolamento del 2002, adottato da Banca d'Italia il 25 marzo 2021 (e sul quale il Garante, nell'esercizio delle sue funzioni consultive, si era già pronunciato con parere 10 giugno 2020, n. 97, doc. web n. 9433428) e dall'altro il decreto di modifica del d.m. n. 458/2001 varato dal Ministero della giustizia il 12 gennaio 2021, n. 33 (sul cui schema il Garante ha reso il previsto parere con provv. 1° ottobre 2020, n. 178, doc. web n. 9483571) – consente a coloro che procedono al pagamento degli importi dovuti successivamente alla segnalazione, di ottenere la menzione dell'avvenuto adempimento nella Cai, ferma restando la permanenza del nominativo di tali soggetti nell'archivio per due anni (nota 25 maggio 2021).

Furto d'identità in ambito bancario e finanziario

Molteplici sono state le segnalazioni di casi di cd. furto d'identità con metodi sempre più sofisticati sul piano tecnologico, utilizzati per appropriarsi di informazioni personali riservate al fine di compiere operazioni fraudolente e illeciti penalmente rilevanti. Al riguardo è stata richiamata l'attenzione degli interessati su una scheda informativa, da tempo disponibile sul sito del Garante, volta a sensibilizzare l'utenza affinché adotti accorgimenti e cautele per evitare di incorrere in comportamenti illeciti (v. doc. web n. 5779914). Preso atto delle denunce sporte dagli interessati nelle competenti sedi giudiziarie per l'accertamento delle fattispecie di reato rinvenibili nei fatti segnalati, l'Ufficio si è anche riservato – in considerazione di quanto stabilito dagli artt. 140-*bis* (in ordine all'alternatività tra la tutela amministrativa e quella giurisdizionale) e 167, comma 4, del Codice (in base al quale, spetta al pubblico ministero, quando ha notizia dei reati dal cui accertamento può dipendere l'adozione di un provvedimento di competenza del Garante, informarne l'Autorità senza ritardo) – di assumere eventuali determinazioni all'esito e sulla base delle risultanze degli accertamenti già attivati nelle sedi appropriate.

I ruoli di alcuni soggetti operanti in ambito bancario

È stato definito il tema della qualifica di titolare o responsabile del trattamento da attribuire ai soggetti (banche, società di gestione del risparmio, ecc.) che erogano a terzi specifici servizi su base contrattuale (servizi di tesoreria, servizi di regolamento, custodia e amministrazione di strumenti finanziari, ecc.).

La questione, originariamente sottoposta con richieste di parere formulate da alcuni istituti di credito, è stata, successivamente, estesa all'intero settore bancario, mediante un'indagine conoscitiva curata, su richiesta dell'Autorità, dall'Associazione bancaria italiana (Abi) per verificare il numero degli istituti di credito o di gruppi bancari che avessero difficoltà a definire i ruoli da attribuire ai soggetti in questione nonché le tipologie di rapporti contrattuali in relazione alle quali fossero sorte eventuali difficoltà interpretative. Sono emerse criticità solo rispetto al ruolo da attribuire alle banche affidatarie del cd. servizio di tesoreria di enti locali.

In una comunicazione indirizzata ad Abi si è pertanto confermato che designare le banche affidatarie dei servizi di tesoreria da parte di enti locali come responsabili del trattamento è corretto e risponde alle disposizioni di cui al RGPD, non rinvenendosi specifici indici normativi volti a riconoscere, in capo alle banche, autonomi poteri decisionali. Ciò, peraltro, non impedirebbe, in ogni caso, alle banche di godere di margini di discrezionalità tecnico-operativa e organizzativa – riconosciuti, indirettamente, anche dall'art. 28 del RGPD – sufficienti per la migliore erogazione del servizio (nota 13 aprile 2021).

Settore bancario-finanziario e tracciamento delle operazioni

Anche la comunicazione di dati bancari a soggetti terzi non autorizzati ha continuato ad essere oggetto di numerose segnalazioni e reclami da parte di cittadini ormai consapevoli che l'Autorità, con il provvedimento sul cd. tracciamento degli accessi (provv. 12 maggio 2011, n. 192, doc. web n. 1813953) ha prescritto l'adozione, da parte degli istituti di credito, di misure necessarie adeguate a prevenire il rischio che il personale dipendente effettui accessi ai dati bancari dei clienti non giustificati da esigenze operative.

Mentre in numerose fattispecie sottoposte all'attenzione dell'Autorità, le verifiche effettuate sul tracciamento degli accessi e sui sistemi di *alert* implementati dagli istituti di credito hanno consentito di verificare la legittimità delle operazioni e, di conseguenza, del trattamento effettuato, in qualche caso sono stati adottati provvedimenti correttivi e/o sanzionatori nei confronti degli istituti medesimi.

Con provvedimento 27 maggio 2021, n. 270 (doc. web n. 9718112), l'Autorità ha dichiarato l'illiceità del trattamento di dati personali posto in essere da una dipendente di una banca – ex coniuge del reclamante – che avvalendosi delle abilitazioni informatiche attribuitele per lo svolgimento delle sue mansioni e in assenza di

esigenze operative specifiche, aveva consultato rapporti intestati al reclamante senza il consenso di quest'ultimo o altro legittimo presupposto, in violazione dei princìpi generali in materia di protezione dei dati di cui agli artt. 5, par. 1, lett. *a*) e *f*) e 6 del RGPD.

In particolare, a conclusione di un'articolata istruttoria, che ha comportato l'esame tecnico della documentazione acquisita, si è ritenuto che la violazione accertata fosse imputabile alla mancata adozione di specifici *alert* volti a rilevare intrusioni o accessi anomali e abusivi ai sistemi informativi dell'istituto bancario (in difformità da quanto già affermato dal Garante nel citato provv. 12 maggio 2011, n. 192, ai sensi dell'art. 154, comma 1, lett. *c*), del previgente Codice), misura che un titolare del trattamento è tenuto ad adottare, anche in attuazione dei principi di integrità e riservatezza di cui all'art. 5, par. 1, lett. *f*) e 32, parr. 1 e 2 del RGPD.

Sulla base delle considerazioni sopra esposte l'Autorità ha ingiunto alla banca entro 120 giorni dal provvedimento di adottare ulteriori e adeguate misure (*alert*) volte a implementare i controlli sulla legittimità e liceità degli accessi ai dati della clientela da parte di tutti i soggetti autorizzati al trattamento e a sensibilizzare gli stessi al rispetto delle istruzioni loro impartite.

Ancora, l'Autorità ha accertato che presso un ufficio di Poste italiane spa, in occasione della ricarica, su richiesta della madre dell'interessato, della carta prepagata intestata al reclamante, l'operatore aveva rilasciato alla stessa il saldo riferito alla carta ricaricata, in assenza del consenso del titolare della carta. È stata quindi riconosciuta l'illiceità del trattamento per violazione degli artt. 5, par. 1, lett. *a*) e 6 del RGPD, nonché delle specifiche misure e accorgimenti di cui ai parr. 3.1 e 3.2 del provv. del Garante 25 ottobre 2007 concernente linee guida in materia di trattamento dei dati personali della clientela in ambito bancario (doc. web n. 1457247). L'Autorità, tenendo conto in particolare delle istruzioni impartite al personale dipendente, ha altresì irrogato a Poste italiane spa una sanzione amministrativa pecuniaria (provv. 27 maggio 2021, n. 210, doc. web n. 9688307).

Il Garante ha più volte chiarito, inoltre, di non avere il potere di accertare eventuali reati, come quelli segnalati a seguito della verifica di indebiti prelievi di denaro da conti correnti e carta di credito degli interessati, i quali nella maggior parte dei casi avevano già sporto denuncia alle autorità competenti (nota 6 ottobre 2021).

Nel 2021 sono state numerose le richieste di collaborazione e supporto a iniziative promosse da realtà private e associazioni inviate al Garante, che in taluni casi ha espresso apprezzamento per i progetti e le modalità di realizzazione programmate, come nel settore delle *Alternative Dispute Resolutions* e protezione dei dati personali (nota 10 maggio 2021).

15.3. *Codici di condotta in ambito privato*

Nel corso dell'anno sono proseguite le iniziative volte ad incoraggiare l'elaborazione di codici di condotta previsti dagli artt. 40 e 41 del RGPD, strumento idoneo a fornire indicazioni e regole condivise per gestire le operazioni di trattamento dei dati, tipiche di un determinato ambito economico, sociale e associativo.

Nella prima parte dell'anno il Garante ha approvato la versione definitiva del codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali (provv. 29 aprile 2021, n. 181, doc. web n. 9586215). L'efficacia di tale codice, approvato con riserva con provv. 12 giugno 2019, n. 127 (doc. web n. 9119868), era infatti subordinata all'accreditamento dell'Organismo di monitoraggio (Odm) ai sensi dell'art. 41 del RGPD. L'*iter* di accreditamento di tale Odm si è

15

concluso con l'adozione del provv. 11 febbraio 2021, n. 59 (doc. web n. 9565426). All'Odm spetta, in particolare, il compito di verificare l'osservanza del codice di condotta da parte degli aderenti e di gestire la risoluzione dei reclami proposti dagli interessati.

Tale codice, il primo a livello nazionale approvato in ambito privato ai sensi degli artt. 40 e 41 del RGPD, fornisce agli operatori del settore un quadro di regole certe e, allo stesso tempo, maggiori garanzie agli interessati, accrescendo la loro fiducia nel rispetto di tali regole da parte degli operatori aderenti.

Percorso in qualche misura parallelo è in corso relativamente al codice di condotta riferito all'attività dei cd. sistemi di informazioni creditizie (Sic), anch'esso approvato con riserva il 12 settembre 2019 (n. 163, doc. web n. 9141941) in relazione al quale si sono svolti diversi incontri con i promotori in vista del prossimo accreditamento dell'Odm che completerà l'*iter* approvativo del codice.

Inoltre, il Garante, in ottemperanza a quanto disposto dall'art. 40 par. 6, del RGPD, secondo il quale ogni autorità di controllo competente che approva un progetto di codice di condotta deve registrare e pubblicare il codice, ha avviato i lavori per la realizzazione del registro dei codici di condotta approvati dall'Autorità a livello nazionale. Una volta realizzato, tale registro sarà pubblicato sul sito istituzionale dell'Autorità e conterrà le informazioni essenziali di ogni codice di condotta: le generalità dei promotori, la data di approvazione o eventuale modifica e proroga, nonché le informazioni sull'accreditamento dell'Odm e l'Url del sito web dell'organismo.

15.4. *Imprese*

Nel corso del 2021, come già negli anni passati, un elevato afflusso di istanze ha impegnato l'Autorità su diversi profili in materia di trattamenti di dati personali effettuati nel settore delle attività a carattere economico. In tale contesto gli interventi del Garante sono stati sia di portata generale, in quanto volti a dare piena attuazione alla normativa di cui al RGPD e al d.lgs. n. 101/2018, sia, più specifici, ovvero concernenti lo svolgimento di accurate istruttorie su temi puntuali e di varia natura.

Protocolli di intesa

In primo luogo, in materia di trattamento di dati personali relativi a condanne penali e reati, il Garante è intervenuto, su richiesta del Ministero dell'interno, al fine di consentire, nelle more dell'adozione del decreto del Ministro della giustizia di cui all'art. 2-*octies,* comma 2, del Codice, i trattamenti di dati giudiziari posti in essere da soggetti privati in attuazione dei protocolli di intesa stipulati con il Ministero dell'interno (o con le prefetture) per la prevenzione e il contrasto dei fenomeni di criminalità organizzata (art. 22, comma 12, d.lgs. n. 101/2018); ciò con particolare riferimento ai protocolli approvati precedentemente all'entrata in vigore del d.lgs. n. 101/2018 o comunque allo stato in corso di sottoscrizione (parere 22 luglio 2021, n. 284, doc. web n. 9693175). Al riguardo, l'Autorità, preso atto di quanto sostenuto dal Ministero in ordine all'efficacia dei protocolli di legalità nella lotta al contrasto alle infiltrazioni mafiose e della criminalità organizzata, ha previsto con riferimento al principio di minimizzazione, che ai soggetti privati aderenti ai predetti protocolli, in adempimento degli obiettivi perseguiti da questi ultimi, siano comunicati i risultati delle verifiche antimafia con la modalità della mera informazione relativa all'eventuale sussistenza (si/no) di cause ostative al rilascio della documentazione antimafia liberatoria e/o all'eventuale censimento (si/no) degli interessati nella banca dati nazionale unica della documentazione antimafia, senza ulteriori specificazioni. Nel rispetto del principio di trasparenza, oltre all'obbligo per i titolari di rendere agli interessati idonea informativa preventiva (artt. 13 e 14 del RGPD), di norma in

occasione della stipula dei singoli rapporti contrattuali con le parti coinvolte dalle verifiche, è stato prescritto che i protocolli di intesa siano resi conoscibili mediante adeguate forme di pubblicità (ad es. per il tramite di diffusione attraverso i siti web delle associazioni di categoria aderenti).

Sempre nell'ambito degli interventi di portata generale si è reso necessario – dopo oltre tre anni dalla piena applicazione del RGPD – fornire importanti e ulteriori chiarimenti in merito al ruolo del Rpd anche in ambito privato (cfr. par. 4.6) per fugare eventuali incertezze sulla corretta interpretazione e applicazione delle norme che disciplinano tale figura nel RGPD.

15

FAQ Rpd in ambito privato

È stata perciò pubblicata il 24 maggio 2021 sul sito istituzionale del Garante la versione aggiornata delle FAQ sull'Rpd in ambito privato (doc. web n. 8036793) già rese disponibili il 26 marzo 2018 in aggiunta a quelle adottate dal Gruppo Art. 29 in allegato al WP 243, recante le linee guida sui Responsabili della protezione dei dati del 5 aprile 2017 (cfr. Relazione 2018, p. 137 e 138).

In particolare, si è ritenuto opportuno introdurre una nuova FAQ (n. 6) sulla nomina dell'Rpd quale responsabile del trattamento, nonché apportare diverse modifiche e aggiornamenti sugli aspetti connessi, tra gli altri, all'ambito soggettivo e alle modalità di designazione di tale figura, alla compatibilità del ruolo di Rpd con altri incarichi e ai criteri di individuazione dello stesso anche in un gruppo imprenditoriale (v. le FAQ nn. 3, 4, 5, 8, 9 e 10), precisando altresì i profili relativi alla procedura telematica di comunicazione al Garante dei dati di contatto del Rpd (v. FAQ n. 7). Al fine di rendere più fruibile il testo, sono stati inoltre inseriti, a margine di ogni FAQ, i riferimenti normativi più significativi, le parole chiave e alcuni spunti in ordine ad eventuali approfondimenti.

Istruttorie in materia di esercizio dei diritti

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. In particolare, con provvedimento 14 gennaio 2021, n. 17 (doc. web n. 9542781), il Garante ha disposto la misura dell'ammonimento ai sensi dell'art. 58, par. 2, lett. *b*), del RGPD nei confronti di una società automobilistica per la violazione degli artt. 12 e ss. del RGPD in relazione al mancato tempestivo riscontro alle richieste di accesso ai dati avanzate dall'interessato. La società, infatti, aveva proceduto alla rettifica dei dati di contatto, ma, a causa di un errore materiale, non aveva adempiuto alla richiesta di accesso formulata dall'interessato. Il successivo riscontro fornito dalla società non era risultato comunque idoneo, mancando di alcune informazioni relative all'indirizzo *e-mail.*

Il Garante, ha ritenuto, in ragione delle misure già implementate dalla società, che non vi fossero i presupposti per l'applicazione delle misure correttive e ha qualificato il caso come violazione minore, ai sensi dell'art. 83 e del cons.148 del RGPD.

È stata inoltre ribadita la necessità che le istanze di cui agli artt. 15-22 del RGPD siano sempre rivolte all'effettivo titolare del trattamento. Nella specie, in relazione a un reclamo presentato nei confronti di una società aeroportuale per l'inesatto riscontro, da parte della stessa, ad una richiesta di accesso ai dati contenuti in una lista passeggeri, l'Autorità ha osservato che la predetta società è titolare unicamente dei dati dei passeggeri relativi al passaggio, ai controlli di sicurezza dello scalo ma non dispone della lista passeggeri inerente ad un volo in transito presso il medesimo aeroporto. La lista passeggeri è infatti detenuta, nei limiti e alle condizioni indicate dalla legge, dalle compagnie aeree che operano il volo.

È stata inoltre esaminata un'istanza di cancellazione ai sensi dell'art. 17 del RGPD avente ad oggetto i dati personali identificativi di un ex amministratore di una società contenuti nella nota integrativa e nella relazione sulla gestione del bilancio della stessa. Sul punto, (cfr. provv.ti 3 aprile 2003, doc. web n. 1128778 e 26 marzo

15

2009, doc. web n. 160623), si è chiarito che la disciplina in materia di tutela dei dati personali non interferisce con le disposizioni di legge relative alla documentazione e alla trasparenza dell'attività delle società, (cfr. anche CGUE 9 marzo 2017, causa C-398/15) sostanzialmente volta a garantire nei confronti dei soci e dei terzi una piena, attendibile e trasparente informativa, a tutela dello stesso mercato (nota 29 marzo 2021).

All'esito dell'istruttoria il Garante ha rilevato che il riferimento – nella nota integrativa e nella relazione sulla gestione del bilancio sopra citati – all'iniziativa volta alla convocazione dell'assemblea dei soci per deliberare sul possibile esercizio di un'azione sociale di responsabilità nei confronti del reclamante in qualità di ex amministratore, è stato posto in essere nell'osservanza dei principi di cui all'art. 5 del RGPD. Tutto ciò anche in ragione del fatto che la società, nel redigere i predetti documenti, ha fornito, attraverso un resoconto oggettivo e completo dei fatti, una mera descrizione degli accadimenti societari occorsi nell'anno di riferimento e delle relative azioni rilevanti intraprese dalla stessa al riguardo (v. Trib. di Torino, sez. IV, 12 giugno 2017). L'Autorità ha comunque precisato che resta fermo, in conformità al principio di esattezza dei dati (v. art. 5, par. 1, lett. *d*), del RGPD), l'obbligo di garantire, se del caso, non solo la corretta contestualizzazione del riferimento sopra indicato ma anche il relativo aggiornamento (cfr. Corte di cassazione 15 aprile 2012, n. 5525).

Videosorveglianza

Nel corso del 2021, l'Autorità, in continuità con gli orientamenti già consolidati negli anni precedenti, ha adottato diversi provvedimenti sanzionatori nei confronti di società che avevano effettuato trattamenti di dati personali per mezzo di impianti di videosorveglianza in violazione del principio di trasparenza e dell'obbligo di fornire agli interessati un'idonea informativa (provv.ti 13 maggio 2021, n. 191, doc. web n. 9687040; 28 ottobre 2021, n. 386, doc. web n. 9721758; 28 ottobre 2021, n. 387, doc. web n. 9721784 e 16 dicembre 2021, n. 442, doc. web n. 9765298).

In tutti i casi, gli accertamenti erano stati eseguiti dalle Forze dell'ordine, che avevano rilevato la mancanza dei cartelli recanti l'informativa e trasmesso gli atti all'Autorità a cui spetta l'esercizio dei poteri correttivi, ai sensi dell'art. 58, par. 2, del RGPD.

In un caso, in particolare, l'Autorità ha adottato un provvedimento di ammonimento nei confronti di un soggetto, titolare di un bar, il quale in relazione ad alcune telecamere installate nel proprio locale aveva predisposto informative inidonee, in quanto prive dell'indicazione del titolare e delle finalità del trattamento (provv. 27 maggio 2021, n. 245, doc. web n. 9709141). Le circostanze concrete del caso hanno indotto l'Autorità a ravvisare una violazione minore, ai sensi dell'art. 83, par. 2 e del cons. 148 del RGPD.

15.5. *Concessionari di pubblici servizi*

Nel 2021 l'esame delle segnalazioni e dei reclami presentati nei confronti di concessionari di pubblici servizi è stato prevalentemente rivolto ai trattamenti di dati personali dei clienti di fornitori operanti nel mercato libero dell'energia elettrica e del gas.

Al riguardo, i profili oggetto del maggior numero di contestazioni hanno riguardato: i presupposti di legittimità del trattamento (con specifico riferimento all'attivazione dei servizi di ultima istanza), le modalità di esercizio dei diritti dell'interessato (in particolare, ove concernenti dati di soggetti terzi, ad es. in caso di voltura del contratto di fornitura), l'adesione ai servizi offerti dai portali clienti *online* (soprattutto relativamente alle funzioni di bolletta via web).

15

Le istanze pervenute hanno costituito l'occasione per ribadire alcuni principi già espressi in provvedimenti di carattere generale, confermandone la loro efficacia anche nel nuovo quadro normativo, nonché per precisare e meglio definire la portata di alcune norme del RGPD con riferimento allo specifico settore di riferimento.

In materia di liceità del trattamento, è stato precisato, ad esempio, che l'attivazione dei servizi di ultima istanza nel settore del gas (nello specifico la "Fornitura del servizio di *default*" su rete di distribuzione e la "Fornitura di ultima istanza") è espressamente prevista dalla regolamentazione di settore, a tutela degli utenti finali, al ricorrere di specifiche circostanze (v. artt. 30 e 32, deliberazione Arera 28 maggio 2009, ARG/gas/64/09, all. A - Testo integrato di vendita gas). Tale tipologia di fornitura è, infatti, connessa al verificarsi di condizioni di fatto (l'interruzione del rapporto di fornitura di gas per cause indipendenti dalla volontà del cliente), che – in quanto espressamente previste dalla legge – non richiedono una condotta positiva da parte dell'interessato. Pertanto, le connesse attività di trattamento dei dati personali risultano lecite trovando idonea base giuridica in un presupposto di liceità diverso dal consenso dell'interessato ma ugualmente legittimo (cfr. art. 6, par. 1, lett. *c*), del RGPD (nota 28 aprile 2021).

Con riferimento alle modalità di registrazione alle aree clienti *online* messe a disposizione dai fornitori di energia sui propri siti internet, in particolare per attivare i servizi digitali di gestione del rapporto di fornitura, è stato chiarito che alcuni dati personali richiesti dal sistema (nello specifico il recapito telefonico e/o *e-mail* dell'utente) sono necessari a consentire al titolare di garantire la riservatezza e l'integrità (artt. 5 e 32 del RGPD) degli *account* a tal fine creati (ad es. mediante l'introduzione del codice *one-time-password* – inviato sull'utenza mobile/*e-mail* del cliente – quale secondo fattore di verifica all'atto della registrazione); ciò, in specie, al fine di prevenire la creazione di *account* falsi (nota 19 gennaio 2021). In altri casi, relativamente alla presenza, all'interno della cd. bolletta web, del *link* "contattami" (servizio che consente di essere direttamente richiamati sul proprio numero telefonico da un operatore a ciò specificatamente incaricato dal fornitore di energia), è stato precisato che esso costituisce una mera funzionalità aggiuntiva e più agevole di contatto del servizio clienti, al quale si può sempre e comunque accedere con le ordinarie modalità riportate dal fornitore in bolletta e reperibili sul sito internet di quest'ultimo. Il *link* "contattami" non obbliga, pertanto, il cliente a fornire i propri dati personali inerenti al numero di telefono, essendo sempre possibile contattare il servizio clienti attraverso i canali tradizionali messi a disposizione dalle società (nota 1° febbraio 2021).

Nella diversa materia dell'esercizio dei diritti, è stato inoltre precisato l'ambito di applicazione di alcune disposizioni del RGPD (nota 5 novembre 2021). In particolare, con riferimento ad alcune richieste di accesso ai dati del terzo contraente (ad es. in caso di voltura dell'utenza), è stato chiarito che la normativa in materia di protezione dei dati personali riconosce la facoltà di esercitare il diritto di accesso ai dati personali esclusivamente in capo all'interessato, *id est* alla persona fisica cui si riferiscono i dati personali oggetto della richiesta di accesso (art. 4, n. 1 del RGPD). Le predette norme sono state ulteriormente specificate dalla disciplina nazionale di recepimento (d.lgs. n. 101/2018), che, novellando il d.lgs. n. 196/2003, ha sancito il diritto di accesso anche con riferimento ai dati personali concernenti persone decedute da parte di chi ne abbia un interesse proprio (cons. 27 del RGPD e art. 2-*terdecies* del Codice). Ne consegue l'esclusione della facoltà di ottenere la comunicazione di dati personali di soggetti terzi, anche ove "partecipanti" alla medesima attività contrattuale (art. 15, par. 4, del RGPD).

Con riferimento alla cancellazione dei dati personali (spesso richiesta a seguito del recesso dal contratto di fornitura o del passaggio ad altro operatore nel mercato

15

libero), è stato ribadito (nota 5 marzo 2021) che l'art. 17 del RGPD sancisce il diritto per l'interessato di ottenerla ove sussista una delle condizioni individuate al par. 1 del medesimo articolo, tra cui la circostanza che i dati personali oggetto della richiesta non siano più necessari alle finalità per le quali sono "stati raccolti o altrimenti trattati" (art. 17, par. 1, lett. *a*), del RGPD). La cancellazione non potrà, pertanto, avere luogo ove la legge preveda espressamente che il titolare ponga in essere alcune attività di trattamento (ad es. la conservazione dei dati ai sensi dell'art. 2220 del c.c.) o nell'ipotesi in cui il trattamento medesimo possa proseguire sulla base di altri idonei presupposti di legittimità (art. 6 del RGPD, quale ad es. nei casi di trattamento per il recupero di un credito).

Particolarmente intensa è stata, inoltre, l'attività di vigilanza e di controllo con riferimento alle pratiche illecite dei cd. contratti non richiesti, ove effettuate per il tramite di trattamenti di dati personali inesatti e non aggiornati. Tali operazioni, 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, si affiancano, nella maggior parte dei casi, all'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). Per tali ragioni, l'attenzione dell'Autorità è stata rivolta soprattutto alla verifica, anche per il tramite dei poteri di cui all'art. 58, par. 1, lett. *b*), del RGPD, delle misure preventive da questi implementate; ciò anche in considerazione delle prescrizioni già fornite con il provvedimento 11 dicembre 2019, n. 231 (doc. web n. 9244358), decisione che, per quanto riferita ad uno specifico operatore, contiene tuttavia principi valevoli per l'intero settore di riferimento (v. provv. cit., punto 4). Dalle attività di indagine condotte è emerso, *in primis,* un generalizzato impegno, da parte degli operatori del mercato libero, nell'adozione di misure analoghe a quelle prescritte dal Garante, circostanza peraltro in linea di continuità con quanto già rilevato in merito nel 2020 (cfr. Relazione 2020, p. 187).

Ciò nonostante, i reclami e le segnalazioni hanno evidenziato il continuo evolversi delle predette attività fraudolente mediante l'individuazione di modalità di illecito sempre nuove e diversificate (si vedano, ad es. i recenti tentativi di attivazione non richiesta per il tramite del canale web di contrattualizzazione ovvero a prescindere dal rapporto di agenzia). L'Autorità ha pertanto in diverse occasioni invitato i fornitori di energia a rafforzare ulteriormente le misure individuate in adempimento al provvedimento di cui sopra, ad es. mediante la definizione di sistemi di *alert* sensibili a varie anomalie procedurali quali l'inserimento nel CRM di numerazioni e indirizzi ricorrenti, l'inesattezza o l'incompletezza dei dati contrattuali acquisiti, la numerosità dei contratti stipulati da ciascun agente/venditore, la molteplicità di proposte di contratto a nome di un medesimo soggetto (note 31 marzo e 23 aprile 2021).

15.6. *Attività di recupero crediti*

A seguito di un reclamo, un'attività di recupero crediti è risultata in contrasto con la disciplina in materia di protezione dei dati personali (art. 5, par. 1, lett. *a*) e *c*), del RGPD e con le specifiche prescrizioni impartite dal Garante con provvedimento 30 novembre 2005 sulla liceità, correttezza e pertinenza nell'attività di recupero crediti (doc. web n. 1213644).

Con provvedimento 16 dicembre 2021, n. 438 (doc. web n. 9742468), il Garante ha sanzionato una banca per aver inviato al reclamante una missiva recante all'esterno, sul fronte della busta, la dicitura "credito anomalo Chieti".

Nella specie la società aveva dichiarato che la missiva in questione non conteneva solleciti di pagamento bensì una comunicazione sulla trasparenza dei servizi bancari e finanziari e di aver utilizzato nelle successive comunicazioni, in luogo della medesima dicitura, un codice allo scopo di anonimizzare l'unità operativa inviante la missiva.

Ad avviso dell'Autorità, tale locuzione, indipendentemente dal contenuto della missiva, era suscettibile di palesare a soggetti terzi informazioni inerenti alla situazione di solvibilità del destinatario della comunicazione.

15.7. *Procedure IMI relative a trattamenti di dati in ambito economico-produttivo*

Le autorità di protezione dei dati, per la gestione dei meccanismi di cooperazione e coerenza previsti dal Capo VII del RGPD accedono alla piattaforma IMI, uno strumento veloce, sicuro, flessibile e trasparente.

La partecipazione alle procedure di cooperazione tra le autorità di protezione dei dati in presenza di trattamenti transfrontalieri occupa ormai una parte sempre più rilevante dell'attività dell'Autorità sia in termini di risorse impegnate che di quantità di lavoro svolto (cfr. parte IV, tab. 10-12).

Si conferma nel 2021 la prevalenza delle procedure IMI ai sensi dell'art. 56 del RGDP, volte all'identificazione dell'autorità capofila (*Lead Supervisory Authority*) e delle autorità interessate (*Concerned Supervisory Authority*), che rappresentano circa il 90% dei casi trattati.

Nel 2021 l'Autorità si è dichiarata "interessata", ai sensi dell'art. 4, n. 22, del RGPD, in 95 casi (47%) assumendo invece la posizione di "autorità capofila" in un numero limitato di casi riguardanti imprese con stabilimento unico o principale in Italia.

Rimane sostanzialmente stabile, rispetto al 2020, il numero delle procedure IMI di consultazione informale previste dall'art. 60, par. 1, del RGPD. A questo proposito si rileva come nel settore in questione, con l'esperienza maturata nei tre anni di funzionamento del meccanismo dello sportello unico, le autorità di protezione dei dati abbiano compreso l'importanza, più volte ribadita dal Comitato, di ricorrere a tale procedura volta a consentire lo scambio, fra l'autorità capofila e le autorità interessate, di informazioni, valutazioni e documenti relativi alla controversia prima della fase decisoria vera e propria che si esplica con il "caricamento" sulla piattaforma IMI del progetto di decisione da parte dell'autorità capofila.

La scelta di quest'ultima di coinvolgere, attraverso tale consultazione preventiva, le autorità interessate anticipando il dibattito in ordine al progetto di decisione vero e proprio è infatti volta ad evitare che le stesse, una volta sottoposto loro il progetto di decisione, sollevino obiezioni pertinenti e motivate, peraltro nei tempi strettissimi previsti dall'art. 60, par. 4. Tale approccio consente pertanto, già in una fase prodromica, di raggiungere un consenso in ordine al progetto di decisione fra le autorità che partecipano al procedimento di co-decisione previsto dal meccanismo dello sportello unico, limitando contemporaneamente il ricorso al meccanismo di coerenza previsto dall'art. 65, par. 1, lett. *a*), per la composizione delle controversie da parte del Comitato.

A questo proposito, si segnala che nel corso dell'anno, il Garante, in qualità di capofila, ha avviato la procedura IMI art. 60 di consultazione informale in relazione alle seguenti questioni: il ritardo del titolare nel rispondere all'istanze per l'esercizio dei diritti dell'interessato in violazione dell'art. 12, par. 3, il mancato riscontro all'istanza di cancellazione dei dati da parte del titolare che avrebbe continuato ad

15

utilizzare, a fini pubblicitari, la sua immagine senza il suo consenso; la violazione dei dati personali consistenti nell'invio ad un terzo della corrispondenza intercorsa tra il titolare e l'interessato.

Sono invece lievemente aumentate, rispetto al 2020, 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 invece che nel corso dell'anno sono state adottate dal Garante, in qualità di autorità competente, alcune decisioni emesse all'esito del procedimento di cooperazione.

In particolare, in due casi riguardanti trattamenti transfrontalieri con impatto esclusivamente locale di cui all'art. 56, par. 2, del RGPD – posti in essere da società operanti nel settore del cd. *food delivery* e facenti parte di gruppi societari con stabilimento principale in altro Stato membro – l'Autorità ha attivato la specifica procedura IMI nei confronti delle competenti autorità capofila le quali hanno dichiarato di non avere interesse a trattare i casi secondo il meccanismo dello sportello unico previsto dall'art. 60 del RGPD.

L'Autorità, quindi, dopo aver valutato la liceità dei trattamenti effettuati esclusivamente nei confronti di interessati residenti nel territorio nazionale, ha esercitato pienamente i poteri di cui all'art. 58 del RGPD adottando autonome decisioni che sono state condivise con l'autorità capofila nell'ambito della mutua assistenza (v. par. 14.2).

Inoltre, il Garante, in qualità di capofila, ha adottato una decisione su un reclamo proposto da un cittadino inglese nei confronti di una nota società automobilistica con sede principale in Italia. A riguardo, a conclusione dell'istruttoria, è stato caricato nel sistema IMI il progetto di decisione previsto dall'art. 60, par. 3, rispetto al quale è stata sollevata un'obiezione pertinente e motivata ai sensi dell'art. 60, par. 4. Il Garante ha dato seguito all'obiezione, modificando conformemente il progetto di decisione, che, in linea con una *best practise* – già utilizzata in casi analoghi e volta a raggiungere un consenso sul progetto di decisione –, è stato informalmente trasmesso all'autorità in questione mediante la procedura IMI art. 61 (*voluntary mutual assistance*) per la verifica della congruità delle correzioni apportate con l'obiezione sollevata. È stata quindi adottata ai sensi dell'art. 60, par. 7, la decisione, poi notificata al titolare del trattamento e comunicata all'autorità di controllo a cui è stato presentato il reclamo.

In via di conclusione è invece la procedura di cooperazione avente ad oggetto il reclamo proposto da un cittadino tedesco volto a segnalare una possibile violazione dell'art. 32 del RGPD da parte di una società con sede in Italia (il titolare gli avrebbe inviato, nella *e-mail* di conferma della registrazione al proprio sito web, la sua *password* in chiaro).

Per quanto riguarda l'assistenza reciproca fra le autorità di controllo ex art. 61 del RGPD, sempre con riferimento al settore privato, 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 (ad es. riguardanti l'ambito della esenzione prevista per trattamenti per scopi esclusivamente personali o domestici di cui all'art. 2, comma 2, lett. *c*), del RGPD, con particolare riferimento alla videosorveglianza o sui profili *privacy* connessi alla normativa in materia di contrasto al riciclaggio).

In aumento anche i reclami al Garante proposti, ai sensi degli art. 143 e ss. del Codice, nei confronti di società con sede in altro Stato membro; per essi si è reso

necessario avviare le procedure di cooperazione applicabili, trasmettendo la relativa documentazione alla competente autorità capofila.

Infine in conseguenza della Brexit, l'Autorità di controllo inglese (*Information Commissioner Office*-ICO) non è più coinvolta nelle procedure di cooperazione europea. Rispetto ad alcuni casi tuttora pendenti che interessano società con sede nel Regno Unito, l'Autorità, anche grazie alla collaborazione con le altre autorità di controllo, ha appurato che tali titolari hanno deciso di mantenere lo stabilimento principale nel Regno Unito; pertanto, non applicandosi più il meccanismo dello sportello unico, l'Autorità, in quanto autorità competente ai sensi dell'art. 55, si interfaccerà direttamente con il titolare per il tramite del rappresentante designato ai sensi dell'art. 27 del RGPD o, in mancanza, attraverso contatti con lo stabilimento locale nel territorio italiano, ove esistente.

15.8. *Accreditamento e certificazioni*

Nel 2021 è proseguito il rapporto collaborativo tra il Garante e l'Ente nazionale di accreditamento, Accredia.

A seguito della convenzione del 2019 (cfr. Relazione 2019, p. 159) finalizzata allo scambio di informazioni riguardanti le attività di certificazione e accreditamento previste dall'art. 43 del RGPD, a marzo 2021 è stata sottoscritta una nuova convenzione (doc. web n. 9570342), della validità di tre anni, che amplia gli obblighi informativi reciproci, anche alla luce dell'approvazione, in data 29 luglio 2020, da parte del Garante, dei requisiti nazionali di accreditamento degli organismi di certificazione aggiuntivi rispetto a quelli stabiliti dalla norma UNI CEI EN ISO/IEC 17065 (doc. web n. 9445086, v. Relazione 2020, p. 190). Nel nuovo accordo particolare cura è stata dedicata all'individuazione delle informazioni che ciascuna delle parti si impegna a fornire all'altra, sia con riguardo ai poteri di controllo del Garante in materia di certificazione dei trattamenti di dati personali, sia rispetto agli sviluppi e agli orientamenti in ambito europeo con particolare riferimento alle attività svolte dal Comitato europeo (cfr. par. 23.1).

Inoltre, sono state pubblicate il 14 luglio 2021 sui siti internet dei due Enti alcune FAQ, – anche in merito all'ambito di applicazione soggettivo e oggettivo del meccanismo delle certificazioni e dell'accreditamento – allo scopo di fugare eventuali incertezze in ordine alla corretta interpretazione e applicazione della relativa normativa in materia.

16 Altri trattamenti in ambito privato

16.1. *Il trattamento dei dati personali nell'ambito del condominio*

Nel 2021 si è registrato un significativo afflusso di istanze in materia condominiale che, sebbene in larga parte riguardanti argomenti già esaminati in passato e trattati più volte in sede di precedenti Relazioni, hanno comunque comportato un intenso e proficuo impegno. Al riguardo il Garante, da una parte ha continuato a fornire ai cittadini i necessari chiarimenti in merito ai vari temi; dall'altra, ha intensificato gli interventi volti a promuovere la consapevolezza da parte dei titolari e dei responsabili del trattamento degli obblighi previsti, in tale settore, dalla normativa. Tutto ciò anche con riguardo alle ulteriori richieste e quesiti – in ragione della situazione contingente e del persistente stato di emergenza – in ordine alla possibilità di raccogliere e condividere, nel settore condominiale, informazioni in merito alla salute degli interessati, come misura di prevenzione dal contagio epidemiologico (cfr. Relazione 2020, p. 192). In tale contesto, è stata altresì colta l'occasione per chiarire che, rispetto alla specifica misura delle certificazioni verdi Covid-19 introdotta nel 2021, in ragione del quadro normativo vigente non è previsto l'obbligo di esibire il cd. *green pass* per partecipare alle assemblee condominiali (nota 9 novembre 2021).

Altra questione ha riguardato la possibilità di accedere ai dati del registro dell'anagrafe condominiale. In particolare, è stato chiesto al Garante se un condòmino potesse avere accesso al registro dell'anagrafe condominiale in relazione ai dati personali di un affittuario appartenente al medesimo condominio. L'Ufficio, nel richiamare una decisione del Tribunale di Palermo ed una del Tribunale di Brescia (rispettivamente n. 2514/2021 e n. 2177/2018), ha ricordato 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" (cfr. Relazione 2015, p. 130).

Ferma restando, pertanto, l'accessibilità del registro in questione nei termini indicati dalla medesima disciplina civilistica (art. 1129, comma 2, del c.c.), in base al principio di *accountability* (art. 5, par. 2, del RGPD), spetta allo stesso titolare valutare la rispondenza dei trattamenti effettuati ai princìpi di protezione dei dati personali, selezionando le sole informazioni pertinenti rispetto allo scopo della richiesta alla luce del principio di minimizzazione dei dati (art. 5, par. 1, lett. *c*), del RGPD) (nota 24 dicembre 2021).

A seguito di alcune istanze sono state fornite indicazioni in merito agli obblighi gravanti sul titolare qualora il trattamento dei dati venga posto in essere, nel contesto condominiale, dal responsabile del trattamento (cfr. art. 28 del RGPD). Sul punto, con particolare riguardo alla figura dell'amministratore, è stato sottolineato – richiamando in tal senso quanto già riportato a suo tempo sul tema nel *vademecum* sopra citato (doc. web n. 2680240, p. 5) –, che è "l'assemblea [alias il condominio] che può decidere di designare [l'amministratore] anche formalmente "responsabile del trattamento" dei dati personali dei partecipanti al condominio (proprietari, locatari, usufruttuari), attribuendogli uno specifico ruolo in materia di *privacy*". Al contempo l'Autorità ha precisato che la nomina dell'amministratore del condominio,

quale responsabile del trattamento, riveste il carattere dell'eventualità (cfr. provv. 18 maggio 2006, doc. web n. 1297626) e che a prescindere da tale opportunità resta comunque in capo all'amministratore la concreta gestione del trattamento dei dati del condominio in base alle regole del mandato (provv. 19 maggio 2000, doc. web n. 42268; v. note 27 maggio e 23 settembre 2021).

16.2. *I trattamenti dei dati da parte di associazioni, partiti politici e confessioni religiose*

Con riferimento ai trattamenti dei dati personali in ambito associativo, l'attività ha riguardato sia, in generale, le modalità di applicazione del RGPD in considerazione delle specificità del terzo settore, sia, più nello specifico, le peculiarità proprie dei trattamenti posti in essere da partititi politici e da confessioni religiose.

Nel settore associativo, le questioni oggetto di maggiori criticità hanno riguardato i presupposti di legittimità del trattamento (con specifico riferimento alla circolazione dei dati degli associati all'interno dell'organizzazione), le modalità di contatto degli interessati (nella specie per le finalità di rendicontazione dell'attività associativa), la comunicazione di dati a terzi (in particolare in caso di produzione di atti in giudizio o di richieste provenienti da autorità pubbliche).

In ordine all'ambito e alle modalità di circolazione dei dati degli associati all'interno della compagine associativa, l'Autorità, con provvedimento 29 aprile 2021, n. 165 (doc. web n. 9672215), ha ritenuto illecito il trattamento di dati personali posto in essere da una associazione che rappresenta istituti privati per le investigazioni, per l'avvenuta comunicazione a tutti gli associati, tramite *newsletter,* di informazioni di carattere personale riferite all'interessato, come riportate nei verbali delle riunioni degli organi sociali; questi ultimi, in particolare, avevano deliberato il deferimento al collegio dei probiviri di ogni decisione relativa ad eventuali provvedimenti da adottare nei confronti dell'associato, responsabile di una lettera dai contenuti ritenuti offensivi e denigratori nei confronti della federazione.

Nel provvedimento l'Autorità ha così evidenziato come il trattamento dei dati personali degli aderenti, con riferimento ai dati comuni, è lecito laddove gli stessi abbiano prestato il loro consenso (art. 6, par. 1, lett. *a*), del RGPD) ovvero il trattamento sia necessario per il perseguimento del legittimo interesse dell'associazione o di terzi a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali degli interessati (art. 6, par. 1, lett. *f*), del RGPD) "tenendo conto delle ragionevoli aspettative nutrite dall'interessato medesimo in base alla sua relazione con il titolare" e delle circostanze in cui l'interessato non possa "ragionevolmente attendersi un ulteriore trattamento dei suoi dati" (cfr. cons. 47 del RGPD).

Nel caso di specie, accertata l'assenza – nelle norme statutarie o in altro atto adottato dall'associazione – di una precisa regolamentazione (e di una correlata informativa) dei casi e delle condizioni in cui i dati personali di un iscritto possono essere comunicati agli altri iscritti (con particolare riguardo alla fase di deferimento al collegio dei probiviri precedente all'attivazione del procedimento istruttorio da parte dello stesso) e considerato che il consenso prestato dal reclamante al momento dell'adesione alla federazione concerne i trattamenti posti in essere dalla stessa per il perseguimento delle finalità associative come individuate nello statuto, il trattamento è stato ritenuto illecito in quanto effettuato in assenza del consenso dell'interessato o di altro legittimo presupposto (art. 6, par. 1, del RGPD), nonché in violazione dei principi generali di liceità, correttezza e minimizzazione nel trattamento dei dati rispetto alle finalità perseguite di cui all'art. 5, par. 1, lett. *a*) e *c*), del RGPD. L'Autorità ha infatti rilevato che sebbene rientri nell'esercizio dell'autonomia privata

16

stabilire i casi, le modalità e i limiti della circolazione dei dati riferiti agli associati all'interno della compagine associativa, anche in assenza del consenso dei singoli purché nel rispetto del principio di finalità, resta fermo che il titolare è comunque tenuto ad assicurare che i trattamenti siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità associative perseguite.

Alcune segnalazioni hanno riguardato i presupposti di legittimità della comunicazione di dati personali degli associati all'esterno della compagine associativa. In particolare, in un caso è stata lamentata la produzione in giudizio di un documento relativo a un provvedimento disciplinare comminato da un'associazione non meglio identificata ai danni dell'interessato e da questa consegnato alla controparte in assenza di apposita autorizzazione. Al riguardo, l'Ufficio ha chiarito che, in base alla disciplina vigente e al consolidato orientamento del Garante, spetta agli stessi organi giudiziari valutare la conformità alla legge, secondo le pertinenti disposizioni di rito, dei trattamenti di dati personali connessi ad atti, documenti e provvedimenti prodotti in giudizio (art. 160-*bis* del Codice). Si è pertanto invitato l'interessato a valutare l'opportunità di rivolgersi direttamente all'Autorità giudiziaria al fine di far valere in tale sede eventuali profili di illegittimità in relazione alla documentazione dallo stesso menzionata, ferma restando la possibilità di comunicare a terzi i predetti dati sulla base di un idoneo presupposto di legittimità (art. 6, par. 1, lett. *b*) e ss. del RGPD) (nota 7 dicembre 2021).

In un'altra fattispecie, l'Autorità si è espressa con riferimento ad una richiesta di chiarimenti, proveniente da un'associazione, in merito alla possibilità di comunicare a una commissione parlamentare di inchiesta, in assenza del consenso degli interessati, l'elenco dei partecipanti ai progetti di sostegno realizzati con il proprio contributo. L'Ufficio, rilevato che le commissioni parlamentari di inchiesta sono legittimate a operare, con i poteri riconosciuti dall'ordinamento e nei limiti da questo stabiliti, in base a espresse disposizioni di legge, ha rappresentato all'associazione che la predetta commissione, considerati anche gli ampi poteri istruttori e investigativi (propri dell'Autorità giudiziaria) riconosciuti dalla legge istitutiva, poteva legittimamente chiedere e acquisire, indipendentemente dalla volontà degli interessati, informazioni, atti e documenti necessari all'esecuzione dei propri compiti istituzionali, fermi restando i limiti generali connessi all'adeguatezza e pertinenza dei dati richiesti (art. 5, par. 1, lett. *c*), del RGPD) e, ove opponibili, quelli connessi al segreto professionale o d'ufficio.

Con riferimento alle modalità di trattamento per finalità associative alcune associazioni e *onlus* hanno chiesto al Garante di valutare eventuali controindicazioni, sotto il profilo della disciplina di protezione dei dati personali, in ordine a una proposta di modifica normativa volta a consentire loro, su base consensuale, di conoscere i dati dei propri contribuenti; ciò, al fine anzitutto di informarli in merito alle attività di gestione dei fondi e di dimostrare loro la propria affidabilità e responsabilità, anche in vista di ulteriori donazioni.

In proposito, l'Ufficio ha confermato che la conoscibilità dei menzionati dati richiede, oltre al consenso degli interessati, un intervento normativo che, incidendo sulla disciplina di riferimento, consideri – calibrandone la portata in rapporto ai diritti e alle libertà fondamentali degli interessati – presupposti, modalità e limiti dell'operazione, anche rispetto ai compiti e alle attività dell'Agenzia delle entrate. Nel contempo, evidenziando la necessità di ulteriori riflessioni su alcuni aspetti di dettaglio (quali, tra gli altri, i compiti dell'Agenzia delle entrate, le modalità di contatto degli interessati, le finalità del trattamento, i tempi di conservazione dei dati, la revocabilità del consenso), si è riservato di formulare eventuali ulteriori considerazioni, sulla base di un testo normativo compiutamente definito, in occasione della

consultazione formale prevista ai sensi degli artt. 36, par. 4, 57, par. 1, lett. *c*) e 58, par. 3, lett. *b*), del RGPD (nota 19 novembre 2021, doc. web n. 9728518).

Da ultimo a seguito di una segnalazione presentata dall'Associazione Movimento 5 Stelle, è stato adottato in via d'urgenza il provvedimento 1° giugno 2021, n. 223 (doc. web n. 9592011) con il quale è stato ingiunto all'Associazione Rousseau, quale responsabile del trattamento dei dati degli iscritti al Movimento 5 Stelle (titolare del trattamento), di provvedere, nel termine di cinque giorni, a dare attuazione al disposto di cui all'art. 28, par. 3, lett. *g*), del RGPD, mediante consegna al titolare medesimo di tutti i dati personali degli iscritti (di cui l'Associazione risulti responsabile del trattamento), astenendosi – nelle more – da ogni ulteriore trattamento dei dati stessi, salvo il caso di esplicite e specifiche richieste del Movimento. Come è ben noto (posto che la questione è stata oggetto di ampia risonanza mediatica), l'Associazione Rousseau ha adempiuto nel termine prescritto, trasferendo i dati degli iscritti al Movimento.

Inoltre nel corso dell'anno sono state presentate dall'Associazione Movimento 5 Stelle una serie di richieste di accesso documentale agli atti del complesso procedimento istruttorio condotto dall'Autorità nei confronti della Piattaforma Rousseau (conclusosi con il provv. 4 aprile 2019, n. 83, doc. web n. 9101974, v. Relazione 2019, p.131) nonché richieste di accesso civico da singoli iscritti all'Associazione.

Sempre con specifico riferimento ai trattamenti di dati personali posti in essere da partiti e movimenti politici, l'Ufficio sta inoltre valutando la questione relativa ai tempi di permanenza dei *curricula* e dei certificati del casellario giudiziale dei candidati alle elezioni pubblicati sui siti web di partiti e movimenti politici in ottemperanza alla legge n. 3/2019. Muovendo da un reclamo – che contestava la mancata cancellazione dei dati personali contenuti nei predetti documenti nonostante l'interessata non fosse stata eletta e fossero trascorsi oltre due anni dalla conclusione della consultazione elettorale – è emersa l'esigenza, più generale, di individuare congrui termini, non previsti dalla citata legge n. 3/2019, entro cui provvedere alla rimozione dei predetti documenti – potenzialmente contenenti informazioni anche molto delicate – dai siti web di partiti e movimenti politici; ciò, anche alla luce dell'esigenza, manifestata dalla stessa commissione di garanzia degli statuti e per la trasparenza e il controllo dei rendiconti dei partiti politici, di esercitare i propri poteri sanzionatori nei confronti dei soggetti inadempienti entro il termine quinquennale previsto dalla legge n. 689/1981. La questione, considerata la portata e i risvolti di carattere generale, è attualmente all'esame dell'Autorità, che sta valutando le opportune iniziative da intraprendere al fine di individuare un ragionevole punto di equilibrio tra le esigenze di trasparenza sottese alla legge n. 3/2019, quelle espresse dalla citata commissione di garanzia e il diritto all'oblio degli interessati.

In materia di confessioni religiose, sono pervenuti diversi reclami e segnalazioni relativi al trattamento posto in essere dalla Congregazione cristiana dei testimoni di Geova in relazione alle finalità religiose perseguite. All'esito degli approfondimenti effettuati, è emersa una sostanziale conformità al RGPD delle attività di trattamento poste in essere dalla Congregazione nonché l'esigenza di fornire alcune indicazioni, in particolare in materia di esercizio dei diritti, volte ad ulteriormente rafforzare il livello di conformità del predetto titolare alla disciplina di protezione dei dati.

Nello specifico l'Autorità ha *in primis* chiarito che la Congregazione è una confessione religiosa cui è stata riconosciuta, con decreto del Presidente della Repubblica (d.P.R. 31 ottobre 1986, n. 783), la qualità di ente morale con personalità giuridica ex art. 2, l. n. 1159/1929 (cfr. anche art. 10, r.d. n. 289/1930; v. anche Consiglio di Stato, parere 30 luglio 1986, n. 1390). Nell'ambito di tale cornice normativa, essa tratta i dati personali relativi agli aderenti in conformità ai principi di culto cui

16

essa si inspira e alla propria organizzazione interna, circostanza rappresentata nell'informativa resa ai sensi dell'art. 13 del RGPD. In particolare, i dati personali degli aderenti (ivi comprese le categorie particolari di dati degli stessi ai sensi dell'art. 9 del RGPD) sono trattati per lo svolgimento delle attività religiose connesse al culto e all'assistenza spirituale dei fedeli trovando idonea base giuridica, con riferimento ai dati comuni, nell'art. 6, par. 1, lett. *f*), del RGPD (cd. legittimo interesse del titolare, cfr. relazione illustrativa che accompagna lo schema di d.lgs. n. 101/2018, p. 3) e, con riguardo al trattamento di categorie particolari di dati, nell'art. 9, par. 2, lett. *d*), del RGPD.

Quest'ultima disposizione, più nello specifico, legittima i trattamenti dei dati personali cd. sensibili degli aderenti ad un'associazione – quale anche una confessione religiosa – ove si sostanzino in comunicazioni interne alla predetta organizzazione e a condizione che siano effettuati nel rispetto delle regole definite dalla medesima comunità. Appartengono a tale tipologia di trattamenti quelli svolti dalle articolazioni territoriali della Congregazione e dai vari organi religiosi e ministri di culto della stessa, secondo le prassi interne alla suddetta confessione religiosa; ciò anche con riferimento alle procedure di "valutazione" degli aderenti per l'attribuzione dei diversi incarichi di culto, nonché per "richiamare alla fede" – anche per il tramite dei cd. annunci pubblici e sempre ai sensi dei sopra richiamati precetti religiosi – chi è rimasto "inattivo" o chi ha manifestato l'intenzione di allontanarsi dalla comunità. Le menzionate attività di trattamento di dati personali, in quanto effettuate nell'ambito delle prassi inerenti all'esercizio del culto, non appaiono poste in essere in contrasto con i principi di protezione dei dati personali (artt. 5, 6 e 9 del RGPD); ciò sia perché effettuate nel rispetto delle attività di fede professate dall'organizzazione religiosa, sia in considerazione del fatto che le suddette informazioni circolano esclusivamente all'interno della predetta comunità (v. artt. 6, par. 1, lett. *f*) e 9, par. 2, lett. *d*), del RGPD). Per le medesime ragioni, è sulla base dei suindicati principi che devono essere valutati i tempi di conservazione di alcune tipologie di dati personali, quali ad esempio quelle relative all'ex aderente, nonché le modalità di accesso da parte dei ministri di culto e degli altri organi religiosi ad alcune informazioni contenute negli archivi della Congregazione (es. in caso di trasferimento dell'aderente ad altra circoscrizione). Con la medesima decisione, l'Autorità è intervenuta anche in materia di esercizio dei diritti. In tale ambito, il Garante, oltre a ribadire che il diritto di accesso ai sensi dell'art. 15 del RGPD consente all'interessato di accedere ai propri dati personali effettivamente detenuti dal titolare, ma non accorda a quest'ultimo alcun diritto di ottenere dal medesimo titolare anche copia degli atti che li contengono, è intervenuto con specifico riferimento al diritto di rettifica in ordine alla posizione di ex aderente alla predetta confessione religiosa; ciò in considerazione delle diverse istanze pervenute da ex membri della Congregazione e volte ad ottenere la cancellazione dei propri dati personali dagli archivi della stessa. Sul punto, è stato chiarito che, in analogia a quanto già statuito con riferimento alla Chiesa cattolica (v. provv. 13 settembre 1999, doc. web n. 1090502) la registrazione dell'adesione ad una confessione religiosa costituisce un evento storico di cui non può essere rimossa ogni traccia nel predetto ordinamento interno, ma di cui comunque deve essere fornita idonea rappresentazione, mediante l'apposizione di un'annotazione a margine del dato oggetto di rettifica. Sul punto, l'Autorità si è inoltre espressa con specifico riferimento ai casi in cui la predetta istanza di rettifica del dato inerente alla non appartenenza alla Congregazione, ha ad oggetto la condizione di soci dimissionari, cd. dissociati, ovvero di soggetti che hanno espresso la propria volontà di recedere dalla comunità mediante presentazione di lettera di dimissioni dalla qualifica di associato. Tale condizione, che è tenuta distinta, nel predetto ordinamento confessionale, dalla

16

diversa qualifica di disassociato, ovvero di colui che è stato allontanato dalla comunità per decadenza o per espulsione (quale conseguenza di comportamenti suscettibili di sanzione disciplinare), costituisce un elemento significativo dell'identità dei reclamanti meritevole di fedele ed esatta rappresentazione all'interno degli archivi della Congregazione.

Al riguardo, pertanto, il Garante, accertata nel corso dell'attività istruttoria la fedele trasposizione nei predetti archivi dell'avvenuto allontanamento dell'ex aderente dalla comunità, corredata dalle specifiche modalità di realizzazione dello stesso (dissociazione o disassociazione), ha inoltre riconosciuto le legittime aspettative degli interessati di essere resi edotti, a seguito di presentazione di istanza di esercizio del diritto di accesso ai propri dati, della predetta avvenuta annotazione, ammonendo la Congregazione a conformare, per il futuro, le proprie modalità di riscontro ex art. 12 del RGPD, alle indicazioni sopra specificate (provv. 25 febbraio 2021, n. 71, doc. web n. 9574136).

17 Intelligenza artificiale e diritto alla protezione dei dati personali

A partire dalla sua istituzione, il Garante ha costantemente seguito gli sviluppi tecnologici (comunque) correlati al trattamento di dati personali susseguitisi nel tempo, interessandosi delle relative ricadute individuali e sociali; ciò in ragione delle attribuzioni facenti capo alle autorità di protezione dei dati, che da ultimo hanno trovato il proprio fondamento nell'art. 8 (e anzitutto nel par. 3) della CDFUE e nei compiti istituzionali loro rimessi (si pensi anzitutto a quelli indicati all'art. 57, par. 1, lett. *a*) ed *i*), ma anche *m*) e *n*) oltre che *b*) e *d*), del RGPD).

In tempi più recenti, ciò è avvenuto anche con riguardo alle tematiche dell'intelligenza artificiale: esse hanno formato oggetto di prime considerazioni nell'ambito dell'indagine, svolta congiuntamente con l'Agcom e l'Agcm, dedicata al tema dei *big data* (v. in merito i numerosi richiami all'IA contenuti nel Rapporto finale pubblicato nel 2020: doc. web n. 9264297); ma si pensi anche al tema dei *deepfake,* al quale è stato dedicato un primo *vademecum* (doc. web n. 9512226); v. altresì l'audizione del Presidente del Garante 12 gennaio 2021 sul d.d.l. 1900 e 1549 (Commissione parlamentare d'inchiesta sulla diffusione massiva di informazioni false, doc. web n. 9518110: cfr. par. 3.1.1) e al tema degli assistenti digitali (cfr. *vademecum* al doc. web n. 9696995); in più occasioni l'argomento ha catalizzato l'attenzione del Garante anche nell'ambito di convegni e seminari (cfr. par. 25.5).

La presentazione, il 21 aprile 2021, da parte della Commissione europea, della proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (COM(2021) 206 *final*) – sulla scorta degli approfondimenti preliminari curati dal Gruppo di esperti ad alto livello sull'IA (confluiti, tra l'altro, negli Orientamenti etici per un'IA affidabile, resi pubblici l'8 aprile 2019) – ha tuttavia segnato una svolta decisiva, ponendo la materia (i cui ambiti applicativi già si palesano estesissimi e difficilmente circoscrivibili) al centro dell'attenzione delle autorità europee di protezione dei dati personali in ragione delle significative implicazioni per i diritti e le libertà fondamentali dei singoli (e della società nel suo insieme), sia in relazione al cd. addestramento che al successivo impiego dell'IA. La proposta, tuttora in corso di discussione a livello europeo (e affiancata dai lavori della Commissione speciale sull'intelligenza artificiale in un'era digitale, istituita con la decisione del Parlamento europeo del 18 giugno 2020), ha così formato oggetto di un parere congiunto, reso il 18 giugno 2021 dall'EDPB e dal GEPD (https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_it.pdf) nel quale, pur a fronte di una valutazione (nel complesso) positiva del testo predisposto dalla Commissione europea, sono state comunque evidenziate anche rilevanti criticità. Tra queste, si è evidenziata la mancata previsione di forme di cooperazione internazionale in materia nell'ambito dell'IA, atteso il rischio significativo di elusione delle garanzie individuali (ad es. nel caso di Paesi terzi o di organizzazioni internazionali che gestiscono applicazioni ad alto rischio su cui fanno affidamento le autorità pubbliche nell'UE). Ancora, nel soffermarsi sulle pratiche volte a determinare il "punteggio sociale" (*social scoring*) – peraltro ambito di intervento in passato da parte del Garante (cfr. provv. 24 novembre 2016, n. 488, doc. web n. 5796783 e successiva ordinanza-ingiunzione 26 luglio 2018, n. 442, doc. web n. 9052099; v. inoltre, in merito alla vicenda, Cass. civ. 25 maggio 2021,

n. 14381) – il parere suggerisce l'opportunità che il futuro regolamento sull'IA le vieti (non solo in ambito pubblico, ma anche privato) in considerazione dell'intrinseco rischio elevato di discriminazione legato al loro utilizzo.

Nel richiamato parere – il cui contenuto è più ampiamente sintetizzato al par. 23.1 – particolare attenzione è altresì dedicata alle forme di identificazione biometrica da remoto delle persone fisiche in spazi accessibili al pubblico, propendendo per l'introduzione di un divieto generale di qualsiasi utilizzo dell'IA a fini di riconoscimento automatico delle caratteristiche umane (volto, andatura, impronte digitali, DNA, voce, sequenze di battute su tastiera e altre caratteristiche biometriche o comportamentali). È quest'ultima, a ben vedere, tematica particolarmente sensibile, oggetto delle *Guidelines on Facial Recognition* del 28 gennaio 2021, T-PD(2020)03rev4, del *Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention* 108 (cfr. par. 23.3), e da tempo pure all'attenzione del Garante, con particolare riferimento ai sistemi Sari e Sari *Real Time* (cfr. rispettivamente, provv.ti 26 febbraio 2020, n. 54, doc. web n. 9309458 e 25 marzo 2021, n. 127, doc. web n. 9575877). Materia sulla quale, da ultimo, è intervenuto anche il legislatore nazionale, che ha introdotto, con l'art. 9, comma 9, d.l. 8 ottobre 2021, n. 139 (convertito, con modificazioni, in legge 3 dicembre 2021, n. 205), fino al 31 dicembre 2023, una moratoria nell'impiego dei sistemi biometrici di riconoscimento facciale in luoghi pubblici, peraltro di portata limitata (nei termini indicati al comma 12 della disposizione).

Non meno significativi, sempre nella cornice sovranazionale, sono stati gli sviluppi dei lavori tenutisi presso il Consiglio d'Europa: dapprima con le linee guida in materia di IA e protezione dei dati, adottate dal Comitato consultivo (cd. T-PD) della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108) il 25 gennaio 2019 (T-PD(2019)01); quindi con i lavori (cui pure l'Autorità ha preso parte) dell'*Ad hoc Committee on Artificial Intelligence* (CAHAI) – che ha operato sulla base di tre articolazioni principali: il *Policy Development Group* (PDG), il *Consultations and Outreach Group* (CoG) e il *Legal Framework Group* (LFG) (cfr. Relazione 2020, p. 240) – conclusisi con l'adozione di un documento finale all'esito della riunione del 30 novembre-2 dicembre 2021 (più ampie informazioni in https://www.coe.int/en/web/artificial-intelligence/cahai); esso prelude all'attività che verrà svolta dal neo-istituito Comitato sull'IA (*Committee on Artificial Intelligence* - CAI), i cui lavori inizieranno nella prima parte del 2022.

Entro questa più generale cornice di riferimento – arricchitasi della *Recommendation on the Ethics of Artificial Intelligence* dell'UNESCO (SHS/BIO/REC-AIETHICS/2021, in https://unesdoc.unesco.org/ark:/48223/pf0000380455) – ed in considerazione dell'interlocuzione fattasi più frequente con l'Autorità su questioni connesse all'IA, il Garante ha istituito una nuova unità organizzativa di primo livello, il Dipartimento intelligenza artificiale, cui è tra l'altro rimesso il compito di seguire i vari sviluppi nelle aree di interazioni tra IA e diritto alla protezione dei dati personali, anche in relazione ai tavoli di lavoro nazionali, europei e internazionali (indicazioni più puntuali si rinvengono nella deliberazione 27 maggio 2021, n. 222, modifiche al regolamento n. 1/2000 in materia di organizzazione e funzionamento dell'Ufficio del Garante per la protezione dei dati personali, doc. web n. 9669371).

Tra le iniziative intraprese, preordinate ad acquisire una maggiore consuetudine con le tematiche dell'IA e a dotare l'Autorità di nuove professionalità (in particolare nel contesto della *data science*), merita segnalare l'attività volta ad individuare sinergie sul territorio nazionale con primari centri di ricerca dotati di *expertise* specifiche nel settore dell'IA: in questa prospettiva, sono stati coltivati contatti con il Cini

17

(Consorzio interuniversitario nazionale per l'informatica), confluiti nella stipula di un accordo triennale di collaborazione, come pure un protocollo di intenti, di durata biennale, con Fondazione Leonardo civiltà delle macchine (doc. web n. 9590916). Parimenti, prosegue 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 partecipa in qualità di *partner.* L'iniziativa, che vede la partecipazione dell'Università del Lussemburgo, dell'Università Paul Sabatier Tolosa III, della *Vrije Universiteit* di Bruxelles, dell'Università del Pireo, dell'Università Jagellonica e del Consiglio nazionale delle ricerche, nonché di alcune (piccole, medie e grandi) imprese, mira a formare esperti in *data science* e diritto in grado di operare nel settore dell'IA.

Approfondimenti, talora in ragione delle tematiche portate all'attenzione dell'Autorità, sono stati curati infine rispetto a vari contesti nei quali l'IA è chiamata ad assumere un ruolo particolarmente rilevante: in ambito fiscale, in chiave di contrasto all'evasione (v. in merito, da ultimo parere 22 dicembre 2021, n. 453, sullo schema di decreto attuativo dell'art. 1, comma 683, della legge 27 dicembre 2019, n. 160, doc. web n. 9738520, cfr. par. 4.1.3), come pure in relazione al fenomeno conosciuto con la locuzione *predictive policing,* anche alla luce della risoluzione del Parlamento UE 6 ottobre 2021 sull'IA nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI). Tra gli ulteriori ambiti presi in considerazione meritano infine di essere richiamati quelli della medicina di iniziativa (cfr. parere 16 dicembre 2021, n. 431, doc. web n. 9738538) ed il *focus* che, mediante attività di controllo, l'Autorità ha indirizzato rispetto a talune applicazioni algoritmiche nell'ambito della cd. *gig economy* (v. *amplius* quanto riferito nel par. 14.2 in relazione ai trattamenti effettuati mediante piattaforme digitali nel settore del *food delivery*).

18 Violazione dei dati personali

Con provvedimento 27 maggio 2021, n. 209 (doc. web n. 9667201), il Garante – considerato l'elevato numero di notifiche di violazione dei dati personali pervenute annualmente (talvolta prive di informazioni necessarie per una compiuta valutazione) – ha ritenuto necessario adottare un'apposita procedura telematica per la notifica delle violazioni dei dati personali e per l'individuazione delle informazioni da fornire all'Autorità ai sensi dell'art. 33 del RGPD o dell'art. 26, d.lgs. n. 51/2018.

Dal 1° gennaio al 31 dicembre 2021 sono state notificate all'Autorità 2.071 violazioni dei dati personali ai sensi dell'art. 33 del RGPD o dell'art. 26, d.lgs. n. 51/2018, da parte di soggetti pubblici (50,5%) e privati (49,5%). Alcune violazioni dei dati personali sono state notificate per fasi (come previsto dall'art. 33, par. 4, del RGPD e dall'art. 26, comma 1, d.lgs. n. 51/2018) con l'invio, in un primo momento, di una notifica preliminare e, successivamente, di una o più notifiche integrative.

In particolare, nel settore pubblico, le violazioni dei dati personali hanno riguardato soprattutto comuni, istituti scolastici e strutture sanitarie (Asl, Aziende ospedaliere, policlinici e Irccs); nel settore privato, sono stati invece coinvolti sia piccole e medie imprese e professionisti, sia grandi società del settore delle telecomunicazioni, energetico, bancario e dei servizi.

I fenomeni più frequentemente riscontrati sono la diffusione di *malware* di tipo *ransomware,* che ha compromesso la disponibilità dei dati all'interno dei sistemi *server,* delle postazioni di lavoro e dei *database* di numerose organizzazioni pubbliche e private, e che, in alcuni casi, ha anche inciso sulla riservatezza delle informazioni trattate; l'accesso non autorizzato o illecito ai dati personali trattati all'interno di sistemi informativi complessi; la diffusione accidentale di dati personali a causa di erronee configurazioni dei sistemi *software* di gestione della posta elettronica.

L'attività istruttoria svolta a seguito della notifica delle violazione dei dati personali ha avuto come 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 di valutare la necessità di comunicare la violazione agli interessati coinvolti, fornendo indicazioni specifiche sulle misure da adottare per proteggersi da eventuali conseguenze pregiudizievoli.

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.

Nei casi in cui è emersa una possibile inadeguatezza delle misure di sicurezza adottate dal titolare o dal responsabile, sono stati acquisiti gli elementi necessari a individuare le lacune organizzative e tecniche che hanno determinato, o hanno contribuito a determinare, le violazioni dei dati personali notificate. Tale attività di approfondimento, resa più difficoltosa a causa della sospensione delle attività ispettive (cfr. par. 20.1), ha portato all'adozione di alcuni provvedimenti collegiali di tipo correttivo e, nei casi più gravi, sanzionatorio.

In merito, si segnalano un provvedimento sanzionatorio relativo ad un istituto bancario per violazione degli artt. 33 e 34 del RGPD (provv. 14 gennaio 2021,

18

Procedute IMI

n. 4, doc. web n. 9582744, cfr. Relazione 2020, p. 196); le attività svolte in occasione dell'incendio che ha coinvolto in Francia il fornitore *cloud* OVH e che, di conseguenza, ha riguardato numerose titolari italiani che usufruivano dei suoi servizi; quelle riguardanti numerose amministrazioni comunali, colpite in modo massivo da attacchi di tipo *ransomware.*

Nel corso del 2021 sono pervenute n. 67 notifiche di violazione di dati personali transfrontaliere da diverse autorità capofila, che corrispondono a 133 procedure IMI di diversa natura.

Nello specifico, le procedure IMI pervenute sono così suddivise: n. 56 procedure preliminari ex art. 56; n. 24 procedure di cooperazione informale ex art. 60, rispetto alle quali vi è stata una partecipazione dell'Autorità; n. 23 progetti di decisione (o revisione di decisione) ex art. 60; n. 21 decisioni finali in cui ha partecipato anche il Garante e n. 9 richieste di assistenza reciproca ex art. 61 (cfr. parte IV, tab. 10-12).

L'Autorità in un solo caso ha promosso una procedura preliminare ex art. 56, in quanto il titolare del trattamento, seppur con diverse sedi in UE, aveva il principale stabilimento in Italia. In questo caso, il Garante, dopo una complessa e lunga istruttoria, ha adottato una bozza di provvedimento, che è stata sottoposta nel 2021 all'attenzione delle altre autorità che si erano dichiarate interessate. La procedura è tuttora aperta.

19 Il trasferimento dei dati personali all'estero

Nel 2021 vi è stata un'intensa attività di cooperazione tra il Garante e le altre autorità di controllo europee nel settore dei trasferimenti di dati verso Paesi terzi.

In particolare, è proseguita la collaborazione con una *task force* (TF101) incaricata di coordinare l'esame di 101 reclami presentati nei confronti di diversi titolari del trattamento stabiliti negli Stati membri del See. I reclami, tutti dall'identico contenuto, contengono la richiesta alle autorità di pronunciarsi sulla legittimità dei trasferimenti dei dati personali verso gli USA, posti in essere da alcuni gestori di siti web, in conseguenza dell'utilizzo, tramite i loro siti internet, di Google Analytics, Facebook Pixel e Facebook Connect. Tutto ciò tenuto conto delle novità introdotte a seguito della pronuncia del 16 luglio 2020 della CGUE, cd. Schrems II (cfr. causa C-311/18) e dell'adozione dei documenti del Cepd, recanti raccomandazioni sulle misure volte a garantire, nel contesto dei trasferimenti transfrontalieri di dati, il rispetto del RGPD (EDPB, raccomandazioni 1/2020 e 2/2020, rispettivamente del 18 giugno 2021 e 10 novembre 2020).

La TF101 ha avviato un'attività di coordinamento delle istruttorie poste in essere a livello nazionale dalle singole autorità partecipanti e volta ad acquisire maggiori elementi in merito alle caratteristiche dei servizi resi da Google e Facebook nei casi di specie.

Con riguardo ai reclami riferiti a Google, le autorità hanno raggiunto una posizione comune in ordine alle valutazioni giuridiche da condividere ai fini delle decisioni da adottare a livello nazionale. Rispetto alle istanze riguardanti i servizi prestati da Facebook, resta tutt'ora in corso l'attività istruttoria del Garante, anche considerato che, nell'ambito della TF101, è stata valutata la necessità di effettuare ulteriori approfondimenti.

Con riferimento agli strumenti di trasferimento di cui all'art. 46 del RGPD ed in particolare alla recente adozione, da parte della Commissione europea, delle clausole tipo previste dalla decisione 4 giugno 2021 n. 2021/914, (cfr. par. 23.1), il Garante ha innanzitutto aggiornato le informazioni presenti sul sito istituzionale dell'Autorità; soprattutto in relazione alle decisioni di adeguatezza ed ai documenti di recente adozione da parte dell'EDPB e della Commissione europea (cfr. ad es. il documento dell'EDPB recante le *Guidelines 04/2021 on codes of conduct as tools for transfers* del 7 luglio 2021; la decisione n. 2021/914 sopra citata; la decisione della Commissione UE n. 2021/1773 inerente l'adeguata protezione dei dati personali da parte del Regno Unito).

Sono stati altresì forniti diversi chiarimenti in merito all'interpretazione ed applicazione del Capo V del RGPD.

In particolare, è stato rappresentato che le clausole tipo di recente adozione costituiscono un'importante novità nel panorama normativo delle garanzie adeguate ex art. 46 del RGPD ai fini dei trasferimenti di dati verso Paesi terzi, consentendo un approccio più flessibile e funzionale a trasferimenti che coinvolgono numerosi importatori ed esportatori nonché lunghe e complesse catene di trattamento. È stato sottolineato inoltre che le clausole tipo prevedono garanzie specifiche qualora la legislazione del Paese terzo incida sul rispetto delle clausole stesse, in particolare in caso di richieste di accesso da parte di autorità pubbliche in conformità alle indicazioni

19

fornite dalla CGUE nella summenzionata pronuncia Schrems II.

Sono stati altresì forniti chiarimenti sulle decisioni di adeguatezza adottate dalla Commissione ai sensi dell'art. 45 del RGPD quale idoneo presupposto ai fini del trasferimento, invitando i titolari e i responsabili ad effettuare una puntuale verifica del relativo ambito di applicazione ed è stata ribadita l'opportunità di individuare con attenzione i ruoli di *exporter* ed *importer* rivestiti dai soggetti di volta in volta coinvolti nel *data transfer* al fine di valutare, in relazione alle specifiche caratteristiche del trasferimento, la tipologia di strumento più idonea quale garanzia appropriata di cui all'art. 46 del RGPD (note 31 marzo e 25 ottobre 2021).

20 L'attività ispettiva

20.1. *L'attività ispettiva ai tempi della pandemia*

L'attività ispettiva svolge da sempre un ruolo di estrema delicatezza nell'ambito delle complesse funzioni di vigilanza e controllo affidate all'Autorità. In effetti, sia con le attività svolte nell'ambito di istruttorie già in corso, sia con le cosiddette attività di iniziativa volte ad un controllo su enti, società, ecc. in relazione ad ambiti di trattamento dei dati che appaiono di interesse, è possibile assicurare quella presenza diffusa del Garante sul territorio che contribuisce efficacemente ad aumentare e migliorare il recepimento delle disposizioni in materia di protezione dei dati personali.

Ciò, specie alla luce dei compiti delineati dal RGPD che, nel prefigurare, tra l'altro, un ampio apparato sanzionatorio, postula una puntuale ed efficace attività di controllo sull'azione di tutti i titolari del trattamento.

Da questo punto di vista, l'Autorità ha dovuto naturalmente confrontarsi, anche nel 2021, con i problemi connessi all'emergenza sanitaria in corso. Lo stato di emergenza ed i molteplici limiti posti agli spostamenti, unitamente alla necessità di evitare rischi al personale dell'Ufficio, ha ovviamente indotto nei primi mesi dell'anno a ridurre ai soli casi di estrema urgenza gli interventi *in loco.* L'Ufficio ha comunque "sfruttato" tutti gli spazi disponibili per la prosecuzione di tale attività (specie nei periodi di attenuazione dei contagi) e non ha mai mancato di provvedere alla redazione e all'esecuzione (seppur parziale) dei programmi ispettivi semestrali (contenuti nei provv.ti 22 luglio 2021, n. 286, doc. web n. 9689657 e 22 dicembre 2021, n. 452, doc. web n. 9737049).

Peraltro, nella prima parte dell'anno è stata sviluppata un'attività di controllo ispettivo da remoto con particolare riferimento alle ipotesi di trattamento dei dati svolti attraverso la raccolta di dati e informazioni a mezzo di siti web, anche per lo svolgimento di attività di *e-commerce.*

Alle verifiche iniziali sulla *homepage* dei siti allo scopo di controllare completezza e pertinenza delle informative e delle (eventuali e correlate) richieste di consenso, si è affiancata, nei casi in cui le verifiche preliminari avevano dato adito a dubbi, una successiva serie di approfondimenti tramite richieste di informazioni e contatti diretti con i responsabili dei siti, attività che hanno contribuito alla più completa trasparenza e aderenza dei siti medesimi al quadro normativo.

Non appena, a partire dall'autunno 2021, è stato possibile impiegare personale in condizioni di sicurezza si è comunque ripresa l'attività ispettiva *in loco,* cercando di intervenire tempestivamente nelle situazioni di particolare urgenza e delicatezza segnalate dai dipartimenti dell'area giuridica.

In questo contesto si sono inseriti gli interventi svolti presso alcune società in ordine al trattamento dei dati per finalità di *marketing* e profilazione, nonché in relazione alle ipotesi di acquisizione non corretta di nuovi rapporti contrattuali nel settore energetico, attraverso un trattamento dei dati svolto in modo spesso scorretto e addirittura illecito. Sono tutte fattispecie da tempo all'attenzione degli uffici, rispetto alle quali l'acquisizione sul campo di riscontri obiettivi, documentazione tecnica e ogni altro tipo di informazione permette ora di predisporre i relativi provvedimenti prescrittivi e/o sanzionatori.

20

20.2. *La collaborazione con la Guardia di finanza*

In questo quadro di attività si colloca la tradizionale collaborazione, che ha ormai una durata ventennale, fra il Garante ed il Corpo della Guardia di finanza. Collaborazione che ha trovato un rinnovato punto di riferimento nel nuovo Protocollo di intesa firmato il 31 marzo 2021 dal Presidente dell'Autorità e dal Comandante generale della Guardia di finanza. Si tratta di un documento che formalizza l'evoluzione dei rapporti fra Garante e Guardia di finanza avendo come faro la necessità di dotare l'Autorità di adeguati strumenti di intervento sul territorio con possibilità di svolgere in modo efficiente e tempestivo ogni attività di vigilanza e controllo, mettendo a frutto sia la competenza specialistica degli ispettori del Corpo, sia il valore aggiunto rappresentato dalla capillare articolazione territoriale del Corpo.

Il testo del nuovo Protocollo ha riposto un'attenzione particolare al contributo che potrà essere portato dalla componente tecnica presente nel Nucleo *privacy* e frodi tecnologiche costituito, nella sua unitarietà, da pochi anni e della quale l'Autorità ha già potuto beneficiare.

È diventata infatti modalità consueta di lavoro coinvolgere il Nucleo *privacy* in indagini conoscitive e in altre attività di studio, svolte anche *online,* al fine di acquisire elementi preliminari di valutazione funzionali all'individuazione e selezione delle categorie di soggetti da sottoporre ad un più approfondito intervento ispettivo.

In questa logica si collocano gli approfondimenti (cui ora stanno seguendo le ispezioni mirate *in loco*) relativi ai trattamenti di dati personali connessi all'utilizzo di applicazioni informatiche installate su apparecchi di telefonia mobile (specie quando associate a modalità occulte di trattamento dati, quali quelle effettuate a mezzo microfono).

Sono stati poi oggetto di attenzione (tuttora in corso) i meccanismi di verifica del cd. *green pass* diversi dalla *app* ufficiale del Governo Verifica C19.

Sono in corso di approfondimento anche i trattamenti dei dati svolti attraverso dispositivi (potenzialmente anche molto invasivi) connessi a giocattoli e ad altri tipi di oggetti di uso comune.

Negli ultimi mesi si è poi cercato di migliorare l'interazione fra uffici del Garante e Nucleo favorendo al massimo lo scambio di dati e di informazioni e la condivisione di prassi ed approcci istruttori. La complessità delle materie trattate dai vari dipartimenti giuridici richiede infatti che l'attività ispettiva delegata alla Guardia di finanza sia svolta con la profondità di conoscenze degli ambiti specifici, oggetto di intervento *in loco,* che l'attuale complessità del quadro regolatorio richiede. Per questo è ormai prassi abituale fare precedere l'inizio dei cicli ispettivi con incontri di formazione e preparazione presso gli uffici dell'Autorità.

Si è rivelato anche molto utile lo svolgimento di ispezioni con la presenza affiancata di ispettori del Nucleo e funzionari del Garante. Allo stesso modo si sta cercando di favorire l'osmosi fra informatici del Dipartimento tecnologie digitale e sicurezza informatica del Garante e ispettori del gruppo frodi tecnologiche della Guardia di finanza.

Va infine ricordato che, per consolidare ulteriormente le potenzialità di intervento del Garante, il nuovo Protocollo prevede che possano essere distaccati presso l'Autorità fino a 6 ispettori, collocati in posizione di fuori ruolo.

21 L'attività sanzionatoria del Garante

21.1. *Procedimenti ante Regolamento 2016/679*

Come è noto, dall'entrata in vigore del RGPD la competenza a comminare le sanzioni amministrative previste dal nuovo plesso normativo è stata trasferita in capo ai singoli dipartimenti dell'Ufficio del Garante, sicché delle sanzioni adottate si dà conto, per materia, nei diversi capitoli di questa Relazione. Per le procedure sanzionatorie adottate sulla base del previgente Codice permane una sorta di gestione stralcio.

Al riguardo occorre rammentare che l'art. 18, d.lgs. n. 101/2018 aveva previsto, per i procedimenti sanzionatori non ancora definiti alla data del 25 maggio 2018 un'alternativa: da una parte un meccanismo di definizione agevolata degli stessi attraverso la corresponsione di una somma di limitata entità (due quinti del minimo edittale); dall'altra, in assenza di tale pagamento, un meccanismo semplificatorio che attribuiva valore di ordinanza-ingiunzione all'atto di contestazione a suo tempo effettuato, senza obbligo di ulteriore notificazione, salvo che il contravventore presentasse tempestivamente nuove memorie difensive. In assenza di tali ulteriori memorie, il contravventore era tenuto a pagare per intero l'importo a suo tempo indicato, entro il 16 febbraio 2019.

Il meccanismo sopra evidenziato, concepito come una modalità per favorire, attraverso una significativa riduzione dell'importo della sanzione, la conclusione di molti procedimenti in corso da tempo, ha presentato alcune complessità di cui, in parte, si è dato conto anche nella Relazione dello scorso anno (cfr. Relazione 2020, p. 202). Sta di fatto che un numero relativamente limitato di interessati si è avvalso del beneficio del pagamento in misura ridotta o ha presentato nuove memorie difensive.

Di conseguenza l'Ufficio ha dovuto dare corso all'iscrizione a ruolo delle molte sanzioni rimaste pendenti e ora pervenute (*ex lege*) alla fase esecutiva.

Peraltro, questa fase ha subito ulteriori, imprevedibili slittamenti temporali per effetto dell'emergenza sanitaria. Nella prima fase dell'emergenza (iniziata nelle prime settimane del 2020) sono stati infatti adottati diversi provvedimenti di sospensione della notificazione delle cartelle esattoriali, poi più volte prorogati. Di fatto, questa situazione si è manifestata in modo molto evidente nel trascorso anno 2021 alimentando un flusso consistente di richieste e istanze di vario tipo (dalla mera richiesta di spiegazioni e di accesso ad atti e documenti più strutturati con cui si sollecitava l'Ufficio ad annullare sanzioni e iscrizioni a ruolo).

Su queste vicende è venuta recentemente a incidere la sentenza della Corte costituzionale 28 dicembre 2021, n. 260 che ha dichiarato l'illegittimità costituzionale dell'art. 18, comma 5, d.lgs. n. 101/2018, che aveva previsto l'interruzione dei termini di prescrizione per tutte le contestazioni adottate in materia di protezione dei dati personali non ancora definite alla data del 25 maggio 2018.

22 Il contenzioso giurisdizionale

22.1. *Considerazioni generali*

Tutte le controversie che riguardano l'applicazione della normativa in materia di protezione dei dati personali devono essere notificate al Garante, anche se non sono relative all'impugnazione di provvedimenti dell'Autorità (artt. 152 del Codice e 10, comma 6, d.lgs. n. 150/2011, come modificato dall'art. 17, d.lgs. n. 101/2018).

Gli effetti di tali disposizioni hanno inciso sul numero delle notifiche effettuate al Garante relative a tale tipologia di giudizi registrando al riguardo un andamento costante: a fronte dei 49 nel 2019 e dei 56 nel 2020, nel 2021 sono stati notificati all'Autorità e da questa trattati 58 ricorsi.

Permane comunque la rilevanza dell'obbligo per le cancellerie – purtroppo non sempre puntualmente adempiuto – di trasmettere al Garante copia dei provvedimenti emessi dall'Autorità giudiziaria in relazione alle previsioni del Codice e a quelle in materia di criminalità informatica (art. 154, comma 6, del Codice).

Fermo restando quanto si dirà al par. 22.4, tale strumento, unitamente alle notifiche dei ricorsi, consente all'Autorità di avere conoscenza dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e di segnalare al Parlamento e al Governo gli interventi normativi ritenuti necessari per la tutela dei diritti degli interessati.

22.2. *I profili procedurali*

In tema di incompetenza funzionale si sono avute cinque pronunce. In tre casi, è stata dichiarata inammissibile l'impugnazione in appello avverso le sentenze che confermavano i provvedimenti del Garante, in quanto ai sensi dell'art. 10, comma 10, d.lgs. n. 150/2011, avverso tali sentenze, si sarebbe dovuto proporre ricorso per cassazione e non appello (Corte di appello di Catanzaro, 13 ottobre 2021, n. 1345, Corte di appello di Roma 2 febbraio 2021, n. 702 e Corte di appello di Palermo, 30 aprile 2021, n. 723).

La Commissione tributaria di Viterbo ha dichiarato difetto di giurisdizione in relazione ad un ricorso presentato avverso una cartella di pagamento emessa dall'Agenzia delle entrate per la riscossione (Ader), nonché avverso il rispettivo ruolo emesso dal Garante, con cui si intimava il pagamento di somme quali sanzioni amministrative ex art. 162, comma 2-*bis,* del Codice *ante* riforma; ciò in virtù di quanto disposto dall' art. 152, comma 1, del medesimo Codice, secondo il quale le controversie che riguardano l'applicazione delle disposizioni in esso contenute sono attribuite all'Autorità giudiziaria ordinaria (Comm. trib. di Viterbo, 7 giugno 2021, n. 200). Per le medesime ragioni il Giudice di pace si è dichiarato incompetente per materia in relazione ad un ricorso proposto avverso cartella di pagamento, a seguito dell'iscrizione a ruolo di una sanzione amministrativa comminata al Garante (Giudice di pace di Milano, 21 gennaio 2021, n. 553).

Non si sono riscontrate pronunce che hanno dichiarato un difetto di competenza territoriale né per materia.

22

22.3. *Le opposizioni ai provvedimenti del Garante*

L'anno 2021 ha registrato un notevole decremento delle opposizioni a provvedimenti dell'Autorità: 115 a fronte dei 171 ricorsi del 2020. Tale variazione è dovuta essenzialmente alla diminuzione dei ricorsi proposti avverso cartelle esattoriali emesse ex art. 18, d.lgs. n. 101/2018: 27 rispetto alle 119 del 2020. Di seguito si dà conto delle sentenze di maggior rilievo.

Opposizioni a ordinanze-ingiunzioni

Complessivamente l'Autorità, ha avuto notizia di 86 decisioni dell'Autorità giudiziaria relative a opposizioni a provvedimenti del Garante (delle quali 55 relative a ordinanze-ingiunzioni, di cui 32 cartelle di pagamento), nei cui giudizi si è sempre costituita tramite l'Avvocatura dello Stato territorialmente competente.

Informativa e consenso

Due casi hanno avuto ad oggetto provvedimenti del Garante che hanno comminato la sanzione prevista dall'art. 161 del Codice previgente per aver intestato schede telefoniche a molteplici soggetti ignari, omettendo di rendere la prescritta informativa ai sensi dell'art. 13 del medesimo Codice.

Nel primo caso la Corte di cassazione, confermando la sentenza di primo grado del Tribunale di Milano del 2 dicembre 2016, n. 12576 ha respinto il ricorso della società ricorrente che obiettava di avere rivestito nella vicenda la mera posizione di responsabile, invocando l'accordo sottoscritto con il *master dealer* di un operatore telefonico. La Corte ha osservato che «In tema di protezione dei dati personali, affinché ricorra il fatto del "responsabile del trattamento", ai sensi dell'art. 4, lett. *g*) e dell'art. 29 del d.lgs. n. 196/2003, [….] in caso di preposizione di un soggetto al trattamento dei dati su incarico del "titolare", è necessario che l'effettivo trattamento dei dati da parte del preposto si svolga nell'osservanza delle istruzioni impartite dal "titolare", con la conseguenza che, ove non vi sia tale osservanza, il "responsabile" potrà essere riconosciuto come effettivo "titolare", responsabile in concreto del trattamento, in ragione dell'autonomia decisionale e gestionale manifestata nell'aver disatteso le disposizioni impartite dal "titolare"» (ord. 23 luglio 2021, n. 21234). È stata pertanto confermata l'ordinanza ingiunzione del Garante 13 maggio 2015, n. 293 (doc. web n. 4210697).

Nel secondo caso sempre la Corte di cassazione, con ordinanza 30 marzo 2021, n. 8769, ha respinto il ricorso proposto da una società avverso la sentenza di primo grado del Tribunale di Vicenza 28 febbraio 2017, n. 1040, respingendo tra le altre, l'eccezione della ricorrente circa la mancata pronuncia, da parte del giudice di primo grado, sull'invocata applicazione del cumulo giuridico di sanzioni (da cui sarebbe derivata una riduzione quantitativa della sanzione irrogata). La Corte ha osservato che, con riferimento alle violazioni in questione, deve ritenersi correttamente applicato da parte del Garante il criterio del cumulo materiale ai fini della quantificazione della sanzione in materia amministrativa, posto che le condotte illecite (consistite, ognuna, nell'utilizzazione di dati all'insaputa di singoli soggetti, omettendo di rendere le corrispondenti informative sulla *privacy*) si sono realizzate attraverso distinte azioni riguardanti diversi destinatari, ciascuna integrante una differente violazione amministrativa (ancorché della stessa natura e tipologia). Anche in questo caso è stata confermata l'ordinanza-ingiunzione in origine impugnata, 11 aprile 2013, n. 189 (doc. web n. 2601680).

Trattamento dei dati da parte di soggetti pubblici

In un altro caso una Asl aveva impugnato l'ordinanza-ingiunzione 5 luglio 2017, n. 308 (doc. web n. 6814717) con cui le era stata comminata la sanzione amministrativa pecuniaria prevista dagli artt. 164 e 162, comma 2-*bis* per la violazione degli artt. 157 e 19, comma 3, del Codice, per aver omesso di fornire al Garante le richieste di informazioni e per aver diffuso dati personali sul proprio sito web istituzionale in assenza di un idoneo presupposto normativo. In applicazione del divieto

22

di retroattività di cui all'art. 25 Cost., il Tribunale ha accolto l'opposizione limitatamente alla sanzione irrogata ai sensi dell'art. 162-*bis,* in relazione all'art. 19 comma 3, in quanto volta a sanzionare un fatto che nell'ordinamento giuridico ha perso il proprio carattere di illiceità, essendo state abrogate entrambe le norme dall'intervento riformatore del 2018.

Invece, pur avendo la riforma abrogato l'art. 164 del previgente Codice, ha tuttavia lasciato inalterata la fattispecie di cui all'art. 157, relativa ai poteri del Garante di richiedere al titolare, responsabile o interessato informazioni circa il trattamento dei dati, richiamandola nell'art. 166. Ritenendo per tale fattispecie persistente il disvalore oggettivo del fatto – sebbene ricondotto entro un ordinamento sanzionatorio formalmente differente e connotato da un coefficiente diverso di gravità, tale da non giustificare l'esenzione di punibilità di chi lo abbia commesso precedentemente alla intervenuta riforma – il Tribunale ha rigettato l'opposizione *in parte qua,* rideterminando la sanzione rispetto alla sola violazione dell'art. 157 (Trib. Catanzaro 21 maggio 2020, n. 659).

In altro caso un comune ha impugnato l'ordinanza-ingiunzione 22 febbraio 2018, n. 108 (doc. web n. 8997443), comminata per aver omesso di comunicare al Garante un caso di *data breach* in violazione dell'obbligo prescritto dal Garante alle p.a., ai sensi dell'art. 154, comma 1, lett. *c*), del Codice all'epoca vigente, con il provvedimento 2 luglio 2015, n. 393 (doc. web n. 4129029).

Nella sentenza adottata, il Tribunale di Civitavecchia si è soffermato sulle censure relative all'asserita violazione dei principi di riserva di legge e di tassatività, affermando che "la sussistenza di una riserva di legge in materia di sanzioni amministrative perfettamente coincidente a quella penale sotto il profilo dei contenuti e dei limiti non è affatto pacifica. Anzi, la giurisprudenza di legittimità è orientata in senso diverso". Più in particolare, secondo il Tribunale, anche qualora si volessero ritenere assimilabili le norme che irrogano sanzioni amministrative a quelle penali, attesa l'identità dello scopo punitivo, l'art. 162, comma 2-*ter,* del Codice non costituisce una norma sanzionatoria in bianco, essendo in sé completa, laddove prevede un obbligo, sia pure generico, di obbedienza, del quale il provvedimento costituisce semplice presupposto di fatto, che nulla aggiunge al contenuto sanzionatorio. Peraltro, lo stesso precetto sanzionatorio è integrato non già dal provvedimento, ma dalla norma primaria che lo prevede e alla quale l'art. 162, comma 2-*ter* rinvia ovvero dall'art. 154, comma 1, lett. *c*), del Codice. Né la disposizione in esame è censurabile sotto il profilo del rispetto del principio di tassatività nella descrizione della fattispecie rilevante.

Infine, il Tribunale ha affermato che le asserite difficoltà organizzative rappresentate dal comune ricorrente si configuravano quale mera circostanza di fatto, come tale del tutto inidonea a rilevare su un piano giuridico nel senso dell'esclusione della colpa che, per quanto riguarda la p.a., si configura quale cd. colpa d'apparato. Non è risultata, quindi, applicabile l'esimente della buona fede, prevista dall'art. 3 della l. n. 689/1981, essendo riservato al contravventore "l'onere di provare di aver agito incolpevolmente" (cfr. tra le tante, Cass. civ., sez. I 8 febbraio 2016, n. 2406; Cass. civ., sez. II 9 dicembre 2013, n. 27432; Cass. civ., sez. I, 7 settembre 2006, n. 19242) (Trib di Civitavecchia, 2 novembre 2021).

Ulteriori casi

Il Tribunale di Milano ha respinto l'opposizione proposta da una società avverso la cartella di pagamento emessa dall'Agenzia delle entrate per la riscossione della somma di cui all'ordinanza-ingiunzione 1° marzo 2018, n. 128 (doc. web n. 9026802), con cui è stata comminata la sanzione per la violazione dell'art. 157 del Codice, avendo omesso la società di fornire riscontro alle richieste di informazioni dell'Autorità. Pur avendo la società impugnato tempestivamente l'ordinanza-

ingiunzione, non essendo stata sospesa dal giudice titolare di tale processo, l'efficacia esecutiva della medesima ai sensi dell'art. 5, d.lgs. n. 150/2011, è rimasta efficace. Pertanto, secondo il Tribunale di Milano "la cartella esattoriale che è stata notificata all'attrice è stata emessa legittimamente in presenza di un idoneo titolo esecutivo (a prescindere da ogni considerazione sulla legittimità di tale atto che è di competenza del giudice del processo in cui lo stesso è stato impugnato)" (Trib. di Milano, 16 aprile 2021).

Opposizioni a provvedimenti

Complessivamente l'Autorità ha avuto notizia di 31 decisioni dell'Autorità giudiziaria relative a opposizioni a provvedimenti del Garante, nei cui giudizi si è sempre costituita tramite l'Avvocatura dello Stato territorialmente competente.

Cessione di una biobanca contenente informazioni genetiche e sullo stato di salute

Con ordinanza 7 ottobre 2021, n. 27325, la Suprema Corte ha accolto il ricorso proposto dal Garante avverso la sentenza del Tribunale di Cagliari 6 giugno 2017, n. 1569 che ha annullato il provvedimento del Garante di blocco del trattamento dei dati personali contenuti in una biobanca (provv. 6 ottobre 2016, n. 389, doc. web n. 5508051). La Suprema Corte ha riconosciuto che con il fallimento di una società, alla quale erano stati affidati originariamente i dati genetici degli interessati, ed il successivo acquisto della banca dati da parte di un'altra società, si era verificata una cessazione del trattamento originario e non la successione nel medesimo trattamento della società acquirente, con conseguente inizio di un nuovo trattamento ad opera del nuovo titolare, tenuto al rispetto della disciplina in materia di informativa e consenso (cfr. art. 16 Codice *ante* riforma). La Suprema Corte ha affermato, quindi, che "in tema di trattamento di dati personali sensibili, nella vigenza del Codice della *Privacy* (d.lgs. n. 196 del 30 giugno 2003) […] il titolare del trattamento dei dati che abbia acquisito i dati (o una banca dati) a seguito di cessione da altro titolare è tenuto ad informare gli interessati ai sensi dell'art. 13, comma 4, CP [Codice *Privacy*], a meno che la fattispecie non rientri nelle ipotesi in deroga previste dall'art. 13, comma 5, CP e la deroga sia fatta valere alle condizioni previste". Quanto alla questione dell'acquisizione del consenso ex artt. 23, 24 e 26 del Codice *ante* riforma, la Suprema Corte, nel richiamare la disciplina relativa anche ai dati genetici, ha affermato che "la cessione di dati o banche dati è consentita dall'art.16 del d.lgs. n. 196 del 2003; tuttavia la cessione dei dati ad un terzo, ed il conseguente mutamento soggettivo del titolare del trattamento, determina l'avvio di un nuovo trattamento, a sua volta soggetto alle disposizioni generali in tema di informativa e di consenso; in questo caso, il rinnovo dell'informativa e della raccolta del consenso può essere derogata, in misura più o meno ampia, solo ove ricorrano le specifiche condizioni previste dal codice della *privacy;* per quanto riguarda i "dati sensibili" e i "dati genetici", che costituiscono un sottoinsieme dei primi, la disciplina si connota di particolare rigore, temperato mediante il riconoscimento di poteri istruttori ed autorizzativi al Garante previsti dagli artt. 13, comma 5, 26, comma 4, 110, comma 1, CP - che non possono essere derogati, essendo volta ad assicurare lo svolgimento del trattamento ritenuto meritevole di tutela per le finalità perseguite, senza intaccare in maniera significativa i diritti degli interessati". Alla luce di tali disposizioni, si è quindi confermata, in linea generale, l'imprescindibilità del consenso informato al trattamento dei dati personali in caso di cessione di una banca dati genetica, laddove non ricorrano le deroghe previste dagli artt. 13, comma 5, 26, comma 4, e 110, comma 1, del Codice.

Giornalismo

Con ordinanza 24 dicembre 2020, n. 29584 la Suprema Corte ha respinto il ricorso proposto da una società editrice avverso la sentenza del Tribunale di Milano, che aveva confermato il provvedimento del Garante relativo all'illiceità del trattamento dei dati relativi ad un personaggio pubblico, realizzato attraverso la divulgazione della conversazione telefonica, via radio, tra il reclamante e un collaboratore

22

della trasmissione radiofonica che si presentò al suo interlocutore con l'identità e l'imitazione della voce di altro personaggio pubblico, al fine di raccogliere alcune informazioni confidenziali sulla sua possibile candidatura politica (provv. 11 settembre 2014, n. 400, doc. web n. 3405138). La Suprema Corte ha rigettato il ricorso proposto dalla società editrice della suddetta trasmissione radiofonica, riconoscendo natura sensibile al dato idoneo a rivelare le opinioni politiche dell'interessato (art. 4, comma 1, lett. *d*), del Codice *ante* riforma), tenuto conto che "le ragioni dell'attribuzione di "sensibilità" a un simile dato personale ha un fondamento costituzionale, essendo da rinvenire nell'esigenza di evitare trattamenti discriminatori dell'individuo per ragioni attinenti alle sue caratteristiche, condizioni o convinzioni, nel quadro di una rilettura in senso moderno del principio di eguaglianza (art. 3 Cost)". La Corte ha ricordato, altresì, che il trattamento dei dati personali per finalità giornalistiche può essere effettuato anche senza il consenso dell'interessato, ai sensi dell'art. 137, comma 2, del Codice "ma sempre nel rispetto delle modalità tese a garantire il rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato, del diritto all'identità personale, nonché del codice deontologico dei giornalisti, che ha valore di fonte normativa in quanto richiamato dal detto d.lgs. n. 196 del 2003, art. 139". In siffatti termini costituisce violazione dell'art. 2 del codice deontologico dei giornalisti, che vieta artifici e pressioni indebite nell'attività di raccolta delle notizie, la divulgazione di una conversazione ripresa con una telecamera nascosta dal giornalista all'insaputa del suo interlocutore (v. Cass. civ. n. 18006/2018). Lo stesso criterio di giudizio non può che valere, per identità di *ratio,* dinanzi a modalità altrettanto subdole di acquisizione dei dati informativi, come quelle insite nell'imitazione dell'identità personale altrui: segnatamente nell'imitazione, abilmente realizzata durante il corso di una telefonata, della voce di un soggetto che si trovi in rapporto privilegiato con l'interlocutore, allo scopo di ricevere informazioni private. La Corte ha affermato, inoltre, che il giornalista ha un duplice dovere: egli è tenuto a rendere note "la propria identità, la propria professione e le finalità della raccolta" delle notizie ed è pure tenuto a evitare "artifici e pressioni indebite". Se la prima condizione recede a fronte della possibilità accordata al giornalista di non rendere nota la finalità della raccolta dei dati personali quando "ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa", non recede invece la seconda, nel senso che "in ogni caso la funzione informativa non può essere invocata dinanzi ad artifici irrispettosi della dignità della persona. E a tal proposito è innegabile la differenza che corre tra il mero fatto di celare la propria identità e l'uso di metodi artificiosi come lo spacciarsi per un soggetto determinato, in grado di condurre l'interlocutore a manifestare opinioni personali o apprezzamenti indicativi del proprio orientamento politico che altrimenti non avrebbe fatto".

In analogia alla vicenda appena descritta il Tribunale di Milano, con sentenza 15 ottobre 2021, n. 8106, ha confermato la legittimità del provvedimento del Garante a seguito dell'opposizione al provvedimento 2 dicembre 2015, n. 631 (doc. web n. 4634594), con cui è stato dichiarato illecito il trattamento dei dati del reclamante in ragione delle modalità utilizzate – consistenti nel raccogliere telefonicamente dichiarazioni dello stesso con l'artificio della simulazione dell'identità di un personaggio pubblico e nel diffonderle successivamente nel corso di una trasmissione radiofonica e sul web – ed ha prescritto alla società ricorrente di astenersi dall'utilizzare le modalità indicate. Il Tribunale di Milano ha richiamato i principi sanciti dalla Suprema Corte nel 2020 (ordinanza n. 29584), affermando, inoltre, che quelle raccolte e registrate dalla società editrice sono informazioni personali fornite confidenzialmente, in ragione degli artifici e raggiri di cui sono vittime, dagli stessi soggetti dei quali viene in tal modo leso il diritto alla riservatezza; può anzi ragionevolmente

affermarsi che la natura diretta della fonte delle informazioni personali (e, cioè, gli stessi titolari dei dati), la natura confidenziale del rapporto sussistente tra la vittima ed il simulato interlocutore nonché l'impostazione fraudolenta delle conversazioni (dirette dolosamente a sollecitare il destinatario a rivelare informazioni e convinzioni personali) non possono che culminare di per sé in un trattamento illecito di dati personali (ed eventualmente anche nel trattamento di dati sensibili).

Sempre in tema di trattamento di dati personali per finalità giornalistiche, a seguito dell'impugnazione da parte di una società editrice del provvedimento 24 giugno 2020, n. 112 (doc. web n. 9471155), con cui il Garante aveva ammonito una testata giornalistica in relazione ad un articolo concernente un personaggio pubblico che consentiva l'identificazione dei propri figli (minori di età), nonché delle loro inclinazioni ideologiche e aspirazioni personali, il Tribunale di Milano, con la sentenza 8 settembre 2021, n. 3995 ha respinto il ricorso della società editrice, affermando che nome ed età costituiscono dato personale a mente dell'art. 4 del Codice. L'opinione riportata in ordine alla opportunità o meno di partecipare ad una manifestazione pubblica in favore della tutela dell'ambiente costituisce inoltre dato sensibile. Con riguardo a tale profilo, oggetto di specifica contestazione da parte della ricorrente, il Tribunale ha osservato che il contenuto delle espressioni letteralmente riportate dal giornalista evidenziava con lampante chiarezza l'opinione dei due giovani in ordine alla utilità della partecipazione ad una manifestazione, su un argomento che veniva da uno dei due definito "montatura mediatica". Ha sottolineato, inoltre, che "costituisce trattamento anche la sola replicazione di un dato già noto, facendo riferimento la disposizione a qualunque forma di comunicazione e diffusione del dato; in ogni caso, come sottolineato nel provvedimento del Garante, sono stati aggiunti ulteriori dati idonei ad identificare direttamente i minori". Peraltro, con riguardo ai dati riferiti a minori, il Tribunale ha rappresentato, altresì, che "la qualità di minore, infatti, richiede una particolare attenzione nella divulgazione del dato, e ciò indipendentemente dalle caratteristiche "divulgative" appartenenti alla figura genitoriale di riferimento. Sul punto si richiama la decisione della Suprema Corte (Cass. civ., sez. I, n. 27381/2013) che ben chiarisce che la preventiva divulgazione del dato da parte dell'esercente la responsabilità genitoriale non sia sufficiente a costituire la base giuridica della liceità del trattamento sia perché il minore potrebbe avere un diverso interesse sia perché il consenso potrebbe non essere sempre aggiornato. L'art. 7 del codice deontologico prescrive una indicazione chiara di garanzia dell'anonimato rispetto ai minori interessati da fatti di cronaca. Il principio è il precipitato dei principi affermati dalla Carta di Treviso, pure espressamente richiamata, e sottolinea la necessità di una attenta valutazione in ordine alla necessità di divulgazione del dato personale in tali casi. Sul punto si richiama il principio affermato da Cass. sez. 3, ordinanza 13 maggio 2020, n. 8880 (Rv. 657866 - 01) "La pubblicazione dell'immagine di un minore in scene di manifestazioni pubbliche (o anche private, ma di rilevanza sociale) o di altre iniziative collettive non pregiudizievoli, in assenza di consenso al trattamento validamente prestato, è legittima, in quanto aderente alle fattispecie normative di cui all'art. 97 della l. n. 633 del 1941, se l'immagine che ritrae il minore possa considerarsi del tutto casuale ed in nessun caso mirata a polarizzare l'attenzione sull'identità del medesimo e sulla sua riconoscibilità". Ciò considerato, il Tribunale ha ritenuto violato il principio della essenzialità della informazione rispetto a tali dati.

Con sentenza 23 novembre 2021, n. 9556 il Tribunale di Napoli ha confermato la legittimità del provvedimento 26 novembre 2020, n. 244 (doc. web n. 9523234), con cui il Garante ha disposto la misura dell'avvertimento in relazione alle modalità scelte dall'editore per escludere l'identificabilità di un soggetto, in evidente stato di

22

alterazione psico-fisica, ripreso mentre compie atti autolesionistici all'interno dei locali di un commissariato di polizia. Ha osservato, in particolare, che "il trattamento dei dati personali per finalità giornalistiche, che può essere effettuato anche senza il consenso dell'interessato, ai sensi dell'art. 137, comma 2, del d.lgs. n. 196 del 2003, deve pur sempre essere effettuato secondo modalità che garantiscano il rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato, del diritto all'identità personale, nonché del codice deontologico dei giornalisti, che ha valore di fonte normativa in quanto richiamato dall'art. 139 del detto d.lgs. n. 196 del 2003 (cfr. sez. 1, n. 18006/2018, Lamorgese, Rv. 649524-01)". In particolare per i profili che qui interessano, con riferimento alla diffusione dell'immagine degli interessati, la presenza delle condizioni legittimanti l'esercizio del diritto di cronaca non comporta di per sé solo la legittimità della pubblicazione o diffusione anche dell'immagine delle persone coinvolte che è subordinata, oltre che al rispetto delle prescrizioni contenute negli artt. 10 c.c., 96 e 97 della l. n. 633 del 1941, nonché dell'art. 137, d.lgs. n. 196/2003 e dell'art. 8 del codice deontologico dei giornalisti, anche alla verifica in concreto della sussistenza di uno specifico ed autonomo interesse pubblico alla conoscenza delle fattezze dei protagonisti della vicenda narrata, nell'ottica della essenzialità di tale divulgazione ai fini della completezza e correttezza della informazione fornita (cfr. Cass. civ. sez. I sent. 22 luglio 2015, n. 15360 - Rv. 636199). Nel caso di specie, pur essendo stato riconosciuto l'interesse alla notizia, per i motivi indicati non è risultato l'interesse pubblico alla conoscenza del soggetto coinvolto e da qui è stata confermata la legittimità del provvedimento adottato dal Garante.

Trattamenti per finalità di *marketing*

In un caso la Corte di cassazione (ordinanza 26 aprile 2021, n. 11019), ha posto fine ad una annosa controversia tra un operatore telefonico ed il Garante in ordine alla nozione di comunicazione a fini promozionali o di *marketing*. In particolare, la società ricorrente ha condotto una campagna, definita "recupero consenso", che ha riguardato ben 1.976.266 soggetti che non avevano fornito il loro consenso per finalità di *marketing* nelle forme di cui all'art. 130, comma 3, del Codice (versione previgente), o che avevano espressamente manifestato la volontà di non essere contattati a tali fini; ciò, allo scopo di acquisire il consenso al trattamento dei dati per finalità promozionali degli interessati precedentemente negato o non concesso, nell'intento di determinare un loro ripensamento.

Con provvedimento 22 giugno 2016, n. 275 (doc. web n. 5255159), il Garante ha vietato alla società ricorrente l'ulteriore utilizzo, per finalità commerciali, dei dati personali di terzi acquisiti con tale campagna, ritenendone illegittima l'acquisizione. La società ha impugnato il provvedimento del Garante sostenendo, in particolare, che la campagna "recupero consensi" non aveva finalità promozionali – non essendo diretta alla vendita di beni o servizi, ma solo al recupero del consenso mancante o negato, – onde non poteva ritenersi soggetta alle disposizioni del Codice circa le modalità di acquisizione del consenso per finalità di *marketing*.

Il Tribunale di Milano e, in via definitiva, la Cassazione, hanno rigettato le doglianze della società, accogliendo completamente le tesi difensive proposte dal Garante. La Cassazione ha riconosciuto che "una comunicazione telefonica finalizzata ad ottenere il consenso per fini di *marketing,* da chi l'abbia precedentemente negato, è essa stessa una comunicazione commerciale. La finalità alla quale è imprescindibilmente collegato il consenso richiesto per il trattamento non può non concorrere a qualificare il trattamento stesso, ragione per cui il trattamento dei dati dell'interessato per chiedere il consenso per fini di *marketing* è esso stesso un trattamento per finalità di *marketing*. […] La previsione del sistema dell'*opt-out* introdotto con l'art. 130 comma 3-*bis* del Codice, realizza – come osservato dal Garante nel controricorso – un equilibrato bilanciamento tra libertà d'impresa e tutela della riservatezza dei dati personali".

Diritto all'oblio

Il Tribunale di Milano ha rigettato il ricorso presentato dal ricorrente per l'annullamento del provvedimento del Garante 16 febbraio 2017, n. 66 (doc. web n. 6240230), che aveva respinto la sua istanza volta ad ottenere la rimozione da un noto motore di ricerca, di alcuni Url, tra cui quello relativo ad alcuni articoli pubblicati il 9 maggio 2002 ed il 24 settembre 2002, relativi ad una vicenda giudiziaria che lo aveva coinvolto.

I giudici milanesi hanno accolto la tesi difensiva del Garante, riconoscendo la persistenza, nonostante il tempo trascorso dall'accertamento dei fatti, dell'interesse alla diffusione delle notizie riportate nelle citate pubblicazioni, sia per la natura e gravità dei reati contestati (per i quali il ricorrente era stato condannato all'ergastolo, con sentenza divenuta definitiva nel 2004), sia per il fatto che gli esiti delle complessive vicende delittuose e giudiziarie in cui egli si è trovato coinvolto costituiscono tuttora una realtà con cui il ricorrente stesso si deve confrontare quotidianamente non soltanto nella propria dimensione privata, ma altresì nella propria dimensione pubblica, non avendo ancora ultimato l'*iter* di espiazione della complessiva pena inflittagli, trovandosi attualmente in regime di semilibertà (sentenza 20 luglio 2021, n. 4230).

In un'altra pronuncia è stato confermato il provvedimento del Garante 16 aprile 2020 ritenendo sussistente il diritto all'oblio nell'ipotesi in cui una rivista contenente immagini riguardanti il ricorrente sia stata legittimamente pubblicata e successivamente messa in vendita come oggetto da collezione su un sito di vendite e aste *online.* La successiva collocazione in vendita della stessa non è assimilabile ad una nuova pubblicazione o ad una rievocazione, fattispecie diverse rispetto alle quali, effettivamente, potrebbe porsi un problema circa l'attualità dei requisiti legittimanti di interesse alla diffusione (Trib. di Roma, 22 ottobre 2021).

Diritto di accesso degli eredi ai dati del *de cuius*

In un caso il Tribunale di Enna ha respinto il ricorso dell'erede avverso il provvedimento del Garante 16 febbraio 2021 volto a conoscere i beneficiari delle polizze assicurative espletate dal *de ciuis,* riaffermando l'importante principio, consolidato nell'orientamento del Garante, ma ancora oggetto di incertezze interpretative in parte della giurisprudenza di merito, secondo cui i dati personali di persone terze distinte dal *de cuius* non sono accessibili ai sensi della vigente normativa in materia di protezione dei dati personali. Il Tribunale siciliano ha in particolare affermato che "Secondo il Regolamento generale per la protezione dei dati personali, infatti, l'unico titolare dei diritti *privacy* è l'interessato, ossia il soggetto a cui si riferiscono i dati personali oggetto della richiesta. Al riguardo, gli artt. 13 comma 3, della legge n. 675 del 1996, 9 comma 3, del Codice ante-riforma e 2-*terdecies* del Codice vigente, laddove consentono l'esercizio dell'accesso ai dati nella titolarità dell'interessato-deceduto rappresentano, quindi, una deroga a questo principio generale, in quanto si ritiene meritevole di tutela chi agisce per "un interesse proprio" o "a tutela dell'interessato" oppure "per ragioni familiari meritevoli di protezione", per cui l'erede non ha un diritto proprio bensì ha titolo per esercitare i diritti del *de cuius,* ma non di acquisire dati personali di terzi diversi dall'interessato (ossia il defunto)" (30 settembre 2021 n. 426).

Ulteriori casi

La Corte di cassazione con ordinanza 25 maggio 2021 n. 14381 ha accolto l'appello proposto dall'Autorità avverso la sentenza del Tribunale di Roma del 4 aprile 2018, n. 5715. Con tale pronuncia, la Suprema Corte ha posto un importante principio di diritto con riferimento al consenso che eventuali interessati possono prestare per trattamenti preordinati all'elaborazione di profili reputazionali, incentrati su un sistema di calcolo basato su un algoritmo finalizzato a stabilire i punteggi di affidabilità. Secondo detto principio, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati.

22

La sentenza è stata quindi cassata, con assorbimento dei restanti motivi di ricorso e rinviata al medesimo Tribunale, in diversa composizione, che dovrà uniformarsi al sopra indicato principio di diritto. È stato, pertanto, confermato il provvedimento del Garante 24 novembre 2016, n. 488 (doc. web n. 5796783).

In altro caso il Tribunale di Roma ha dichiarato inammissibile l'opposizione proposta da una società che fornisce servizi di trasporto privato nei confronti del provvedimento 13 dicembre 2018, n. 498 (doc. web n. 9069046), con cui il Garante ha rilevato l'illiceità del trattamento posto in essere dalle società, riservandosi, con autonomo procedimento, di valutare la contestazione delle violazioni amministrative rilevate. Ciò, in quanto il provvedimento *de quo* non avrebbe natura di decisione giuridicamente vincolante ai sensi dell'art. 78 del RGPD. Tale natura nel procedimento sanzionatorio di cui ai commi 4, 5 e 6 dell'art. 166 del Codice, si può attribuire solo all'ordinanza-ingiunzione essendo l'opposizione all'ordinanza-ingiunzione, ai sensi dell'art. 22, l. n. 689/1981, "la sede propria deputata alla contestazione, dinanzi al giudice, di tutti gli elementi che hanno condotto all'irrogazione della sanzione" (sentenza 29 novembre 2021).

Una pronuncia ha respinto l'opposizione presentata dal ricorrente in relazione al provvedimento 25 luglio 2018 (adottato ai sensi dell'art. 11, reg. Garante n. 01/2019) con il quale il Garante aveva rigettato il reclamo avverso il trattamento da parte della società datrice di lavoro privata di dati contenuti in una sentenza di condanna pronunciata contro il ricorrente dal Tribunale di Milano. Il trattamento del dato giudiziario è stato ritenuto effettuato nell'esercizio del potere disciplinare del datore di lavoro e ai soli fini della gestione del rapporto di lavoro con lo scopo, da un lato, di esigere dal dipendente un comportamento rispettoso degli obblighi assunti e con l'obiettivo, dall'altro, di provvedere alla tutela di altra dipendente del medesimo datore di lavoro (persona offesa dalle condotte di *stalking* poste in essere dal ricorrente, secondo la sentenza di primo grado).

Il trattamento del dato giudiziario in questione è apparso dunque lecito, in quanto effettuato "per adempiere o esigere l'adempimento di specifici obblighi o eseguire specifici compiti previsti da leggi, dalla normativa dell'Unione europea, da regolamento o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro" (Trib. di Roma 17 novembre 2021, n. 16824).

22.4. *L'intervento del Garante nei giudizi relativi all'applicazione del Codice*

Come si è visto al paragrafo 22.1 il Codice prevede l'obbligo per le cancellerie di trasmettere al Garante copia dei provvedimenti emessi dall'Autorità giudiziaria in relazione a quanto previsto dallo stesso Codice o in materia di criminalità informatica (art. 154, comma 6).

Inoltre, in base al novellato art. 10, d.lgs. 1° settembre 2011, n. 150, l'Autorità giudiziaria deve comunicare al Garante la pendenza di una controversia, trasmettendo copia degli atti introduttivi (art. 10, comma 9, come modificato dall'art. 17, 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, ha limitato la propria attiva presenza ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari

questioni di diritto. 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 comunque informata sullo svolgimento delle vicende processuali e di ricevere comunicazione in merito agli esiti.

Al riguardo si consideri che la notifica al Garante dei ricorsi in materia di protezione dei dati personali che non riguardano provvedimenti dell'Autorità amplia la casistica di possibile intervento, anche in relazione a questioni di legittimità costituzionale o di compatibilità europea di leggi, anche con riferimento alla CDFUE, nonché alle norme di adeguamento al Regolamento, in relazione a disposizioni la cui difesa per conto della Presidenza del Consiglio dei ministri è affidata all'avvocatura erariale.

La legittimazione attiva dell'Autorità nei giudizi in cui non è parte ed il potere di intervento al fine di sostenere principi rilevanti nell'applicazione della disciplina in materia di protezione dei dati personali, sembrerebbero potersi desumere anche dall'art. 154-*ter* del Codice, nella parte in cui riconosce al Garante la legittimazione ad agire nei confronti del titolare o del responsabile del trattamento *tout court,* senza alcuna qualificazione, "in caso di violazione delle disposizioni in materia di protezione dei dati personali", quindi anche nei confronti dell'autorità pubblica.

Sono stati attribuiti a legali del libero foro incarichi di rappresentare in giudizio l'Autorità, in conformità al nuovo art. 154-*ter* del Codice che, attribuendo la rappresentanza in giudizio del Garante all'Avvocatura generale dello Stato ai sensi dell'art. 1, r.d. n. 1611/1933, prevede che, nei casi di conflitto di interesse, il Garante, sentito l'Avvocato generale dello Stato, può stare in giudizio tramite (propri funzionari iscritti nell'elenco speciale degli avvocati dipendenti di enti pubblici ovvero) avvocati del libero foro.

23 Le relazioni comunitarie e internazionali

Nel 2021, a fronte delle persistenti restrizioni imposte per contenere la diffusione da Covid-19, la maggior parte delle riunioni hanno continuato a svolgersi da remoto, ciò non solo non ha impedito la prosecuzione dei lavori dei diversi tavoli, europei ed internazionali di cui il Garante è parte, ma ha anzi portato all'incremento del numero delle riunioni svolte e consentito l'adozione di un rilevante numero di documenti ed iniziative.

Il tema della pandemia e del bilanciamento tra tutela della salute e altri diritti fondamentali ha via via lasciato spazio all'approfondimento di numerose altre questioni legate alla protezione dei dati e l'attività internazionale del Garante ha riguardato, quindi, molteplici materie e problematiche, anche oggetto di rinvio pregiudiziale alla CGUE.

23.1. *La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dei dati*

Nel corso dell'anno si sono svolte 15 riunioni plenarie, una delle quali in presenza (18 novembre), e 178 riunioni dei sottogruppi e delle *task force* che si occupano dell'applicazione del Regolamento e della direttiva *law enforcement* nei diversi settori.

È proseguita l'attività del Comitato volta ad armonizzare e chiarire l'interpretazione delle norme-chiave del RGPD attraverso l'elaborazione di specifiche linee guida.

Linee guida sulle limitazioni ai sensi dell'art. 23 del RGPD

Il 13 ottobre 2021 è stata adottata la versione finale delle linee guida 10/2020 sulle limitazioni dei diritti e degli obblighi previsti dal RGPD (v. Relazione 2020, p. 222), alla luce della consueta consultazione pubblica cui le linee guida del Comitato vengono sottoposte. La nuova versione specifica meglio i destinatari cui il documento si rivolge (titolari del trattamento, ma anche i legislatori che apportino eccezioni o restrizioni alle norme del RGPD) e aggiunge ulteriori esempi volti ad illustrare la linea interpretativa del Cepd.

Non mutano tuttavia i principi essenziali già espressi nella precedente versione, ovvero *in primis* che qualsiasi restrizione debba rispettare l'essenza del diritto oggetto di limitazioni, che non possano essere giustificate restrizioni estese e intrusive suscettibili di svuotare significativamente il diritto fondamentale alla protezione dei dati personali, che occorra garantire la sussistenza di specifici requisiti, quali in particolare l'accessibilità e la prevedibilità della normativa che introduca limitazioni ai diritti degli interessati, nonché il rispetto dei principi di necessità e proporzionalità.

Linee guida sulla nozione di titolare e responsabile

Anche le linee guida 7/2020 sulla nozione di titolare e responsabile sono state emendate a seguito di consultazione pubblica e adottate, nella versione finale, il 7 luglio 2021 (v. Relazione 2020, p. 222), senza mutare la sostanza del testo originario.

Riguardo alla nozione di titolare, emerge che se, in linea di principio, non vi è alcuna limitazione al tipo di entità che può assumere il ruolo di titolare del trattamento, in pratica è solitamente l'organizzazione in quanto tale e non un individuo al

suo interno ad agire come titolare. Il ruolo di titolare può essere definito dalla legge o derivare da un'analisi degli elementi di fatto o delle circostanze del caso. Non è invece necessario che il titolare del trattamento abbia effettivamente accesso ai dati oggetto di trattamento per essere qualificato come tale.

Il testo si sofferma anche sulla nozione di contitolarità, ravvisata in particolare quando il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti, ovvero il trattamento effettuato da ciascuna parte sia inseparabile, cioè inestricabilmente connesso a quello dell'altra.

Le linee guida sottolineano che per potersi qualificare come responsabile del trattamento, un soggetto deve essere un'entità separata rispetto al titolare del trattamento e trattare i dati per conto del medesimo titolare e secondo le sue istruzioni, pur entro un certo margine di discrezionalità e si soffermano sul rapporto tra titolare e responsabile, sull'affidabilità del responsabile di cui il titolare deve tenere conto ai fini della sua designazione, sugli elementi che devono sussistere nel contratto o altro atto giuridico che deve regolare i loro rapporti ai sensi dell'art. 28 del RGPD, nonché sui rapporti tra contitolari e i relativi accordi tra di essi.

Sempre in tema di rapporti tra titolare e responsabile del trattamento si segnala l'adozione, il 14 gennaio 2021, del parere congiunto Cepd/Gepd sul nuovo set di clausole contrattuali standard (CCS) tra titolare e responsabile ai sensi dell'art. 28 del RGPD e dell'art. 29 del regolamento UE 2018/1725, presentate dalla Commissione. Il parere, in via generale, dà un giudizio positivo sull'adozione di CCS come strumento forte di *accountability* volto a facilitare il rispetto – da parte di titolari e responsabili – degli obblighi previsti dal RGPD e dall'EUDP. Sottolinea inoltre che il fatto che le stesse CCS debbano applicarsi nel rapporto tra titolare e responsabile previsto dalle due normative, consente di fatto una maggiore armonizzazione e certezza giuridica a livello UE.

Cancellazione dei dati e poteri delle autorità

Su richiesta dell'Autorità ungherese, il Cepd ha inoltre adottato un parere, ai sensi dell'art. 64, par. 2, del RGPD, in merito all'interpretazione dell'art. 58, par. 2, lett. *g*), che annovera tra i poteri correttivi della autorità di protezione dati quello di ordinare la cancellazione dei dati personali in base all'art. 17 (parere 39/2021). In tale occasione, il Comitato ha affermato che l'art. 58, par. 2, lett. *g*), consente alle autorità di protezione dei dati di ordinare la cancellazione dei dati personali trattati illecitamente anche d'ufficio, atteso che gli interessati potrebbero non essere a conoscenza del trattamento o non aver presentato alcuna richiesta di cancellazione (v. art. 17 del RGPD).

È proseguito il lavoro di aggiornamento del parere 6/2014 del Gruppo Art. 29 sulla nozione di legittimo interesse al fine di elaborare nuove linee guida sull'interpretazione dell'art. 6, par. 1, lett. *f*), del RGPD. È stata inoltre avviata la discussione sull'interpretazione delle previsioni normative del RGPD in materia di minori ai fini della predisposizione di specifiche linee guida.

Linee guida sulla composizione delle controversie ex art. 65 par. 1 lett. *a*), del RGPD

Il Comitato ha inoltre proseguito la sua attività di interpretazione delle norme concernenti i meccanismi di cooperazione tra le autorità di protezione dati previsti dal Capo VII del RGPD con l'adozione delle linee guida 3/2021 sull'applicazione dell'art. 65, par. 1, lett. *a*), del RGPD (16 aprile 2021). Tali linee guida concernono in un meccanismo volto a risolvere opinioni contrastanti tra le autorità nei casi di trattamento transfrontaliero di dati personali. In particolare esse chiariscono l'applicazione delle pertinenti disposizioni del RGPD e delle regole procedurali del Cepd, delineano le fasi principali della procedura, definiscono la competenza del Comitato ove adotti una decisione giuridicamente vincolante sulla base dell'art. 65, par. 1, lett. *a*), ed includono una descrizione delle garanzie procedurali e dei rimedi a disposizione dei soggetti interessati dalla decisione.

Linee guida 9/2020 sull'obiezione pertinente e motivata

Il lavoro del Cepd volto a chiarire i meccanismi di composizione delle controversie previste dal Regolamento si è esteso anche al concetto di obiezione pertinente e motivata oggetto delle linee guida 9/2020 adottate, nella versione successiva alla consultazione pubblica, il 9 marzo 2021.

La prospettiva da cui muove il Comitato è che le autorità di controllo coinvolte (capofila e interessate) dovrebbero adoperarsi il più possibile per giungere ad un progetto di decisione consensuale anche attraverso un congruo scambio di informazioni. L'obiezione dovrebbe essere considerata come soluzione di ultima istanza per porre rimedio alle presunte carenze in termini di coinvolgimento delle autorità di controllo interessate da parte dell'autorità di controllo capofila nella procedura, anche con riferimento all'analisi giuridica effettuata e all'ambito delle indagini svolte dall'autorità capofila sul caso in questione. I due requisiti, motivata e pertinente, devono essere considerati cumulativi, pertanto, l'art. 60, par. 4, impone all'autorità di controllo capofila di sottoporre la questione al meccanismo di coerenza del Cepd se ritiene che l'obiezione non soddisfi anche solo uno dei due requisiti.

Meccanismo di cooperazione e coerenza

È proseguita inoltre l'attività volta a sostenere il funzionamento efficiente del meccanismo di cooperazione e coerenza attraverso cui tutte le autorità di controllo collaborano per applicare in modo coerente e armonizzato il RGPD. Al riguardo, su richiesta della Commissione per le libertà civili, la giustizia e gli affari interni (commissione LIBE) del Parlamento europeo, come già in passato (cfr. Relazione 2019, p. 184), il 5 agosto 2021 il Cepd ha raccolto un'ampia serie di informazioni e statistiche sulle attività svolte dalle autorità di protezione dei dati nell'ambito del meccanismo di *One stop shop* e sulle risorse messe a disposizione delle stesse da ciascuno Stato membro.

Il 12 luglio 2021, il Cepd ha adottato la sua prima decisione vincolante d'urgenza ai sensi dell'art. 66, par. 2, del RGPD (decisione 1/2021), a seguito di una richiesta dell'Autorità di controllo di Amburgo che il 10 maggio 2021, con misura urgente avente validità di tre mesi, aveva vietato a Facebook Ireland Ltd di trattare, per finalità proprie, i dati degli utenti di Whatsapp residenti in Germania, a seguito delle modifiche dei termini di servizio e *privacy policy* notificate agli stessi da Whatsapp Ireland Ltd. Nella sua argomentata decisione, il Cepd ha ritenuto di non essere in possesso di tutti gli elementi informativi necessari per trarre conclusioni circa la sussistenza o meno di violazioni del RGPD e adottare una misura di urgenza ai sensi dell'art. 66, par. 8, del RGPD; tuttavia ha chiesto all'Autorità irlandese, in qualità di autorità capofila, di valutare attentamente i trattamenti posti in essere dalle due società, con specifico riguardo ai rispettivi ruoli, nell'ambito di una procedura di cooperazione con le altre autorità interessate.

Il 28 luglio 2021, l'EDPB ha adottato la sua seconda decisione vincolante ai sensi dell'art. 65 del RGPD (per la prima, su un *data breach* che ha coinvolto Twitter *international,* cfr. Relazione 2020, p. 223). Tale decisione verte su un progetto di decisione predisposto dall'Autorità di controllo irlandese, in qualità di autorità capofila, in merito al rispetto da parte di Whatsapp Ireland Ltd degli obblighi di trasparenza di cui agli artt. 12, 13 e 14 del RGPD sui quali una serie di autorità di controllo interessate avevano espresso diverse obiezioni. Il Comitato ha rilevato ulteriori violazioni rispetto a quelle già individuate dall'autorità capofila e ha fornito indicazioni rilevanti sul tema delle sanzioni: in primo luogo per il calcolo della sanzione ha ritenuto che deve essere considerato il fatturato consolidato della società madre, Facebook Inc.; in secondo luogo, si è espresso in ordine all'interpretazione dell'art. 83, par. 3, del RGPD, a norma del quale, nel caso di infrazioni multiple per lo stesso trattamento o per operazioni di trattamento collegate, tutte le infrazioni

dovrebbero essere prese in considerazione per il calcolo dell'importo della sanzione (e ciò nonostante l'obbligo per le autorità di controllo di tenere conto della proporzionalità della sanzione e di rispettare l'importo massimo della stessa stabilito dal Regolamento) (cfr. par. 13.6).

L'obiettivo delle linee guida in tema è quello di individuare riferimenti comuni, per calcolare l'ammontare delle sanzioni amministrative, tenuto conto dei fattori aggravanti ed attenuanti eventualmente rilevanti nei singoli casi.

Trasferimento dei dati all'estero e nuove clausole contrattuali standard

Il 4 giugno 2021 la Commissione europea ha adottato la decisione di esecuzione 2021/914 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso Paesi terzi a norma del RGPD. Si tratta del primo nuovo strumento per il trasferimento dei dati messo a disposizione degli operatori dopo l'entrata in vigore del Regolamento utilizzabile da titolari e responsabili quando il trattamento da parte dell'importatore non rientra nell'ambito di applicazione del RGPD. Le clausole riprendono, per quanto possibile, le precedenti – la cui validità, come noto, è stata confermata dalla sentenza della CGUE Schrems II (causa C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems) – ampliandone l'ambito di applicazione attraverso la previsione di quattro (e non più due) differenti set: titolare-titolare; titolare-responsabile; responsabile-sub-responsabile; responsabile-titolare. L'utilizzo delle nuove clausole è obbligatorio per i contratti stipulati dopo il 27 settembre 2021 mentre i contratti stipulati prima di tale data, sulla base delle precedenti decisioni 2001/497/CE e 2010/87/UE, sono tenuti a fornire garanzie adeguate ai sensi dell'art. 46, par. 1, del RGPD fino al 27 dicembre 2022, purché i trattamenti oggetto dei contratti rimangano invariati e il trasferimento di dati personali sia soggetto a garanzie adeguate.

In sede di definizione delle clausole, la Commissione ha tenuto conto del parere congiunto 2/2021, adottato il 14 gennaio 2021, con il quale il Comitato e il Garante europeo hanno fornito specifiche indicazioni sull'originaria proposta di clausole presentata il 12 novembre 2020. In particolare, il parere ha suggerito di chiarire l'ambito di applicazione delle nuove clausole standard, taluni diritti dei terzi beneficiari, taluni obblighi relativi ai trasferimenti successivi e aspetti della valutazione della legislazione dei Paesi terzi, soprattutto per quanto riguarda l'accesso ai dati trasferiti da parte delle autorità pubbliche di tali Paesi. A questo riguardo, il Comitato e il Gepd hanno sottolineato l'importanza di valutare attentamente la legislazione del Paese terzo al fine di decidere in ordine all'adozione, ove necessario, di misure supplementari *ad hoc* che consentano agli importatori di rispettare gli obblighi assunti con la sottoscrizione delle clausole e garantire quindi, in concreto, agli interessati un livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'UE. Il parere ricorda che strumento essenziale per aiutare gli operatori in questa analisi sono le raccomandazioni del Comitato 1/2020 sulle misure supplementari.

Trasferimenti dei dati all'estero e misure supplementari

Quasi in concomitanza con la pubblicazione della menzionata decisione di esecuzione 2021/914 (v. *supra*), il Comitato ha adottato, il 18 giugno 2021, a seguito di consultazione pubblica avviata a novembre 2020, la versione definitiva delle raccomandazioni 1/2020 sulle misure supplementari. Il documento mira ad assistere i titolari e i responsabili del trattamento in qualità di esportatori (siano essi enti privati o pubblici) nella valutazione della legislazione del Paese terzo applicabile al trasferimento da porre in essere al fine di individuare, ove necessario, le misure supplementari appropriate da adottare per consentire il rispetto delle garanzie contenute nello strumento di trasferimento prescelto.

Tra le modifiche apportate alle raccomandazioni – a seguito dei numerosi contributi (quasi duecento) pervenuti – le principali mirano a chiarire: l'importanza di esaminare, oltre alla legislazione, anche le pratiche relative agli accessi da parte delle

23

autorità pubbliche dei Paesi terzi in cui si intende trasferire i dati al fine di valutare se tale legislazione e/o tali pratiche incidano in concreto sull'efficacia dello strumento di trasferimento prescelto; la possibilità che l'esportatore consideri l'esperienza dell'importatore (insieme a informazioni oggettive e accessibili al pubblico provenienti dalla giurisprudenza, dai parlamenti, dagli organi di controllo, dalle Ong e dall'esperienza pratica di altre entità che si trovano in situazioni analoghe a quella dell'importatore); la necessità di documentare la valutazione effettuata e lasciare la documentazione a disposizione delle autorità di protezione dei dati. Le raccomandazioni precisano altresì che anche una legislazione del Paese terzo di destinazione che consenta alle sue autorità governative di accedere ai dati trasferiti senza l'intervento dell'importatore, in particolare sui dati in transito, può incidere sull'efficacia dello strumento di trasferimento e comportare l'adozione di idonee misure supplementari.

Le decisioni di adeguatezza del Regno Unito e Corea del Sud

Nel 2021 il Comitato ha fornito i propri pareri in merito alle proposte di decisione della Commissione sull'adeguatezza della protezione offerta dal Regno Unito, rispettivamente ai sensi dell'artt. 45 del RGPD e 36 della direttiva 2016/680 (pareri 14/2021 e 15/2021) e dalla Corea del Sud (parere 32/2021).

Mentre il parere 15/2021 analizza, per la prima volta, il progetto di decisione di adeguatezza di un Paese terzo nell'ambito dei settori disciplinati dalla direttiva 680/2016 (v. *infra*), il parere 14/2021 si basa sul Regolamento e valuta sia gli aspetti generali in materia di protezione dei dati sia l'accesso da parte dei soggetti pubblici ai dati personali trasferiti dall'UE. Più in particolare, questo, nel rilevare che vi sono aree di forte allineamento tra i quadri di protezione dei dati dell'UE e del Regno Unito, si sofferma su alcuni aspetti critici, richiamando l'attenzione sui trasferimenti ulteriori effettuabili sulla base di future decisioni di adeguatezza rese dalle Autorità britanniche a Paesi che non siano ancora (o più) considerati adeguati dall'UE o da accordi internazionali che non contengano garanzie tali da assicurare ai dati trasferiti nel Regno Unito dall'UE un adeguato livello di protezione nel Paese terzo di (ulteriore) destinazione. Il parere invita inoltre la Commissione a monitorare l'applicazione dell'eccezione legata alla tutela delle frontiere che consente restrizioni ai diritti dell'interessato, nonché gli sviluppi futuri della disciplina britannica al fine di verificare la persistenza dell'attuale allineamento, tenuto conto, in particolare, delle dichiarazioni più volte rese dal governo britannico in ordine all'intenzione di discostarsi dalla disciplina europea di protezione dei dati.

A seguito dei pareri ricevuti e a conclusione della procedura di cui all'art. 93, par. 3, del RGPD, la Commissione ha quindi adottato, il 28 giugno 2021, le due decisioni di esecuzione relative all'adeguatezza per il Regno Unito, essenziali anche per la corretta attuazione dell'accordo sugli scambi e la cooperazione tra l'UE e l'ex Paese UE. In merito al rischio di future divergenze tra i due ordinamenti, entrambe le decisioni prevedono una *sunset clause* che limita la durata dell'efficacia della decisione di adeguatezza a quattro anni.

A pochi mesi di distanza, il 17 dicembre 2021, la Commissione ha anche concluso la procedura di adozione della decisione di adeguatezza della Repubblica di Corea, avviata il 16 giugno con la pubblicazione e l'inoltro al Comitato della sua proposta. Il Comitato si è espresso sulla proposta di decisione con il parere 32/2021, analizzando la legislazione coreana in materia di protezione dei dati personali (PIPA) e gli aspetti legati agli accessi ai dati trasferiti da parte di soggetti pubblici nel Paese terzo per finalità di *law enforcement* e sicurezza nazionale. Il parere ha individuato diversi elementi di affinità delle legislazioni (in particolare con riferimento alle definizioni e ai principi di protezione dei dati) e ha accolto con favore gli sforzi compiuti dalla Commissione europea e dalle autorità coreane per avvicinare i quadri normativi (nella specie l'adozione delle protezioni aggiuntive previste dalla notifica

n. 2021-1 adottata dall'Autorità di protezione dei dati della Corea del Sud (PIPC), che mirano a colmare il divario tra le due legislazioni in materia di protezione dei dati). Proprio alla luce dell'importanza di tale notifica, il Comitato ha invitato la Commissione a monitorare attentamente sulla sua natura vincolante, effettiva applicabilità e validità così come su altre possibili criticità legate, in particolare, alle deroghe nell'applicazione delle norme di protezione dei dati nei casi in cui gli stessi siano pseudonimizzati e trattati per finalità di ricerca scientifica, statistica e archiviazione nel pubblico interesse nonché all'utilizzo del consenso come strumento "principe" per il trasferimento ulteriore dei dati.

Trasferimenti di dati tra soggetti pubblici o ad organizzazioni internazionali

Dopo l'adozione definitiva delle linee guida per il trasferimento di dati a soggetti pubblici nei Paesi terzi o ad organizzazioni internazionali (linee guida 2/2020), il Comitato è tornato sul tema del trasferimento di dati tra i soggetti pubblici (v. al riguardo anche parr. 4.9 e 4.9.1) con un parere ai sensi dell'art. 64, par. 2, del RGPD (parere 5/2021), richiesto dall'Autorità di protezione dei dati francese, sulla bozza di accordo per il trasferimento di dati tra l'autorità di controllo sui revisori dei conti francese (H3C) e l'omologo organismo statunitense PCAOB. Il parere riconosce che la bozza di accordo proposta contiene garanzie adeguate ai sensi dell'art. 46 par. 3, lett. *b*), del RGPD e può quindi essere autorizzata dall'autorità di protezione dei dati competente e precisa che il progetto di accordo potrebbe essere considerato da altre autorità di *audit* dello Spazio economico europeo come un modello da seguire per lo stesso tipo di trasferimenti di dati personali al PCAOB: in tal caso, gli accordi dovranno essere sottoposti all'autorità di controllo competente per la necessaria autorizzazione ma il Comitato non avrebbe necessità di esprimersi tenuto conto che il parere verterebbe sulla medesima questione già affrontata.

Sempre in tema di trasferimenti tra soggetti pubblici, il Comitato il 13 aprile, con uno *statement,* ha invitato gli Stati membri ad avviare il lavoro per rivedere gli accordi internazionali che prevedono trasferimenti di dati personali in vigore al momento dell'applicazione del Regolamento e della *law enforcement directive* (LED) (v. *infra*). Tali accordi, seppure validi alla luce degli artt. 96 del RGPD e 61 LED, dovrebbero essere rivisti e resi conformi al nuovo quadro normativo posto in essere dal RGPD (e, appunto, alle nuove linee guida sui trasferimenti di dati tra soggetti pubblici) e alla direttiva 680/2016. Tra essi, lo *statement* ricorda gli accordi in materia di scambio di informazioni finanziarie (CRS e FATCA) e quelli in materia di sicurezza sociale.

Codici di condotta come strumenti di trasferimento dei dati

Tra le novità introdotte dal RGPD in materia di trasferimenti di dati all'estero c'è la previsione dei codici di condotta come strumenti di trasferimento dei dati all'estero (artt. 40, par. 3 e 46, par. 2, lett. *e*), del RGPD). Il 7 luglio 2021 il Comitato ha adottato le linee guida 4/2021, avviando contestualmente una consultazione pubblica. Tali linee guida – che integrano quelle 1/2019 del Comitato – contengono indicazioni relative: all'ambito di applicazione dei codici di condotta; alle condizioni necessarie per il loro utilizzo da parte di titolari e responsabili in Paesi terzi che non ricadano nell'ambito di applicazione del RGPD ai sensi dell'art. 3, par. 2; alle garanzie necessarie (diritti per gli interessati, principi di protezione dei dati contenuti nel RGPD, misure di *accountability* poste in essere, ecc.) e alle modalità attraverso le quali titolari o responsabili del trattamento nel Paese terzo possano assicurare il proprio impegno vincolante ed esecutivo ad applicare le garanzie contenute nel codice di condotta cui aderiscono.

***Interplay* tra art. 3 e Capo V del RGPD**

Dopo lunga gestazione, nel novembre 2021, il Comitato ha adottato le linee guida 5/2021 che mirano a chiarire l'interazione tra l'ambito di applicazione territoriale del RGPD (art. 3) e le disposizioni sui trasferimenti internazionali di cui al

23

Capo V, nell'intento di assistere i titolari e i responsabili del trattamento nell'UE nel determinare se un trattamento costituisca un trasferimento internazionale di dati. A questo scopo, le linee guida – sottoposte a consultazione pubblica – specificano che il trattamento sarà considerato un trasferimento indipendentemente dal fatto che l'importatore stabilito in un Paese terzo sia già soggetto al Regolamento ai sensi dell'art. 3, par. 2, del RGPD. Alla luce della peculiare situazione che caratterizza tali titolari/responsabili quando agiscono quali importatori, le linee guida evidenziano anche la necessità di individuare strumenti che consentano il trasferimento dei dati in questione tenuto conto che le nuove clausole contrattuali standard della Commissione (SCC) non si applicano in tali casi e che apposite garanzie dovrebbero essere individuate per coprire i rischi di siffatto trasferimento senza dover duplicare gli obblighi cui tali importatori sono già soggetti per via della diretta applicazione del RGPD (in particolare, i rischi che derivano da eventuali conflitti di leggi con il Paese terzo in cui l'importatore è stabilito e alle richieste di accesso da parte di autorità pubbliche del Paese terzo).

Le linee guida precisano inoltre che specifiche misure devono comunque essere adottate nel caso in cui il trattamento sia effettuato da un titolare ex art. 3, par. 1, del RGPD direttamente fuori dal territorio dell'Unione: il titolare infatti, nell'adempiere agli obblighi previsti dal RGPD, in particolare quelli previsti agli artt. 24, 32, 33, 35, 48 del RGPD, deve tenere in debito conto i rischi del suo operare fuori dal territorio UE e adottare le conseguenti misure per assicurarne il pieno rispetto.

Bcr

Diciannove sono state le regole vincolanti di impresa (*Binding corporate rules,* di seguito Bcr) approvate dalle autorità di protezione dei dati competenti (cd. *Bcr Lead* individuate sulla scorta dei criteri indicati nel WP 263 rev. 01: v. Relazione 2018, p. 190) nel 2021, dopo l'adozione del parere da parte del Comitato in merito a ciascun progetto di decisione presentato ai sensi dell'art. 64, par.1, lett. *f*), del RGPD (più in particolare, 12 pareri sono stati relativi all'approvazione di Bcr per titolari e 7 in merito a Bcr per responsabili). I pareri, così come le conseguenti decisioni di approvazione delle Bcr, accertano che le garanzie in esse contenute offrano un livello adeguato di tutela alla luce degli elementi richiesti dall'art. 47 del RGPD e dei documenti di lavoro relativi alle Bcr per titolari e per responsabili (WP 256, rev. 01, e WP 257, rev. 01: cfr. Relazione 2017, p. 167). Nonostante l'approvazione delle Bcr, è necessario quindi che ciascuna impresa appartenente al gruppo interessato, prima di sottoscrivere le Bcr e costantemente nel corso del loro utilizzo, verifichi di poter rispettare le garanzie ivi previste tenuto conto delle specificità di ciascun trasferimento e del Paese terzo in cui è stabilita la società del gruppo che agisce in qualità di importatore. Ove infatti il quadro normativo applicabile non consenta all'importatore di rispettare gli impegni assunti con l'adesione alle Bcr, l'esportatore dovrà – come nel caso di ogni altro tipo di strumento per il trasferimento – porre in essere misure supplementari che gli consentano di rispettare tali impegni (v., al riguardo, *supra,* le raccomandazioni 1/2020) o astenersi dal trasferire i dati.

Requisiti per l'accreditamento degli organismi di certificazione

Il Comitato si è altresì occupato di assicurare 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. L'accreditamento dell'organismo di monitoraggio costituisce una condizione necessaria per l'approvazione di un codice di condotta, con la sola eccezione del trattamento effettuato da autorità pubbliche e da organismi pubblici per il quale non è necessaria l'istituzione di tale organismo. 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

23

autorità di controllo competente in linea con il parere espresso dal Cepd, in ottemperanza al meccanismo di coerenza. Nel corso dell'anno, il Comitato si è espresso in particolare sui progetti dei requisiti di accreditamento presentati dall'Autorità di controllo ungherese (parere 10/2021), norvegese (parere 11/2021), ceca (parere 23/2021), slovacca (parere 24/2021) e maltese (parere 37/2021).

I primi codici di condotta europei

Secondo il RGPD, l'adesione a codici di condotta approvati può essere utilizzata come elemento per dimostrare la conformità alle sue disposizioni. In tale ambito, il Cepd ha adottato due pareri ai sensi dell'art. 64 del RGPD sui primi due progetti di decisione riguardanti codici di condotta relativi ad attività di trattamento in diversi Stati membri (cfr. pareri 16/2021 e 17/2021 del 19 maggio 2021). Si tratta del progetto di decisione dell'Autorità di controllo belga in merito al codice di condotta europeo EU CLOUD, predisposto da Scope Europe e del progetto di decisione dell'Autorità di controllo francese in merito al codice di condotta europeo predisposto dal CISPE (*Cloud Infrastructure Service Providers*). Entrambi i codici mirano a fornire orientamenti pratici e a fissare requisiti specifici (alla luce dell'art. 28 del RGPD) per i responsabili del trattamento che forniscono servizi *cloud* nell'UE, ma non sono utilizzabili come strumenti di trasferimento di dati personali all'estero. Accogliendo con favore gli sforzi compiuti dai proponenti, il Comitato ha considerato che i predetti codici sono conformi al RGPD e soddisfano i requisiti di cui agli artt. 40 e 41 di quest'ultimo.

Requisiti per l'accreditamento degli organismi di monitoraggio di codici di condotta

Altrettanto importante è stata l'attività del Cepd volta ad assicurare la coerenza nell'applicazione del RGPD con riferimento alla definizione dei requisiti di accreditamento degli organismi di certificazione da parte delle autorità di controllo competenti ai sensi dell'art. 43, par. 3, del RGPD. In base alle linee guida del Cepd 4/2018 sull'accreditamento degli organismi di certificazione, tali requisiti dovrebbero basarsi sulla norma tecnica internazionale EN-ISO/IEC 17065:2012 ed essere integrati dai requisiti aggiuntivi stabiliti dalle autorità di controllo nazionali (v. art. 43, par. 1, lett. *b*), del RGPD), in linea con il parere espresso dal Cepd in ottemperanza al meccanismo di coerenza. Nel definire i requisiti aggiuntivi, le autorità di controllo si avvalgono del modello comune definito dal Cepd in allegato alle linee guida 4/2018. In tale contesto, nel 2021, il Comitato ha reso il parere previsto dall'art. 64, par. 1, lett. *c*), del RGPD in ordine ai progetti di requisiti per l'accreditamento degli organismi di certificazione predisposti dalle Autorità di controllo del Portogallo (parere 12/2021), Romania (parere 13/2021), Ungheria (parere 19/2021), Lituania (parere 25/2021), Lettonia (parere 38/2021), Belgio (parere 35/2020) e Norvegia (parere 36/2021).

Linee guida sulla valutazione dei criteri di certificazione

Il 14 aprile 2021 il Cepd ha sottoposto a consultazione pubblica le linee guida sulla valutazione dei criteri di certificazione adottati il 6 aprile 2021, volte ad orientare le autorità di protezione dati e il Cepd stesso nella valutazione dei criteri di certificazione di schemi di certificazione sia nazionali, sia europei, nonché i proprietari dei medesimi schemi nella stesura dei relativi criteri.

Schema di certificazione europea della cybersicurezza per i servizi *cloud*

Sempre in materia di certificazioni, il Cepd, con lettere indirizzate ad Enisa il 9 marzo ed il 18 novembre 2021, ha espresso le proprie valutazioni in merito a uno schema di certificazione europea per la sicurezza informatica dei servizi *cloud* (EUCS - *European Cybersecurity Certification Scheme for Cloud Services*) sviluppato da Enisa in attuazione del regolamento UE 2019/881 sulla cybersicurezza.

Proposte di regolamento UE sul certificato verde digitale

Il Cepd e il Gepd hanno adottato un parere congiunto sulle proposte di regolamento dell'UE che hanno introdotto il certificato verde digitale con l'obiettivo di facilitare l'esercizio del diritto alla libera circolazione in Europa durante la pandemia di Covid-19 stabilendo un quadro comune per il rilascio, la verifica e l'accettazione di certificati Covid-19 di vaccinazione, test e guarigione interoperabili (parere

23

04/2021 del 31 marzo 2021). In particolare, è stata evidenziata la necessità di attenuare i potenziali rischi per i diritti fondamentali dei cittadini e dei residenti dell'UE derivanti dal rilascio del certificato verde digitale, compresi possibili ulteriori utilizzi indesiderati. Inoltre, è stato sottolineato che l'uso del certificato verde digitale non può in alcun modo dar luogo a discriminazioni dirette o indirette nei confronti delle persone e deve essere pienamente in linea con i principi fondamentali di necessità, proporzionalità ed efficacia.

Pertanto è stato chiesto di stabilire norme chiare e precise che disciplinino la portata e l'ambito di applicazione del certificato verde digitale e di introdurre garanzie adeguate affinché gli interessati abbiano la ragionevole certezza che i loro dati personali siano protetti con efficacia dal rischio di potenziali discriminazioni. Al riguardo, è stato precisato che le proposte non possono comportare la creazione di alcun genere di banca dati centralizzata a livello dell'UE. Sono state altresì espresse raccomandazioni specifiche perché siano chiarite le categorie di dati oggetto delle proposte, l'archiviazione dei dati, gli obblighi di trasparenza e l'identificazione dei titolari e dei responsabili del trattamento. Infine, è stato chiesto di prevedere espressamente che, una volta cessata la pandemia, non sia più consentito accedere o usare ulteriormente i medesimi dati. Data la natura delle misure proposte, il Cepd e il Gepd hanno raccomandato che l'uso del certificato verde digitale da parte degli Stati membri sia fondato su un'idonea base giuridica a livello nazionale e che, a seguito di un'adeguata valutazione d'impatto, siano applicate tutte le garanzie necessarie, in particolare, per evitare qualsiasi rischio di discriminazione e sia vietata la conservazione dei dati nel processo di verifica. Il Cepd e il Gepd hanno altresì sottolineato la necessità che l'applicazione dei regolamenti proposti sia strettamente limitata alla situazione di emergenza causata dalla pandemia.

Proposta di regolamento UE sulla *governance* dei dati

Il 9 marzo 2021 il Cepd e il Gepd si sono espressi in merito alla proposta di regolamento del Parlamento europeo e del Consiglio sulla *governance* dei dati (*Data governance act*) con un parere congiunto. La proposta di regolamento mira a promuovere la disponibilità dei dati nell'UE potenziando i meccanismi di messa a disposizione dei dati, in particolare nel settore pubblico mediante il riutilizzo, nonché la condivisione dei dati tra imprese e individui tramite fornitori di servizi appositi, consentendo altresì l'utilizzo dei dati per scopi "altruistici".

Nel considerare legittimo l'obiettivo sotteso alla proposta di regolamento, ossia migliorare le condizioni per la condivisione dei dati nel mercato interno, il parere congiunto sottolinea come la protezione dei dati personali sia parte essenziale e integrante della fiducia nell'economia digitale. Al riguardo il parere richiede, tra l'altro, che il futuro regolamento sulla *governance* dei dati sia pienamente in linea con il quadro giuridico dell'UE in materia di protezione dei dati personali, in particolare per quanto riguarda la competenza delle autorità di controllo, i ruoli dei diversi attori coinvolti, la base giuridica per il trattamento dei dati personali, le garanzie necessarie e l'esercizio dei diritti degli interessati. Più in generale, segnala la necessità che il nuovo regolamento affermi in modo chiaro e inequivocabile che esso non incide sul livello di protezione dei dati personali, né modifica i diritti e gli obblighi stabiliti nella legislazione in materia di protezione dei dati.

Inoltre, chiede di chiarire che il riutilizzo dei dati personali detenuti da enti pubblici possa essere consentito solo sulla base del diritto dell'UE o degli Stati membri. Tale base giuridica dovrebbe includere un elenco di finalità chiaramente compatibili, per le quali può essere lecitamente autorizzato il trattamento ulteriore dei dati ovvero quest'ultimo costituisce una misura necessaria e proporzionata, in una società democratica, per salvaguardare gli obiettivi di cui all'art. 23 del RGPD.

In merito ai fornitori di servizi di condivisione dei dati, il parere congiunto sotto-

linea la necessità di garantire alle persone fisiche la previa informazione sull'utilizzo dei loro dati e dei sistemi di controllo degli stessi, tenendo in considerazione i principi di trasparenza, limitazione delle finalità, *privacy by design* e *by default.* Inoltre si chiede di chiarire le modalità con cui i fornitori di tali servizi possono assistere gli interessati nell'esercizio dei loro diritti.

Per quanto riguarda il cd. altruismo dei dati – ossia il consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o le autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali senza la richiesta di un compenso, per finalità di interesse generale, quali la ricerca scientifica o il miglioramento dei servizi pubblici – il parere congiunto raccomanda di definire meglio le finalità di interesse generale comprese in tale nozione e di permettere alle persone interessate di prestare e revocare facilmente il consenso all'utilizzo dei loro dati per queste finalità. Alla luce dei possibili rischi per gli interessati, si suggerisce di prendere in esame procedure più rigorose rispetto a quelle di mera notifica e registrazione previste rispettivamente per la fornitura di servizi di condivisione dei dati e per le organizzazioni per l'altruismo dei dati, raccomandando il ricorso a strumenti di responsabilizzazione, quali l'adesione a codici di condotta o a meccanismi di certificazione.

Si raccomanda infine di designare le autorità di protezione dei dati quali principali autorità competenti a verificare il rispetto delle disposizioni del nuovo regolamento, in consultazione con le altre autorità di settore competenti.

Al parere congiunto sulla proposta di regolamento europeo sulla *governance* dei dati ha fatto seguito una dichiarazione (05/2021 del 19 maggio 2021) nella quale il Comitato ribadisce che, in assenza di solide garanzie in materia di protezione dei dati, è a rischio la fiducia nell'economia digitale. In particolare la dichiarazione esorta i co-legislatori a esaminare attentamente la compatibilità tra il nuovo regolamento e il RGPD. Lo *statement* contiene anche il riferimento alla natura di "merce non negoziabile" dei dati personali (riprendendo quanto già affermato dall'EDPB nelle linee guida 2/2019) e al carattere inalienabile del diritto alla protezione dei dati personali, al quale "non si può rinunciare" e che non può essere oggetto di diritti di proprietà.

Proposta di regolamento UE sull'intelligenza artificiale

Con il parere congiunto 05/2021 il Cepd e il Gepd nel giugno 2021 si sono espressi sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'IA (*Artificial Intelligence Regulation*). Le due Istituzioni, pur accogliendo favorevolmente l'iniziativa, hanno espresso la loro preoccupazione per l'esclusione dall'ambito di applicazione della proposta delle attività di cooperazione internazionale in materia di polizia e giustizia. Inoltre, hanno sottolineato la necessità di chiarire esplicitamente che la vigente legislazione dell'UE sulla protezione dei dati si applica a qualsiasi trattamento di dati personali che rientra nell'ambito di applicazione del futuro regolamento. Pur accogliendo con favore la distinzione fra sistemi a basso, medio e alto rischio contenuta nella proposta, è stato evidenziato che il concetto di "rischio per i diritti fondamentali" dovrebbe essere allineato al quadro dell'UE in materia di protezione dei dati. Inoltre, hanno raccomandato di valutare e mitigare anche i rischi di carattere sociale riguardanti gruppi di individui. D'altro canto, hanno concordato sul fatto che la classificazione di un sistema di IA come ad alto rischio non significa necessariamente che questo sia di per sé lecito e possa essere utilizzato in quanto tale. Più in generale, il Cepd e il Gepd hanno sottolineato come il rispetto degli obblighi derivanti dalla legislazione dell'UE, compresa la protezione dei dati personali, debba essere una condizione preliminare per l'ingresso nel mercato europeo dei sistemi di IA come prodotti con marchio CE.

Tenendo conto dei rischi estremamente elevati posti dall'identificazione biometrica a distanza di individui in spazi accessibili al pubblico, è stato chiesto di

23

introdurre un divieto generalizzato di qualsiasi uso dell'IA per il riconoscimento automatizzato delle caratteristiche umane in spazi accessibili al pubblico, quali il riconoscimento facciale, quello dell'andatura, delle impronte digitali, del Dna, della voce, la pressione sulla tastiera e di altre caratteristiche biometriche o comportamentali. Analogamente, è stato raccomandato di vietare i sistemi di IA che utilizzano la biometria per classificare gli individui in gruppi in base all'etnia, al genere, all'orientamento politico o sessuale o ad altri motivi per i quali la discriminazione è vietata ai sensi dell'art. 21 della Carta dei diritti fondamentali. Inoltre, il Cepd e il Gepd ritengono che l'uso dell'IA per dedurre le emozioni di una persona sia altamente indesiderabile e dovrebbe essere vietato, ad eccezione di casi molto specifici, come alcuni contesti sanitari, in cui il riconoscimento delle emozioni del paziente è importante e che l'uso dell'IA per qualsiasi tipo di "punteggio sociale" (*social scoring*) dovrebbe essere vietato poiché è contrario ai valori fondamentali dell'UE e per le discriminazioni che comporta.

È stata accolta con sostanziale favore la designazione del Gepd come autorità competente e autorità di vigilanza del mercato per la supervisione delle istituzioni, delle agenzie e degli organi dell'Unione.

Il Cepd e il Gepd hanno poi ricordato che le autorità per la protezione dei dati stanno già vigilando sull'applicazione del RGPD e della LED sui sistemi di IA che coinvolgono dati personali. Di conseguenza, la designazione delle autorità per la protezione dei dati come autorità di vigilanza nazionali garantirebbe un approccio armonizzato e contribuirebbe all'interpretazione coerente delle disposizioni in materia di trattamento dei dati in tutta l'UE.

Infine, è stato messo in discussione il ruolo predominante previsto per la Commissione europea nell'*European Artificial Intelligence Board* (EAIB), poiché esso sarebbe in conflitto con la necessità di un organismo europeo dell'IA indipendente da qualsiasi influenza politica. Per garantirne l'indipendenza, la proposta dovrebbe invece conferire maggiore autonomia all'EAIB, stabilendo che esso possa agire di propria iniziativa.

Dichiarazione sul pacchetto di servizi digitali e sulla strategia per i dati della Commissione europea

In una dichiarazione del 18 novembre 2021 il Cepd ha manifestato preoccupazioni di carattere generale riguardanti le proposte presentate dalla Commissione europea negli ambiti dei servizi digitali e della strategia europea per i dati: il *Data governance act* (DGA), il *Digital services act* (DSA) e il *Digital markets act* (DMA) e il regolamento sull'IA (AIR). In particolare, è stata sottolineata la mancanza di adeguate tutele per i diritti e le libertà fondamentali delle persone, la frammentazione delle attività di supervisione e i rischi di incongruenze con il quadro giuridico esistente in materia di protezione dei dati personali.

Nella dichiarazione, il Cepd ha ribadito la richiesta di vietare qualsiasi uso dell'IA per il riconoscimento automatizzato delle caratteristiche umane in spazi accessibili al pubblico e sollecitato il co-legislatore a considerare l'eliminazione graduale della pubblicità mirata sulla base del tracciamento pervasivo delle persone, nonché l'introduzione del divieto di profilazione dei minori.

Il Cepd ha evidenziato inoltre i rischi di creare strutture di vigilanza parallele e raccomandato che ciascuna proposta introduca una base giuridica esplicita per l'efficace cooperazione e scambio di informazioni tra le autorità di vigilanza competenti nell'ambito di ciascuna proposta e le autorità di protezione dei dati.

Infine, il Cepd ha invitato la Commissione e il co-legislatore a garantire che le proposte non pregiudichino l'applicazione delle norme esistenti in materia di protezione dei dati e che tali norme prevalgano ogni volta che i dati personali siano trattati, anche in relazione alla futura proposta di regolamento della Commissione europea recante norme armonizzate sull'accesso equo e sull'uso dei dati (*Data act*).

Con riferimento al questionario della Commissione europea sul trattamento dei dati personali a scopo di ricerca scientifica e, in particolare, quella relativa alla salute (2 febbraio 2021) il Comitato ha fornito alcune indicazioni preliminari, in attesa delle linee guida sul trattamento dei dati personali a fini di ricerca scientifica a cui il Cepd sta lavorando.

Trattamento dei dati personali a scopo di ricerca scientifica

È proseguita l'attività del Comitato anche con riferimento all'applicazione dei principi di protezione dei dati nel settore finanziario, attraverso uno specifico sottogruppo (*Financial matters*) il cui coordinamento è affidato al Garante.

Affari finanziari

Uno dei temi che ha maggiormente impegnato il Comitato è stato quello della lotta al riciclaggio e al finanziamento del terrorismo (AML/CFT) 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 (composto da un regolamento che istituisce una nuova autorità dell'UE in materia di antiriciclaggio e lotta al finanziamento del terrorismo; un regolamento in materia di AML/CFT; una sesta direttiva in materia di AML/CFT (AMLD6), che sostituirà l'attuale direttiva 2015/849/UE; una revisione del regolamento 2015/847/UE sui trasferimenti di fondi, ai fini del tracciamento dei trasferimenti di cripto-attività).

Antiriciclaggio e lotta al finanziamento del terrorismo

Oltre ad alcuni incontri informali tra il sottogruppo *Financial matters* e la Commissione, in cui sono stati discussi i principi di protezione dati che devono essere garantiti nell'approntamento delle *policy* antiriciclaggio, il Cepd il 19 maggio 2021 in una lettera indirizzata ai Commissari UE McGuinness (concorrenza) e Reynders (giustizia) ha sottolineato che la revisione della normativa AML/CFT in ambito europeo costituisce un'occasione per assicurare, anche in questo settore, il rispetto dei principi di protezione dei dati previsti dal RGPD, in particolare i principi di minimizzazione e proporzionalità dei dati trattati da parte dei cd. soggetti obbligati (*obliged entities,* ad es. banche e istituti finanziari) chiamati a svolgere compiti di monitoraggio e segnalazione di transazioni sospette. Ha invitato il legislatore a definire con maggiore chiarezza i trattamenti che le banche devono effettuare per adempiere ai loro obblighi in materia di AML-CFT, nonché i tempi di conservazione dei dati a seconda delle diverse finalità dei trattamenti effettuati. Particolare attenzione deve essere inoltre prestata all'accuratezza dei dati, anche con riferimento alle informazioni trattate nell'ambito delle cd. *watch-lists* di cui i soggetti obbligati si servono.

Un altro filone inaugurato nel corso dell'anno dal Cepd in ambito finanziario è quello relativo alla questione dell'euro digitale, già al centro di diverse iniziative della Banca centrale europea, tra le quali la consultazione pubblica avviata il 12 ottobre 2020, da cui è emerso che la protezione dei dati rappresenta un tema cruciale nella costruzione di una moneta digitale, che si presta potenzialmente a forme di sorveglianza massive, e che deve basarsi, anche sulla fiducia degli utilizzatori.

Euro digitale

Nella plenaria del 18 giugno 2021 con una lettera indirizzata alle Istituzioni UE competenti, *in primis* la Bce, si è prospettata la possibilità di una costruzione dell'euro digitale quanto più possibile vicina all'uso del contante, fondata cioè sull'utilizzo anonimo della moneta e si è ricordata la possibilità di optare per adeguate tecniche di pseudonimizzazione evidenziando, tuttavia, che il dato pseudonimizzato (ad es. relativo all'utilizzatore del *digital* euro) è un dato personale a norma del RGPD. A fronte della risposta positiva della Bce rispetto ad ipotesi di cooperazione con il *Board* è stato avviato un dialogo tra le due Istituzioni.

Il Cepd ha inoltre adottato, il 19 maggio 2021, le raccomandazioni 02/2021 sulla conservazione dei dati relativi a carta di credito da parte di piattaforme *online.* Tale documento si riferisce a situazioni in cui gli interessati acquistino un prodotto o paghino un servizio tramite un sito web o un'applicazione con carta di credito, il cui numero viene memorizzato per evitare che il cliente debba nuovamente digitarlo

Conservazione dei dati relativi a carta di credito per facilitare futuri acquisti

23

nei successivi acquisti, agevolando così le ulteriori transazioni.

L'unica base giuridica appropriata di cui il titolare può servirsi per conservare i dati della carta di credito dopo l'acquisto, in considerazione dei rischi per la sicurezza derivanti dal trattamento di dati relativi alla carta di credito, e per permettere all'interessato di mantenere il controllo su tali dati, appare il consenso specifico, e non già l'interesse legittimo. Il consenso deve essere fornito mediante un'azione positiva inequivocabile e dovrebbe essere richiesto in modo semplice, ad esempio attraverso una casella di spunta, non preselezionata. Tale consenso specifico deve essere distinto da quello fornito per le condizioni di servizio o di vendita e non deve costituire una condizione per la realizzazione dell'operazione. Ai sensi dell'art. 7, par. 3, del RGPD, l'interessato ha il diritto di revocare in qualsiasi momento il proprio consenso alla conservazione dei dati della carta di credito. La revoca deve essere libera e facile per l'interessato, analogamente alla prestazione del consenso. Essa deve risultare nell'effettiva cancellazione, da parte del titolare del trattamento, dei dati della carta di credito conservati al solo scopo di facilitare ulteriori operazioni.

Linee guida su notifica di violazione dei dati

Le *Guidelines* 01/2021 *on examples regarding data breach notification* sono state approvate dal Comitato nella riunione plenaria del 14 gennaio 2021 per aiutare imprese e p.a. ad affrontare correttamente le violazioni dei dati e definire i processi di gestione del rischio. Sul documento è stata avviata poi una consultazione pubblica conclusasi nel mese di marzo 2021. Le linee guida per i casi più significativi di violazione dei dati subiti da banche, ospedali, medie imprese, municipalità, società che offrono servizi *online* di vario genere presentano esempi di buone o cattive pratiche, raccomandano modalità di identificazione e valutazione dei rischi indicano in quali casi chi tratta i dati deve notificare la violazione all'autorità e, se necessario, informare le persone coinvolte. Il testo raccoglie i casi più rilevanti segnalati dalle autorità di supervisione: attacchi *ransomware*; attacchi di esfiltrazione di dati; fonte interna di rischio umano; dispositivi smarriti o rubati e documenti cartacei; *mispostal;* ingegneria sociale. Le linee guida elencano le misure organizzative e tecniche, per prevenire l'elevato rischio per i diritti e le libertà degli interessati derivante dalla violazione dei dati.

Protezione dei dati e nuove tecnologie: i veicoli connessi

Con riferimento alle nuove tecnologie, il 9 marzo 2021 il Comitato, a seguito della fase di consultazione pubblica, ha adottato la versione finale (v. 2.0) delle linee guida 01/2020 sul trattamento di dati personali nell'ambito dell'uso non professionale dei veicoli connessi e delle applicazioni relative alla mobilità. In particolare, il trattamento riguarda i dati personali trattati all'interno del veicolo e scambiati tra il veicolo e i dispositivi personali ad esso collegati (ad es. lo *smartphone* dell'utente) o raccolti all'interno del veicolo e trasmessi ad entità esterne per ulteriori elaborazioni (ad es. costruttori di veicoli, gestori di infrastrutture, compagnie di assicurazione, autoriparatori). Le linee guida si riferiscono, altresì, alle molteplici applicazioni mobili indipendenti dal veicolo, quali quelle di gestione della mobilità e del veicolo, sicurezza stradale, intrattenimento, assistenza alla guida e benessere.

Il documento evidenzia i rischi connessi a tali tipologie di trattamento e alle misure da adottare per assicurare il rispetto della disciplina in materia di protezione dei dati personali. La regolamentazione dei veicoli connessi vede infatti il coinvolgimento di una pluralità di attori appartenenti sia al settore automobilistico sia a quello digitale, ciascuno dei quali riveste generalmente il ruolo soggettivo di titolare autonomo del trattamento o di contitolare ed anche, in taluni casi, quello di responsabile del trattamento.

Dichiarazione 3/2021 sul regolamento *e-privacy*

Una dichiarazione adottata dal Comitato il 9 marzo 2021 sul progetto di regolamento *e-privacy* accoglie con favore l'accordo sul mandato negoziale del Consiglio quale passo positivo verso la finalizzazione del regolamento *e-privacy* e sottolinea come l'applicazione del futuro regolamento dovrebbe essere affidata al

controllo delle autorità di protezione dati per garantirne un'interpretazione coerente.

In particolare, sulla base delle opinioni espresse in precedenza dal Cepd e dal WP Art. 29:

- si sottolinea che, ove il regolamento *e-privacy* dovesse contenere disposizioni sulla conservazione dei dati, le stesse dovrebbero essere perfettamente in linea con la più recente giurisprudenza della CGUE e con la Carta dei diritti fondamentali dell'UE;
- si richiede una protezione specifica per la riservatezza delle comunicazioni elettroniche;
- si ricorda la necessità di vietare in generale l'uso dei dati di comunicazione elettronica con limitate eccezioni mentre il futuro regolamento non dovrebbe limitare in alcun modo l'uso o l'efficienza della crittografia;
- si richiama al rispetto dell'obbligo del consenso per *cookie* e tecnologie simili, offrendo ai fornitori di servizi strumenti tecnici che consentano loro di ottenere facilmente tale consenso;
- si sottolinea che consentire ulteriori trattamenti per scopi compatibili riduce il livello di protezione offerto dall'attuale direttiva *e-privacy* e che l'uso di dati anonimi dovrebbe essere favorito;
- si insiste sul fatto che le autorità dovrebbero essere competenti ai sensi del regolamento *e-privacy,* al fine di garantire la coerenza con il RGPD ed un elevato livello di protezione, offrire certezza giuridica ed evitare oneri eccessivi per i responsabili del trattamento dei dati. La dichiarazione ribadisce inoltre che il meccanismo di cooperazione e coerenza di cui al capo VII del RGPD dovrebbe essere utilizzato per la supervisione del regolamento *e-privacy.*

Linee guida 02/2021 sugli assistenti vocali virtuali

Il Comitato ha adottato il 7 luglio 2021 la versione finale 2.0 delle linee guida sugli assistenti vocali virtuali (AVV) ovvero sui servizi che comprendono i comandi vocali e li eseguono ovvero, se necessario, mediano con altri sistemi informatici. Com'è noto gli AVV sono attualmente disponibili sulla maggior parte degli *smartphone* e dei *tablet,* sui computer tradizionali e, negli ultimi anni, anche su dispositivi *stand-alone* come gli altoparlanti intelligenti. Ciò comporta che gli AVV hanno accesso a un'enorme quantità di dati personali inclusi tutti i comandi impartiti dagli utenti ai loro dispositivi (come la cronologia di navigazione o di ricerca) e le risposte degli stessi (appuntamenti in agenda).

Le linee guida inizialmente adottate dalla plenaria del *Board* del 9 marzo 2021 sono state poi sottoposte a consultazione pubblica dal 12 al 23 marzo 2021.

Tenendo conto dei contributi ricevuti, il testo definitivo conferma la necessità di implementare adeguate misure di sicurezza e di garanzia, di applicare i principi di *privacy by design* e di *privacy by default* e di ricorrere agli strumenti di *accountability* previsti espressamente dal Regolamento. Inoltre, il *provider* dei servizi AVV deve fornire agli interessati tutte le informazioni previste dal RGPD ai sensi dell'art. 13 e del cons. 58, in una forma semplice, chiara e accessibile. Tali informazioni devono essere rilasciate non solo agli utenti registrati ai servizi AVV, ma anche a chi non è registrato ed agli utenti accidentali (per quanto, nella pratica, quest'ultima condizione sia difficile da rispettare).

Linee guida 8/2020 sul *targeting* degli utenti di *social media*

Le linee guida sul *targeting* degli utenti di *social media* rappresentano un importante documento in considerazione dello sviluppo significativo registrato nel contesto *online* nell'ultimo decennio. Tra le caratteristiche principali dei *social media* figurano la possibilità per le persone fisiche di registrarsi al fine di creare *account* (conti) o profili per sé stesse, di interagire condividendo contenuti nonché di sviluppare collegamenti e reti con altri utenti. Nell'ambito del loro modello aziendale numerosi fornitori di *social media* offrono servizi di *targeting* i quali consentono

23

a persone fisiche o giuridiche *targeter* di comunicare messaggi specifici agli utenti di *social media* per promuovere interessi commerciali, politici o di altro tipo. Le funzioni aggiuntive fornite dai *social media* possono comprendere ad esempio la personalizzazione, l'integrazione di applicazioni, i *plug-in* sociali, l'autenticazione dell'utente, l'analisi e la pubblicazione.

In tale contesto, il Comitato ha adottato il 13 aprile 2021 la nuova versione delle linee guida sul *targeting* degli utenti di *social media* (adottate il 2 settembre 2020), alla luce della consultazione pubblica. Nella nuova versione si chiarisce, tra l'altro, che non è negli intenti delle linee guida fornire un'analisi approfondita dei trattamenti relativi a individui non registrati nel *social network* (che tuttavia vengono menzionati in quanto interessati nelle sezioni successive). Si chiarisce inoltre che, nel contesto della contitolarità del trattamento, il reciproco beneficio dei due contitolari (società X che vende scarpe che si serve della profilazione effettuata dal *social network* Y per campagne pubblicitarie mirate che appaiono sullo stesso *social network*) è un elemento addizionale significativo per dimostrare il legame inestricabile tra le finalità dei trattamenti e dimostrare dunque la contitolarità (conformemente a quanto detto nelle linee guida titolare-responsabile). Si specifica altresì che l'art. 6, par. 1, lett. *b*), del RGPD non può costituire la base giuridica per il trattamento effettuato dal fornitore di *social network* semplicemente perché la pubblicità finanzia il servizio. Stessa cosa per il *targeter* che non può sostenere che il *targeting* sia un elemento intrinseco necessario del suo rapporto contrattuale con l'interessato (conformemente a quanto detto nelle linee guida 2/2019 sull'art. 6, par. 1, lett. *b*).

Raccomandazioni sull'adeguatezza di Paesi terzi ai sensi della direttiva UE 2016/680

Il 2 febbraio 2021 il Cepd ha adottato le raccomandazioni 01/2021 sui criteri di riferimento per l'adeguatezza delle norme in materia di protezione dati di ordinamenti di Paesi terzi o di organizzazioni internazionali ai sensi dell'art. 36 della direttiva 2016/680 cd. *law enforcement directive* (LED) che regola il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Le raccomandazioni hanno l'obiettivo di fornire un elenco di elementi da esaminare nel valutare l'adeguatezza del livello di protezione nell'ambito delle attività di polizia e giustizia. Il documento, nel sottolineare la specificità e gli aspetti procedurali dell'adeguatezza secondo la LED e la giurisprudenza della CGUE in materia, fissa gli standard dell'UE per la protezione dei dati nell'ambito della cooperazione di polizia e giudiziaria in materia penale.

Adeguata protezione dei dati personali nel Regno Unito ai sensi della direttiva UE 2016/680

Il Cepd si è espresso il 13 aprile 2021 con i pareri 14/2021 e 15/2021 sui due progetti di decisione di adeguatezza della Commissione europea nei confronti del Regno Unito. Il primo si basa sul RGPD e valuta sia gli aspetti generali della protezione dei dati nel sistema giuridico del Regno Unito, sia gli aspetti riguardanti l'accesso delle autorità governative ai dati personali trasferiti dall'UE a fini di prevenzione, indagine, accertamento e perseguimento di reati e di sicurezza nazionale (v. *supra*). Il secondo si basa sulla LED e analizza il progetto di decisione di adeguatezza alla luce delle raccomandazioni 01/2021 sui criteri di riferimento per l'adeguatezza ai sensi della LED, nonché delle raccomandazioni 02/2020 sulle garanzie essenziali europee per le misure di sorveglianza, che richiamano la giurisprudenza della CGUE in materia (cfr. Relazione 2020, p. 231). A tale riguardo, il Comitato ha rilevato un forte allineamento tra il quadro di protezione dei dati dell'UE e quello del Regno Unito su alcuni aspetti fondamentali, ed un livello di protezione essenzialmente equivalente a quello garantito dal diritto dell'UE in relazione al trasferimento di dati personali in un Paese terzo da parte delle autorità di *law enfocement* britanniche. Tuttavia, ha sollecitato la Commissione a svolgere il suo ruolo di monitoraggio e, ove il quadro sulla protezione dei dati del Regno Unito dovesse discostarsi dall'*acquis*

dell'UE, a valutare la possibilità di modificare la decisione di adeguatezza per introdurre garanzie specifiche per i dati ivi trasferiti, e/o a sospendere la decisione di adeguatezza, anche, se del caso, per quanto riguarda accordi tra il Regno Unito e Paesi terzi che possano minare il livello di protezione dei dati personali oggetto di ulteriore trasferimento in tali Paesi.

Contributo del Comitato alla valutazione della direttiva UE 2016/680

Il Cepd e le singole autorità nazionali di controllo hanno contribuito alla valutazione e revisione della direttiva sulla protezione dei dati nei settori di polizia e giustizia che la Commissione europea è chiamata a condurre ai sensi dell'art. 62 della stessa direttiva entro il mese di maggio 2022. Nel suo contributo (14 dicembre 2021), il Comitato ha evidenziato che a causa della recente implementazione della direttiva negli ordinamenti nazionali, l'esperienza maturata e i dati al riguardo acquisiti sono piuttosto limitati. Pertanto, ad avviso del Cepd, trarre conclusioni sull'efficacia della direttiva o prendere in considerazione la sua revisione sarebbe al momento prematuro. In tale contesto, il Comitato ha esortato gli Stati membri che non hanno completato la fase di attuazione della direttiva a investire tutte le risorse possibili per garantire che il suo recepimento sia portato a termine senza ulteriori ritardi e in modo conforme alla direttiva. Infine, il Comitato ha sottolineato che l'efficace attuazione dei compiti delle autorità nazionali di controllo nei settori regolamentati dalla direttiva richiede la disponibilità di risorse sia umane che tecniche e ha invitato gli Stati membri a garantire che tali risorse aumentino in proporzione al carico di lavoro delle autorità.

Valutazione della direttiva UE 2016/681 sull'uso dei dati del PNR

Con due lettere indirizzate rispettivamente alla Commissione europea (22 gennaio 2021) e alla Parlamentare europea Sophie In't Velt (25 gennaio 2021), il Cepd si è espresso sul riesame e sulla valutazione della direttiva europea sull'uso dei dati PNR a fini di prevenzione, accertamento e repressione di reati gravi e di terrorismo. Contrariamente alla valutazione positiva espressa dalla Commissione europea nel rapporto pubblicato il 24 luglio 2020 con riferimento ai primi due anni di applicazione della direttiva PNR (COM(2020) 305 *final*), il Comitato ha ricordato che le autorità di protezione dei dati, in una lettera indirizzata alla Commissione europea l'11 aprile 2018 dall'allora Gruppo Art. 29, avevano già individuato la necessità di emendare la direttiva 681 alla luce del parere 1/15 della CGUE sul progetto di accordo tra il Canada e l'UE relativo al trasferimento dei dati PNR (26 luglio 2017), ritenendo che il predetto parere, pur non dispiegando effetti giuridici su altri atti dell'Unione, aveva evidenziato talune carenze riscontrabili anche in altri accordi e atti normativi europei in materia di PNR (https://ec.europa.eu/newsroom/article29/redirection/document/51023). Ad avviso del Comitato, il rapporto della Commissione non conferma esplicitamente, né motiva compiutamente la necessità e la proporzionalità della raccolta indiscriminata e del trattamento dei dati PNR a fini di prevenzione, accertamento e repressione di reati gravi e di terrorismo. Infatti, la grande quantità di persone interessate (rispetto all'esiguità degli elementi probatori sull'utilità di dati PNR, contenuti nei casi studio su cui si basa la valutazione della Commissione), solleva seri dubbi in merito alla proporzionalità del trattamento della enorme massa di dati. Per tali ragioni, il Cepd ha ritenuto, in linea con la recente giurisprudenza della CGUE (cause riunite C-511/18, C-512/18 and C-520/18, La *Quadrature du Net* e altri, par. 133 e causa C-623/17, *Privacy International,* par. 78), che il riesame della direttiva 681 debba basarsi su solidi elementi di prova in grado di dimostrare il collegamento tra la conservazione dei dati PNR e gli obiettivi perseguiti. Pertanto il Cepd ha ribadito il suo appello alla Commissione europea affinché venga garantita la conformità di tutti gli strumenti dell'UE sui dati PNR, inclusa la direttiva 681, al diritto dell'UE e alla giurisprudenza della CGUE.

Secondo Protocollo addizionale alla Convenzione di Budapest

Facendo seguito al contributo fornito nel novembre 2019 in occasione della consultazione pubblica e alla lettera del 29 gennaio 2020, il Cepd si è espresso anche quest'anno sul progetto di secondo Protocollo aggiuntivo alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest), in particolare sul progetto di disposizioni relative alla richiesta di informazioni sulla registrazione dei nomi di dominio e alla comunicazione accelerata di dati informatici memorizzati in caso di emergenza (dichiarazione 2/2021 del 2 febbraio 2021). In particolare, è stato ricordato che queste disposizioni potrebbero incidere sulle condizioni di accesso ai dati personali nell'UE a seguito di richieste di autorità di Paesi terzi a fini di *law enforcement* ed è stata sottolineata la necessità di garantire la piena coerenza con *l'acquis* dell'UE per ciò che concerne la protezione dei dati personali. Nell'ambito del 6° ciclo di consultazioni avviato in aprile dal Comitato *Cybercrime* del Consiglio d'Europa (T-CY), a seguito della pubblicazione del progetto completo del secondo Protocollo, il Cepd ha avuto occasione di intervenire nuovamente sul tema e, in particolare, sulle disposizioni dedicate alle garanzie in materia di protezione dei dati personali (4 maggio 2021). Nel proprio contributo il Cepd ha formulato una serie di osservazioni nel merito di tali disposizioni, la cui introduzione nel progetto di Protocollo è stata accolta con favore, segnalando, anche alla luce della giurisprudenza della Corte di giustizia, che le garanzie approntate dal Protocollo devono essere idonee ad assicurare che il livello di protezione dei dati personali garantito dal diritto dell'Unione non venga compromesso allorché questi siano comunicati e trasferiti in Paesi terzi parti del Protocollo, in attuazione dei meccanismi di cooperazione previsti dallo stesso di *law enforcement* (cfr. par. 23.3).

Sistema di riconoscimento facciale per i migranti in Italia

In riposta alla lettera dell'eurodeputata Sophie In't Veld che chiedeva chiarimenti sull'uso in Italia di un sistema di riconoscimento facciale per i migranti, il Cepd ha confermato di prestare particolare attenzione al tema che solleva preoccupazioni senza precedenti in termini di protezione dei dati, soprattutto quando si tratta di persone vulnerabili come i migranti (10 agosto 2021). Riguardo al caso italiano, è stato precisato che il 25 marzo 2021 il Garante ha reso parere negativo in ordine a un sistema automatizzato di identificazione biometrica su larga scala di supporto generale alle attività investigative, all'esito dell'analisi della valutazione di impatto *privacy* condotta dal Ministero dell'interno previamente all'attivazione del sistema (Sari *Real Time*). Inoltre, il Comitato ha riaffermato il proprio continuo impegno a monitorare l'uso delle nuove tecnologie in UE, quali il riconoscimento facciale, e il loro potenziale impatto sui diritti fondamentali e la vita quotidiana degli individui. Infine, ha reso noto che sta lavorando a linee guida sul riconoscimento facciale in conformità alla strategia definita per il periodo 2021-2023.

Presunto utilizzo dello *spyware* Pegasus

In una lettera di risposta all'eurodeputato István Ujhelyi in merito al presunto utilizzo dello *spyware* Pegasus in Ungheria (14 dicembre 2021), il Comitato ha precisato di essere competente in merito al presunto utilizzo del *software* Pegasus ove questo sia utilizzato per le finalità contemplate nel RGPD e nella LED, pur non avendo le stesse competenze, compiti e poteri delle autorità nazionali, sulla base del diritto dell'Unione applicabile. Nel caso di specie compete infatti all'Autorità per la protezione dei dati ungherese condurre un'indagine in merito al presunto uso di questo strumento in Ungheria, mentre il Comitato è pronto a dare supporto a tutti i suoi membri in relazione a tali questioni.

Domande pregiudiziali davanti alla CGUE ex art. 267 TFUE

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, nei casi in cui le stesse hanno interessato la materia della protezione dei dati personali. Al riguardo, a seguito dell'applicazione dal 25 maggio 2018 del nuovo quadro normativo europeo si registra un incremento dei rinvii pregiudiziali alla

CGUE, in relazione ai quali il Garante fornisce all'Avvocatura dello Stato valutazioni sull'intervento del Governo nelle controversie.

23

23.2. *La cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

Europol Cooperation Board

In virtù del nuovo quadro normativo introdotto dal regolamento (UE) 2016/794, entrato in vigore il 1° maggio 2017, la supervisione sull'attività svolta dall'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) è svolta dal Gepd. Rimane di competenza delle autorità nazionali di protezione dei dati la vigilanza sulla comunicazione di dati ad Europol da parte delle autorità di contrasto (*law enforcement*) e la verifica circa il rispetto dei diritti degli interessati. Al fine di assicurare una stretta cooperazione tra il Gepd e le autorità nazionali è stato istituito, con funzioni consultive, un Consiglio di cooperazione (*Europol Cooperation Board*-ECB), riunitosi in videoconferenza il 23 novembre per esaminare gli ultimi sviluppi relativi alla proposta per la *Europol Regulation,* adottata dal Consiglio d'Europa. Nel corso della medesima riunione il rappresentante dell'EDPS ha riferito circa l'attività di supervisione e i risultati dell'ispezione effettuata insieme con la DPA olandese, con particolare riferimento agli strumenti di *Machine Learnig* (di seguito ML *tools*). È stato inoltre presentato un progetto volto a migliorare l'accesso alle cd. *e-evidence* nell'ambito delle attività di polizia ed indagini giudiziarie, in particolare per fornire supporto alle autorità di *law enforcement* circa i dati detenuti dagli OSPs (*online service providers*) e promuovere una diretta cooperazione tra i *providers* e le autorità di polizia nonché a ricevere commenti e indicazioni da parte delle DPAs.

SIS II

Il sistema d'informazione Schengen (SIS II) è il sistema d'informazione centralizzato su larga scala, utilizzato come strumento d'ausilio per i controlli sulle persone e sugli oggetti alle frontiere esterne dello spazio Schengen. Secondo quanto previsto dal regolamento CE 1987/2006 e dalla decisione del Consiglio 2007/533/GAI, la supervisione coordinata del sistema è di competenza del Gruppo di coordinamento della supervisione SIS II, di cui fanno parte le autorità di protezione dati dei Paesi membri – che assicurano la supervisione delle autorità nazionali competenti per il sistema SIS II – e il Gepd – che supervisiona il trattamento dati posto in essere dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (EU-LISA), cui è rimessa la gestione del sistema centrale. Nel 2021 il Gruppo si è riunito – da remoto – il 25 novembre 2021 e ha adottato la lettera indirizzata all'OCM e ai co-legislatori in merito alla proposta di regolamento del Consiglio relativa all'istituzione e al funzionamento di un meccanismo di valutazione e monitoraggio per verificare l'applicazione dell'*acquis* di Schengen e che abroga il regolamento (UE) n. 1053/2013.

Il Gruppo ha, altresì, lavorato sul questionario relativo alle segnalazioni nel Sistema d'informazione Schengen (SIS), ai sensi dell'art. 36 della decisione 2007/533/GAI del Consiglio. Inoltre, la Commissione ha fornito informazioni sulle date di entrata in vigore del nuovo regolamento SIS II (giugno 2022) e sulla relativa campagna d'informazione (dal mese di marzo 2022).

Nel corso della riunione, inoltre, è stato comunicato lo stato di avanzamento del SIS II da parte del Rpd di EU-LISA e, quindi, l'attività di verifica e controllo del *database.* Il Gruppo è stato quindi informato dell'imminente passaggio al CSC (Comitato di supervisione coordinata) della supervisione svolta dal SCG, la cui ultima riunione si terrà entro la metà del mese di giugno 2022.

Comitato di supervisione coordinata CSC

Il CSC si è riunito il 1° dicembre ed ha esaminato l'indagine effettuata tramite il questionario sottoposto alle DPA per verificare l'utilizzo della piattaforma IMI a livello nazionale. Si è deciso di lavorare su un testo di informativa standard sull'utilizzo di IMI, nonché sui diritti degli interessati.

Nel corso della riunione è stato presentato l'esito di una indagine parziale in merito ai trattamenti effettuati dall'*European Public Prosecutor Office* (EPPO). La Procura europea è un'Istituzione indipendente dell'Unione europea, operativa dal 1º giugno 2021, secondo le disposizioni del Trattato di Lisbona e come cooperazione rafforzata tra ventidue dei ventisette membri dell'UE (al momento non partecipano: Ungheria, Irlanda, Polonia, Svezia e Danimarca). Il suo ruolo è quello di indagare e perseguire frodi e altri reati contro il bilancio e gli interessi finanziari dell'UE. L'organismo è stato decentralizzato con procuratori delegati europei in ciascuno Stato membro.

Inoltre, è stato affrontato il tema del funzionamento del CSC, che diventerà il *forum* unico per il controllo coordinato dei sistemi informativi dell'UE in tema di protezione dei dati per l'intero settore della cooperazione giudiziaria e di polizia nei tre ambiti principali della gestione delle frontiere, cooperazione giudiziaria e di polizia, IMI.

Il CSC ha poi trattato la questione del *Sirius Project,* finanziato dalla Commissione europea dal 2017 (con la collaborazione di Europol ed Eurojust e la rete giudiziaria europea), che mira alla condivisione delle conoscenze in materia di accesso transfrontaliero alle prove elettroniche, aiutando autorità giudiziarie e di polizia a far fronte alla complessità della materia, attraverso linee guida su strumenti investigativi, dati di contatto e *policy* adottate al riguardo dai *providers* (OSPs).

Gruppo di supervisione del sistema Eurodac

Il Gruppo di supervisione del sistema Eurodac è competente ad assicurare il rispetto della protezione dei dati personali all'interno del sistema istituito per la comparazione delle impronte digitali dei richiedenti asilo. Nella riunione da remoto del 24 novembre 2021 è stato trattato il tema della revisione del regolamento Eurodac, le cui modifiche sono in corso di discussione dal Parlamento europeo e il cui voto sugli emendamenti finali è previsto per il mese di gennaio 2022.

Inoltre, in merito al sistema effettuato da EU-LISA, è stata rilevata la diminuzione del traffico globale di dati inseriti nel sistema Eurodac nel 2020 pari a circa il 30% rispetto all'anno 2019. Un'ulteriore diminuzione del predetto traffico di dati è stata registrata nel mese di gennaio 2021 quale conseguenza della Brexit.

È stato tradotto in tutte le lingue degli Stati membri e poi pubblicato l'opuscolo destinato alle autorità nazionali volto a informare gli interessati sui loro diritti.

Gruppo di coordinamento della supervisione del Sistema informativo visti (VIS)

Il Gruppo di supervisione VIS è competente per il monitoraggio del sistema d'informazione dei visti (*Vis Information System*), istituito dalla decisione 2004/512/CE e volto a creare uno spazio di libertà, sicurezza e giustizia senza frontiere interne tramite lo scambio di dati relativi ai visti d'ingresso nello Spazio Schengen tra gli Stati che ne fanno parte. Il funzionamento del VIS è disciplinato dal regolamento (CE) 767/2008 e consiste in una banca dati centrale a livello europeo alla quale sono connesse le interfacce nazionali delle autorità degli Stati Schengen competenti per i visti, tra cui gli uffici consolari e i valichi di frontiera esterni degli Stati. Nel 2021, il Gruppo di supervisione (i cui documenti sono rinvenibili sul sito internet: https://edps.europa.eu/data-protection/european-it-systems/visa-information-system_en) si è riunito in videoconferenza due volte, il 17 giugno ed il 24 novembre.

Nell'ambito delle riunioni, il Gruppo è stato aggiornato da EU-LISA e dalla Commissione sui recenti sviluppi relativi alla gestione del VIS e sulla proposta di digitalizzazione della procedura europea di rilascio dei visti in ambito Schengen. Nell'ambito del suo programma di lavoro 2019-2021, il Gruppo si è occupato della

predisposizione di un quadro comune per i controlli sul VIS, sulla base dell'esperienza analoga maturata nell'ambito del Sistema d'informazione Schengen SIS-II. Il Gruppo ha proseguito l'approfondimento dei meccanismi di cancellazione dei dati dal VIS in caso di acquisto della cittadinanza o di annullamento del rifiuto di un visto (art. 25 del regolamento (UE) 767/2008) operanti prima dei cinque anni previsti ordinariamente per la conservazione dei dati nel VIS. Nel corso dell'anno, a livello nazionale, i partecipanti hanno condotto gli approfondimenti necessari sulle modalità utilizzate dagli Stati membri per dare corretta applicazione alla disposizione citata del regolamento VIS, tenuto conto delle normative e delle specificità nazionali. Ciò al fine di individuare buone pratiche e indicazioni di tipo organizzativo e tecnico per assicurare la tempestiva cancellazione dei dati dal VIS nelle ipotesi previste dalla norma citata.

Il Sistema informativo doganale (SID): ACC Dogane e Gruppo di coordinamento della supervisione SID

Il Sistema informativo doganale (SID) è un sistema informatico che centralizza le informazioni doganali al fine di prevenire, indagare e perseguire le violazioni della normativa doganale o agricola unionale. È composto da una banca dati centrale accessibile tramite terminali in ciascuno Stato membro. I dati inseriti nel SID si riferiscono a merci, mezzi di trasporto, imprese e persone associate a tali violazioni, beni sequestrati o confiscati.

Il Garante per la protezione dei dati italiano, in qualità di membro del Gruppo di coordinamento della supervisione del Sistema informativo doganale (ACC), è chiamato a supervisionare l'eventuale accesso da remoto al SID, con riferimento alle autorità nazionali che attualmente lo utilizzano e ai soggetti incaricati di accedere a tale sistema.

Nel 2021 l'ACC ha approvato la bozza di un questionario relativo alla formazione in materia di protezione dei dati personali del personale che ha accesso al sistema SID.

Le autorità di protezione dei dati sono state invitate a compilare il questionario e a trasmetterlo alle autorità nazionali competenti per l'accesso al Sistema dogane, al fine di restituirlo compilato entro la fine del 2021.

L'Autorità Garante ha acquisito dall'Agenzia delle accise dogane e monopoli, sezione antifrode, i riscontri richiesti; ha poi compilato il questionario per quanto di propria spettanza, restituendolo al Segretariato del Cepd. Il *report* finale, con i contributi di tutte le autorità, verrà presentato dal Segretariato nel mese di giugno 2022.

23.3. *La partecipazione dell'Autorità in seno al Consiglio d'Europa, all'OCSE e ad altri gruppi di lavoro internazionali*

Comitato Consultivo della Convenzione 108/1981 (T-PD)

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, di cui la rappresentante del Garante ha conservato la presidenza per il terzo mandato consecutivo.

Le due plenarie annuali del Comitato e le riunioni del gruppo ristretto (T-PD *Bureau*) sono state contrassegnate da una crescente partecipazione e ruolo attivo dei rappresentanti delle parti e degli osservatori.

Una delle attività principali del Comitato è stata quella di promozione della Convenzione 108 e della sua versione modernizzata, cd. Convenzione 108+.

Il Protocollo emendativo 223, che ha emendato l'originaria Convenzione 108 attualizzandone i principi in uno scenario fortemente mutato da nuove tecnologie e globalizzazione, conta, al 31 dicembre 2021, 43 firme e 15 ratifiche, tra cui quella dell'Italia, che ha depositato gli strumenti di ratifica l'8 luglio 2021. In base all'art.

23

37, par. 2, il Protocollo emendativo può entrare in vigore al raggiungimento di 38 ratifiche entro 5 anni dall'apertura alla firma (10 ottobre 2023). Considerata dunque la necessità di non disperdere l'importante lavoro di aggiornamento della Convenzione 108, il T-PD ha ritenuto particolarmente importante intensificare l'attività di sensibilizzazione degli Stati sull'importanza di una tempestiva ratifica. In occasione del 40° anniversario dall'apertura alla firma della Convenzione 108 (28 gennaio 1981) sotto la presidenza tedesca del Consiglio d'Europa è stata organizzata una conferenza dal titolo *Challenges of international data transfer from the perspective of the Convention 108+ and* GDPR, per esaminare i vantaggi della ratifica della Convenzione modernizzata sul piano dei flussi transfrontalieri dei dati anche in relazione ai requisiti dettati dal RGDP. Interventi della Presidente e dei membri del Comitato sono stati altresì dedicati alla promozione della Convenzione 108 e della 108+ anche in occasione della *Global privacy assembly* organizzata dall'Autorità messicana il 18-21 ottobre (cfr. par. 23.4).

Il 7 dicembre 2021 la Presidente del Comitato ha preso parte ad una riunione del gruppo *Legal cooperation* del Comitato dei Ministri (GR-J) volta anch'essa a sensibilizzare i rappresentanti sulla necessità di una tempestiva ratifica della 108+.

Sempre con riferimento alla Convenzione 108+, il Comitato ha proseguito il lavoro sui meccanismi di monitoraggio che in base al Protocollo emendativo saranno affidati al futuro Comitato convenzionale. Nella plenaria di novembre sono infatti stati finalizzati due importanti documenti: il primo descrive le procedure di valutazione (*evaluation*) dei futuri candidati ad accedere alla 108+ e di periodico riesame (*review*) per verificare la persistente aderenza ai principi della Convenzione stessa degli Stati aderenti; il secondo contiene il questionario da somministrare ai futuri candidati all'accessione e agli aderenti per poter svolgere le valutazioni. In base all'art. 36, par. 2, del Protocollo emendativo, a partire dall'apertura alla firma del Protocollo, qualunque nuova richiesta di accedere alla 108 deve essere accompagnata dalla richiesta di accessione alla 108+ rendendo dunque necessaria una pronta predisposizione dei meccanismi valutativi previsti da quest'ultima. Pertanto, la richiesta di accessione alla Convenzione 108+ inoltrata da Costa Rica su cui il Comitato sta lavorando, anche attraverso un dialogo con le autorità competenti costaricane, si fonda proprio sui criteri già finalizzati dal Comitato per valutare la corrispondenza della normativa nazionale ai principi della Convenzione modernizzata.

Riconoscimento facciale

Sono state adottate le linee guida in materia di riconoscimento facciale (T-PD (2020)03rev4), che forniscono una serie di indicazioni per garantire il rispetto dei diritti fondamentali e della dignità della persona.

Le linee guida sottolineano l'importanza di assicurare un dibattito pubblico e un approccio precauzionale in questo delicato settore e segnalano i particolari rischi derivanti dall'impiego di tecniche di riconoscimento facciale al fine di rilevare tratti della personalità, sentimenti o reazioni emotive dall'immagine del volto, stabilendone il divieto nelle procedure di assunzione di personale, nell'accesso ai servizi assicurativi e a all'istruzione, nonché il divieto dell'uso del riconoscimento facciale al solo scopo di determinare il colore della pelle di una persona, le convinzioni religiose o di altro tipo, il sesso, l'origine etnica, l'età, le condizioni di salute o le condizioni sociali.

Particolare attenzione è altresì rivolta all'impiego di sistemi di riconoscimento facciale da parte delle Forze dell'ordine, che dovrebbe essere consentito solamente ove strettamente necessario per prevenire un rischio imminente e grave alla sicurezza pubblica.

Le linee guida si rivolgono agli sviluppatori di tecnologie di riconoscimento facciale chiamati a prestare attenzione all'attendibilità degli algoritmi e all'accuratezza dei dati trattati, per evitare disparità e possibili ricadute discriminatorie e raccomandano

ad aziende e p.a. che intendano avvalersi di tecniche di riconoscimento facciale di garantire il rispetto dei principi in materia di protezione dati.

Ricordano infine il ruolo cruciale esercitato dalle autorità di supervisione che, in base all'art. 15 (3) della Convenzione 108+, devono essere consultate riguardo a proposte legislative e amministrative che comportino il trattamento dei dati personali mediante tecnologie di riconoscimento facciale, nonché prima di possibili sperimentazioni o utilizzi.

Linee guida sulla protezione dei dati nell'ambito delle campagne politiche

Nella plenaria del 19 novembre 2021 sono state adottate le linee guida sulla protezione dei dati nell'ambito delle campagne politiche. Preso atto del crescente uso della profilazione dell'elettorato per consentire campagne politiche sempre più mirate e dei rischi che ne derivano per la democrazia e le libertà degli elettori, le linee guida forniscono consigli pratici alle autorità di protezione dati, alle altre autorità di regolamentazione e alle organizzazioni politiche su come conciliare il diritto alla *privacy* dell'elettore e gli obblighi democratici che si fondano anche sulla comunicazione con l'elettorato ed auspicano forme di cooperazione tra le autorità per la protezione dei dati personali e le altre autorità di regolamentazione.

Raccomandazione in materia di profilazione

Il 3 novembre 2021 il Comitato dei ministri del Consiglio d'Europa ha adottato la raccomandazione (2021)8 volta a rispondere ai radicali cambiamenti nelle tecniche di profilazione nell'ultimo decennio e alla conseguente necessità di ulteriori tutele per proteggere i dati personali e la vita privata delle persone in tale settore. Il testo, che aggiorna la raccomandazione 2010(13), allinea i principi già sanciti in precedenza alla Convenzione 108 modernizzata. La nuova raccomandazione sottolinea in primo luogo la necessità che il rispetto dei diritti e delle libertà siano garantiti sia nel settore pubblico che in quello privato durante tutte le operazioni di profilazione.

La raccomandazione si riferisce alla profilazione come qualsiasi forma di trattamento automatizzato di dati personali, compreso l'uso di sistemi di apprendimento automatico, consistente nell'uso di dati per valutare determinati aspetti personali relativi a un individuo, in particolare per analizzare o prevedere aspetti riguardanti le prestazioni lavorative, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o spostamenti. Prende atto del fatto che le tecniche di profilazione possano avere un l'impatto sugli individui collocandoli in categorie predeterminate (molto spesso a loro insaputa) e che tale mancanza di trasparenza possa comportare rischi significativi per i diritti umani, in particolare per le persone vulnerabili, compresi i minori. Ricorda dunque i requisiti fissati dalla Convenzione 108+ ed in particolare la necessità di assicurare la presenza di un'adeguata base giuridica e di idonei criteri di trasparenza. Si sofferma sulla necessità che i titolari e, ove possibile, i responsabili del trattamento adottino misure adeguate a correggere i fattori di inesattezza dei dati e a limitare i rischi di errori e distorsioni inerenti alla profilazione, anche attraverso una rivalutazione periodica della qualità dei dati e delle deduzioni statistiche utilizzate, nonché dell'impatto dell'uso della profilazione sui diritti dell'interessato. Analogamente, ove i titolari acquisiscano dati o algoritmi da una terza parte, devono ottenere da essa la documentazione necessaria per verificare la qualità dei dati e degli algoritmi e la loro pertinenza rispetto alla finalità del trattamento.

Specifiche indicazioni sono poi fornite in merito alla profilazione basata su sistemi di IA che utilizzano processi di apprendimento automatico. Anche al fine di garantire la fiducia in tali sistemi, i titolari del trattamento dovrebbero garantire l'uso di sistemi affidabili e sicuri, sufficientemente robusti per evitare attacchi o altre manipolazioni dei dati o degli algoritmi e assicurare l'istituzione di procedure in caso di errori o incongruenze durante l'intero ciclo di vita del sistema.

23

Ai titolari del trattamento è inoltre richiesta una valutazione critica della qualità, natura rappresentativa e quantità dei dati utilizzati, eliminando i dati non necessari e tutti quelli che potrebbero falsare i risultati, nonché rispettando soglie specifiche di accuratezza dei risultati. Le applicazioni di IA dovrebbero infine consentire un controllo efficace, da parte degli interessati e dei gruppi interessati, degli effetti delle loro applicazioni su individui, gruppi e società.

Particolare attenzione viene prestata ai diritti degli interessati, quale quello di conoscere la logica del trattamento e di opporsi a decisioni automatizzate che abbiano conseguenze significative sulla persona. Infine, un altro elemento di novità, rispetto alla originaria raccomandazione, è la previsione di specifici requisiti per la profilazione da parte di soggetti pubblici, in particolare la necessità che tali trattamenti si fondino su un'adeguata base normativa e che siano assicurati idonei criteri di trasparenza.

Vaccinazione Covid-19, attestazioni e protezione dei dati

Il Comitato è tornato ad occuparsi delle misure di contenimento della pandemia Covid-19. Con la dichiarazione adottata il 3 maggio 2021 dal titolo "Vaccinazione Covid-19, attestazioni e protezione dei dati" (T-PD-BUR(2021)6rev2), il Comitato, pur riconoscendo l'utilità di strumenti quali i passaporti vaccinali e attestazioni simili anche al fine di riconquistare alcune delle libertà limitate a causa della pandemia e favorire le esigenze dell'economia, ha ricordato che i dati relativi alla salute, ai sensi dell'art. 6 della Convenzione modernizzata, richiedono garanzie aggiuntive e che per evitare discriminazioni tra persone vaccinate o meno è importante garantire l'alternatività di strumenti, quali l'attestazione della guarigione o dell'effettuazione di un test dal risultato negativo.

Anche in questo caso, come nei precedenti interventi sul bilanciamento tra esigenze di tutela della salute e libertà fondamentali (v. Relazione 2020, p. 237), il Comitato ha sottolineato che le misure adottate per contrastare la pandemia dovrebbero avere carattere temporaneo e collocarsi nell'ambito di strategie coerenti ed efficienti.

Secondo Protocollo alla Convenzione di Budapest sul *cybercrime*

Il Comitato consultivo della Convenzione 108 ha adottato in procedura scritta il 7 maggio 2021 il parere sul secondo Protocollo aggiuntivo alla Convenzione di Budapest sulla criminalità informatica (T-PD(2021)1rev3).

Il parere si concentra in particolare sulla previsione della bozza di Protocollo espressamente dedicata alla protezione dei dati personali (art. 14) riconoscendo il potenziale derivante dall'inclusione di un articolo autonomo sulla protezione dei dati e sottolineando la necessità che le Parti del Protocollo assicurino che a tali garanzie sia data un'effettiva applicazione. Invita le attuali Parti della Convenzione di Budapest e in futuro quelle del Protocollo ad accedere alla Convenzione 108+ o ad utilizzarla come riferimento giuridico per il trattamento dei dati personali che ricadano nell'ambito di applicazione della Convenzione sulla criminalità informatica e del suo Protocollo.

Fornisce infine una serie di osservazioni su altre parti del Protocollo in diretto collegamento con la disposizione sulla protezione dei dati o con l'eventuale futura attuazione di essa.

Art. 11 della Convenzione modernizzata

Il Comitato ha inoltre proseguito le attività di approfondimento rivolte alla stesura degli ulteriori documenti previsti dal programma di lavoro. Sempre avvalendosi di *report* di esperti scientifici è proseguita la riflessione sul trattamento dei dati personali nell'ambito dell'identità digitale, sull'art. 11 della Convenzione 108+ relativo ai criteri che devono accompagnare le possibili restrizioni ed eccezioni ai principi della stessa 108+ per garantire che, anche in questo caso, sia assicurato il rispetto dell'essenza del diritto alla protezione dei dati.

Scambi tra Stati per finalità fiscali

È altresì proseguito il lavoro sul tema degli scambi automatizzati di dati tra Stati per finalità amministrative e di tassazione, al fine di aggiornare il parere del T-PD

del 2014 (T-PD(2014)05), per tener conto delle novità nel frattempo intervenute in questi settori.

Nel corso dell'anno, su richiesta della rappresentante svizzera, il T-PD ha concordato sulla necessità di avviare un lavoro di aggiornamento, alla luce delle novità introdotte dalla Convenzione 108+ in materia di trasferimento dei dati e delle clausole contrattuali standard per i flussi di dati verso Paesi terzi, elaborate dal Consiglio d'Europa nel 1992 e riviste nel 2002.

Clausole contrattuali standard

Con riferimento ad ulteriori lavori del Consiglio d'Europa il 28 aprile 2021 è stata adottata la dichiarazione del Comitato dei ministri sulla tutela dei minori nell'ambiente digitale, che esorta gli Stati membri a migliorare la protezione della *privacy* e dei dati personali dei minori, con particolare riferimento ai dati relativi alla salute e a quelli raccolti in contesti educativi, specie nell'ambito della pandemia Covid-19. La dichiarazione segnala inoltre l'esigenza di intensificare gli sforzi affinché gli Stati ratifichino prontamente la Convenzione 108+, garantendo così una tutela adeguata alla protezione dei dati, anche relativa ai minori, nonché di promuovere attivamente le linee guida sulla protezione dei minori nei contesti educativi, adottate dal Comitato consultivo della Convenzione 108 il 20 novembre 2020.

Tutela dei minori nell'ambiente digitale

In occasione della Giornata europea della protezione dei dati (28 gennaio 2021) è stato assegnato il Premio Stefano Rodotà istituito dal Comitato per ricordare il grande giurista. Il Premio, destinato a ricercatori e studenti e funzionale alla valorizzazione di progetti di ricerca innovativi e originali in tema di protezione dati, è stato assegnato a Gabriel Kasper per il suo lavoro sulla profilazione in ambito lavorativo. La giuria ha inoltre conferito la speciale menzione a Ignacio Cofone per il suo articolo sulla cd. *ownership* dei dati personali.

Premio Stefano Rodotà

Sempre nell'ambito del Consiglio d'Europa è proseguita l'attività del CAHAI, il Comitato *ad hoc,* istituito dal Comitato dei ministri con l'incarico di esaminare la fattibilità 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 e il cui mandato si è concluso il 31 dicembre 2021 (cfr. cap. 17).

CAHAI-Comitato *ad hoc* sull'IA

È proseguita l'intensa attività dell'Autorità in ambito OCSE, in particolare attraverso la partecipazione al DGP (*Working Party on Data Governance and Privacy*), di cui la rappresentante del Garante, è vice presidente dal 2012 (già WPSPDE - *Working Party on Security and Privacy in Digital Economy*) ed ha conservato la vicepresidenza per il 2022.

OCSE-DGP (Gruppo di lavoro *Data Governance and Privacy*)

Si è tenuto (21 e 22 giugno) un terzo *workshop* virtuale sul tema Covid-19: "Un anno dopo: affrontare le implicazioni per la *governance* dei dati e la *privacy* della pandemia Covid-19 e tracciare la strada per il recupero" organizzato con la partecipazione della Assemblea globale della *privacy* (GPA) a cui l'Italia ha partecipato in prima linea con un intervento dell'avv. Guido Scorza, volto a presentare la gestione italiana della pandemia nel rispetto della protezione dei dati. Resta negli intenti del DGP l'organizzazione di futuri *workshop* tematici, tenendo allerta alta per i possibili futuri rischi di compressioni della *data protection* nella lotta alla pandemia.

DGP e lotta alla pandemia

Le due riunioni plenarie del DGP (7-13 aprile e 16-22 novembre), cui si sono come di consueto aggiunte le relative riunioni del *Bureau* (il gruppo ristretto del DGP) sono state anche per il 2021 caratterizzate da un'altissima adesione delle delegazioni dei Paesi membri, anche agevolata dalla partecipazione da remoto e dalla forte motivazione data dal comune obiettivo di vincere la pandemia nel rispetto della *privacy* delle persone.

Linee guida dell'OCSE sulla *privacy*

In primo piano si pone anche per 2021 il lavoro di revisione delle linee guida dell'OCSE sulla *privacy* del 2013 (*Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal*

23

Data) portato a termine con l'adozione da parte del Consiglio OCSE della relazione sulla revisione delle linee guida *privacy* e relativi lavori di *follow on.* Inoltre si è registrato un forte *trend* positivo nei Paesi che hanno gestito la pandemia, facendo tesoro dei principi globalmente condivisi nelle *Privacy Guidelines.* Nel corso dell'anno è altresì proseguito il lavoro di revisione al commentario addizionale delle linee guida *privacy* (*Supplementary explanatory memorandum*) ed è stato concordato il piano di lavoro per la revisione del *memorandum* stesso, compreso il calendario provvisorio.

Raccomandazione OCSE sulla protezione dei minori *online*

Quanto alle raccomandazioni adottate nel 2021, si evidenzia innanzitutto quella sui minori *online* (*Recommendation of the Council on children in the digital environment*) che aggiorna la precedente del 2012. Essa conferma i principi per garantire il più possibile, agli utenti minorenni, un ambiente digitale utile e sicuro quali il rispetto dei diritti umani; la resilienza; l'inclusione; la condivisione della responsabilità, la cooperazione, anche internazionale ed un impegno proattivo degli *stakeholders.* Parallelamente, incoraggia le azioni politiche volte a favorire una legislazione e regolamentazione adeguata ed una opportuna alfabetizzazione digitale. Il documento annesso alla raccomandazione definisce delle linee guida per i fornitori di servizi digitali, che possono svolgere un ruolo essenziale nella protezione dei minori *online,* a partire dall'adozione di criteri di sicurezza già nella progettazione dei sistemi di fornitura dei contenuti (*safety by design*), o garantendo informazioni accessibili e trasparenti, l'utilizzo di un linguaggio chiaro e adatto ai bambini e l'attenzione alla loro *privacy.* La raccomandazione, come tutti gli strumenti di *soft-law,* non è vincolante, ma il tema è molto sentito e potrebbe attirare anche Paesi non OCSE, eventualmente anche attraverso il G20.

Il 18 novembre la prof.ssa Ginevra Cerrina Feroni, vice presidente del Garante, intervenendo ad un evento virtuale OCSE di alto livello per il lancio della *Recommendation on children in the digital environment,* ha illustrato la recente esperienza del Garante italiano in tema di minori nell'ambiente digitale. In particolare la Professoressa si è soffermata sulla procedura avviata dal Garante nei confronti di TikTok a partire dal provvedimento d'urgenza adottato il 22 gennaio 2021, a seguito del suicidio della bambina di dieci anni strangolatasi per una *challenge* indetta da suoi coetanei sulla piattaforma e sottolineato l'intento del Garante di proseguire la battaglia di sensibilizzazione nei confronti delle altre piattaforme anche se non stabilite in Italia. La Professoressa ha anche raccomandato che i bambini siano sempre guidati dai genitori quando hanno in mano un dispositivo. I genitori dovrebbero essere consapevoli di ciò che i loro figli vedono e sentono su internet, chi incontrano e cosa condividono di sé stessi. "Parla con i tuoi figli, usa gli strumenti per proteggerli e tieni d'occhio le loro attività" dovrebbe diventare il mantra di ogni genitore "responsabile" (cfr. par. 9.3).

***Data Governance:* *Enhanced Access and Sharing of Data* (EASD)**

Nel corso dell'anno è stata altresì adottata la raccomandazione sul rafforzamento dell'accesso e della condivisione dei dati (*Recommendation of the Council on Enhancing Access to and Sharing of Data* - EASD). Il testo di raccomandazione EASD riveste grande importanza in quanto la stessa mette in luce come la EASD possa favorire numerosi vantaggi sociali ed economici, attraverso la condivisione di dati di natura scientifica, incluso quelli relativi al contrasto al Covid-19; tra i suoi obiettivi: promuovere la coerenza tra i quadri di *governance* dei dati a livello nazionale e specifici per settore, per migliorarne l'accesso e la condivisione, anche tra diverse giurisdizioni; garantire la coerenza tra le linee guida dell'OCSE, in base agli standard del CDEP (*Digital Economy Policy*), del CSTP (*Committee for Scientific and Technological Policy*) e del PGC (*Public Governance Committee*); consentire la collaborazione e lo sfruttamento di nuove potenziali fonti di dati, anche nell'IA.

Accesso affidabile dei governi ai dati dei privati

Altro tema che ha destato grande attenzione e richiesto un notevole impegno è stato quello dell'accesso affidabile dei governi ai dati detenuti dai privati (*trusted government access to data*). In seguito alla dichiarazione del Cdep del 22 dicembre 2020, nel 2021 è concretamente iniziato il lavoro del Gruppo OCSE di redazione sul tema del *trusted government access to data.* Il lavoro 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 rendono necessarie una *governance* adeguata e idonee garanzie sul modo in cui i governi accedono ai dati personali del settore privato allo scopo di creare fiducia e ridurre al minimo gli ostacoli ai flussi dei dati stessi.

Il Garante e il Maeci hanno rappresentato l'Italia in seno al Gruppo di redazione ampliato (*Expanded Drafting Group*-EDG) che si è riunito frequentemente nel corso del 2021, raggiungendo convergenze sulle prime garanzie per un accesso realmente *trusted* (basi giuridiche; obiettivi legittimi; autorizzazioni; limiti al trattamento; trasparenza; *oversight* e *redress*). I delegati italiani hanno cercato di chiarire che i sette principi individuati dal Comitato Cdep dell'OCSE si applicano a tutte le forme di accesso da parte dei governi (senza differenze tra accesso obbligato e non obbligato) e hanno suggerito una formulazione per illustrare l'applicazione dei principi a situazioni specifiche (anche fornendo, nel tentativo di destare il più ampio consenso, esempi relativi ad accesso obbligato). L'auspicio è che la futura adozione di questi principi come raccomandazione OCSE possa servire a facilitare i flussi di dati con solide garanzie in linea con il RGPD, nonché a promuovere il dialogo globale sul *Data Free Flow* basato su effettive comunanze (*commonalities*) tra i Paesi membri.

Global Privacy Enforcement Network (GPEN)

Nel 2021 è stato lanciato il *Privacy Sweep* 2020-2021 (indagine non effettuata nel 2020 a causa della pandemia), promossa dal *Global Privacy Enforcement Network* (www.privacyenforcement.net), la rete internazionale nata nel 2010 per rafforzare la cooperazione tra le autorità di protezione dati di diversi Paesi del mondo. L'attività di *sweep* (indagine a tappeto), a differenza del passato, è stata svolta attraverso la sottoposizione di un questionario rivolto alle autorità partecipanti sul modo in cui la comunità globale delle autorità di protezione dati si sono impegnate con i governi nazionali, per identificare e comprendere i rischi associati alle iniziative relative al Covid-19 e per migliorare la conformità con le leggi sulla protezione dei dati personali.

Allo *Sweep* 2020-2021 hanno partecipato, oltre a quella italiana, altre 19 autorità garanti della *privacy* di vari Paesi del mondo.

23.4. *Le Conferenze internazionali ed europee*

Global Privacy Assembly (GPA)

La Conferenza annuale della protezione dati, nel 2021 dedicata al tema "*Privacy* e protezione dati: un approccio umano centrico", organizzata dalla Assemblea globale della *privacy,* dal Comitato esecutivo GPA e ospitata dall'Autorità messicana (Inai), si è tenuta dal 18 al 21 ottobre in modalità ibrida. Come di consueto la Conferenza si è articolata in una sessione aperta (*open session*) e una sessione ristretta (*closed session*) a cui hanno partecipato solo le autorità di protezione dati. La prima si è concentrata principalmente sulla convivenza tra lo sviluppo delle nuove tecnologie dell'informazione e i diritti umani, attraverso *keynote lectures, panel* specifici e sessioni parallele. Particolare attenzione è stata dedicata al tema *privacy* e pandemia, con *focus* sui passaporti vaccinali e simili, a quello dei flussi di dati e delle salvaguardie che devono essere adottate per garantire la necessaria fiducia; all'internet delle cose; all'IA, ai diritti digitali e le politiche inclusive. Nella sessione chiusa (20 e 21 ottobre), è stato discusso il tema dell'accreditamento dei nuovi membri GPA e degli osservatori,

23

dell'adozione della lista dei membri votanti ed è stato presentato e adottato il piano strategico della GPA per il 2021-2023, nonché annunciati i risultati delle votazioni sui *report* dei lavori dei vari sottogruppi della GPA. Nella giornata del 20 ottobre la vice presidente del Garante prof.ssa Ginevra Cerrina Feroni nel *panel* sulle lezioni apprese dalla pandemia ha evidenziato la suprema importanza del ruolo delle autorità per la *privacy* nel fornire guida e assistenza ai governi, alle organizzazioni e alle altre parti interessate su come gestire e condividere adeguatamente i dati personali nel contesto della pandemia, riconoscendo che, man mano che i piani di risposta e di recupero diventano operativi, è importante che le misure per adattarsi alla "nuova normalità" tengano pienamente conto dei principi fondamentali in materia di protezione dei dati e di tutte le necessarie garanzie, affinché anche in un momento così difficile i dati siano trattati con la massima proporzionalità e per quanto necessario. Sono state altresì adottate tutte le risoluzioni presentate: la risoluzione sui *children's digital rights,* di cui il Garante è stato coautore insieme alla Cnil; la risoluzione sulla direzione strategica dell'Assemblea 2021-23 (UK); la risoluzione sul futuro della Conferenza (UK); la risoluzione sulla condivisione dei dati per il bene pubblico (Filippine); la risoluzione sull'accesso del governo ai dati, la *privacy* e lo stato di diritto (Cnil, Canada e Giappone).

GPA e Covid-19

Al fine di rafforzare la capacità della GPA nel fornire risposte adeguate alle problematiche relative alle misure adottate in tutto il mondo per contenere la pandemia e ai connessi profili di *privacy,* la 42ª sessione della GPA tenutasi nell'ottobre 2020 aveva deciso di istituire un Gruppo di lavoro temporaneo sul Covid-19 con il mandato di fornire in merito orientamenti ai membri e agli osservatori della GPA, ai governi, alle organizzazioni e ad altri *stakeholder.* Il Gruppo di lavoro, a cui ha partecipato l'Autorità, nel corso del 2021, ha organizzato *workshop* e *webinar* tematici sul tema e ha elaborato una dichiarazione congiunta sull'utilizzo dei dati sanitari al fine di facilitare i viaggi internazionali e nazionali, che è stata adottata dal Comitato esecutivo GPA il 31 marzo 2021 (https://globalprivacyassembly.org/gpa-executive-committee-joint-statement-on-the-use-of-health-data-for-domestic-or-international-travel-purposes/). Tra le misure di risposta alla pandemia, il Gruppo ha individuato talune *best practices* sotto il profilo della protezione dei dati che sono state raccolte nella seconda parte del Compendio della GPA. A conclusione del suo mandato, il Gruppo di lavoro ha proposto una risoluzione, poi adottata dalla Conferenza annuale della protezione dei dati del 2021, per continuare e ampliare il proprio mandato tramite l'istituzione di un Gruppo di lavoro sulla condivisione dei dati per il bene pubblico.

G7 delle autorità di protezione dati

Nel 2021 il Garante ha partecipato al primo *meeting* delle autorità di protezione dati del G7, coordinato dall'Autorità britannica (Ico), svoltosi il 7 e 8 settembre con la partecipazione delle Autorità di protezione dei dati di Canada, Francia, Germania, Giappone, Gran Bretagna, Italia e Stati Uniti d'America e, in veste di ospiti, rappresentanti dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) e del *Forum* economico mondiale (WEF), con la presenza, per il Garante, della prof.ssa Ginevra Cerrina Feroni. Obiettivo dell'incontro è stato quello di individuare soluzioni condivise per rispondere alle più rilevanti questioni collegate alla protezione dei dati personali nell'attuale panorama globale (tecnologie emergenti e emergenza pandemica). Il Garante ha evidenziato due importanti questioni poi recepite nel comunicato finale: la riaffermazione della centralità delle autorità di protezione dati come presidio dei diritti fondamentali collegati alla protezione dati; la necessità di valorizzare e promuovere le competenze delle autorità nel campo dell'IA e dei futuri sviluppi. A chiusura del *meeting,* i Garanti hanno concordato sulla necessità di proseguire con cadenze regolari il positivo dialogo avviato, individuando l'Italia quale Paese ospitante l'incontro ufficiale previsto per il 2024.

23.5. *I progetti per l'applicazione del RGPD finanziati dall'UE*

Gemellaggio con l'Albania *(Twinning)*

Il 15 dicembre 2021, con un'estensione di due mesi e mezzo della durata originariamente prevista, si sono concluse le attività del progetto europeo *Twinning* (gemellaggio) con l'Albania, avviate nell'ottobre del 2020, e coordinate dal Garante, in qualità di *leader* di progetto, con il coinvolgimento della *Ludwig Boltzmann Gesellschaft-Institute of Human Rights* (BIM) (in qualità di *junior partner*) e Csi-Piemonte (Consorzio per il sistema informativo).

I *twinnings* sono progetti finanziati dall'UE che hanno come obiettivo di carattere generale quello di assicurare uno sviluppo moderno ed efficiente delle amministrazioni dei Paesi beneficiari.

L'obiettivo principale del progetto di gemellaggio è stato quello di rafforzare le competenze istituzionali del Commissario albanese per l'informazione e la protezione dei dati (Idp) sulla vigilanza e il monitoraggio della protezione dei dati personali, sia nel settore pubblico che privato, al fine di armonizzare la legge albanese sulla protezione dei dati con il relativo *acquis* dell'UE e promuovere l'adesione della Repubblica di Albania nell'UE.

A causa della pandemia e in considerazione delle relative misure restrittive concernenti i viaggi all'estero in vigore nei Paesi coinvolti, tutte le attività previste sono state eseguite, dall'inizio alla fine del progetto, in modalità da remoto.

Nonostante la situazione pandemica, tutti gli obiettivi previsti sono stati raggiunti senza alcun ritardo.

24 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 una *liason* in proposito con ISO, l'Autorità ha seguito lo sviluppo delle seguenti norme tecniche:

- ISO 27555 - *Establishing a PII deletion concept in organizations,* che fornisce linee guida per la cancellazione dei dati personali che includono la classificazione dei dati, la definizione dei tempi di cancellazione, dei periodi di mantenimento, delle classi di cancellazione, dei requisiti di implementazione nonché processi e responsabilità;
- ISO 27556 - *User-centric framework for the handling of PII based on privacy preference* che definisce un quadro di riferimento per la gestione delle scelte riguardanti le informazioni personali con un approccio *user-centric;*
- 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*);
- ISO TS 27559 - *Privacy enhancing data de identification framework,* che fornisce una guida sull'implementazione della de-identificazione e la valutazione dei rischi di re-identificazione relativi al ciclo di vita dei dati de-identificati;
- ISO 27557 - *Organizational privacy risk management,* che fornisce linee guida per la gestione del rischio *privacy* delle organizzazioni titolari e responsabili del trattamento integrando la valutazione dell'impatto sugli interessati nel *privacy risk management program* delle medesime;
- ISO TS 27560 - *Consent Receipt and Record Standard,* che definisce una struttura e formato comune per *consent receipt* e *consent record;*
- 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 dà supporto alle organizzazioni al fine di definire un modello e metodi standardizzati per la *privacy engineering* di sistemi complessi.

Collaborazione è stata assicurata nell'ambito del *Project Committee* (PC) 317 di ISO, istituito dal *Technical Management Board* a febbraio 2018, per lo sviluppo di una norma tecnica internazionale su *Consumer protection: Privacy by design for consumer goods and services* e nell'ambito del Comitato tecnico 215 di ISO durante i lavori dell'*Ad Hoc Group Application of AI Technologies in Health Informatics* e per la stesura del rapporto conclusivo.

L'Autorità inoltre ha contribuito all'elaborazione di norme tecniche europee 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.* In particolare l'Autorità 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) per l'elaborazione di norme tecniche per la *Privacy by design and by default,* individua obiettivi, requisiti di protezione dati e linee guida per supportare sviluppatori, produttori e fornitori di servizi e prodotti nell'implementazione dei principi 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 RGDP;
- 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;
- JT013037 - *Privacy Information Management System per ISO/IEC 27701 - Refinements in European context,* che adatta il *framework* internazionale offerto dalla ISO 27701 nel contesto europeo.

Del pari è proseguita la collaborazione con le diverse commissioni tecniche UNINFO, l'ente di normazione federato con UNI (Ente nazionale italiano di unificazione).

25 L'attività di comunicazione, informazione e di rapporto con il pubblico

25.1. *La comunicazione del Garante: profili generali*

Nel 2021 la raccolta di grandi quantità di dati per arginare il propagarsi della pandemia e dell'invasività delle tecnologie di tracciamento ha fatto emergere con chiarezza la necessità di individuare nuove forme di tutela soprattutto in relazione alla tecnologia digitale. Il massiccio ricorso al lavoro agile, alla didattica a distanza, alle videoconferenze, allo *shopping online,* all'*e-banking* hanno accentuato i rischi di violazioni e di usi impropri dei dati personali.

Il Garante, chiamato a rispondere tempestivamente all'elevato numero di richieste di pareri e di chiarimenti, provenienti dal Governo, dalle p.a. centrali e periferiche e da soggetti privati ha significativamente incrementato la sua attività. Ha dialogato con spirito collaborativo ricercando il delicato equilibrio tra sicurezza sanitaria collettiva e tutela delle libertà individuali, e vigilato per scongiurare il rischio che le limitazioni – pur talvolta necessarie – potessero diventare irreversibili e sproporzionate minando il diritto costituzionale alla *privacy.*

In questo scenario l'azione di comunicazione istituzionale del Garante ha svolto un ruolo fondamentale nel fornire un'informazione chiara ed accurata e nello sviluppare forme e strumenti sempre più efficaci di divulgazione e di sensibilizzazione sulle tematiche connesse alla protezione dei dati personali. L'attività si è svolta in stretto contatto con i *media* nazionali ed internazionali per diffondere con tempestività le misure adottate dall'Autorità, assicurando una ampia e corretta interpretazione delle norme e l'invio di materiale documentale.

Si pensi soltanto alla diffusione dei tanti provvedimenti adottati, pareri resi e indicazioni fornite dall'Autorità nel 2021, in particolare in ambito sanitario: sistemi di tracciamento e profilazione dei contagi (*app* IO) idonei a rilevare lo stato di salute degli interessati; test sierologici; banche dati genetiche; raccolta dei dati sanitari per ricerca e cura; informazione scientifica; vaccinazioni sui luoghi di lavoro; applicazioni per le certificazioni verdi (*green pass*).

Contestualmente va ricordato il lavoro svolto sui *social network,* sui pericolosi effetti del *revenge porn,* sul riconoscimento facciale e sui rischi di sorveglianza di massa, sul *telemarketing* aggressivo, sui diritti dei *rider,* per citare solo alcuni ambiti di intervento.

È stata potenziata la presenza sugli organi di stampa, sui siti web e sui canali *social* Twitter, Linkedin, Telegram, Youtube e Instagram dell'Autorità, attraverso campagne informative, *tutorial, spot* e schede FAQ.

Le statistiche mostrano come il 2021 sia stato un anno particolarmente difficile sul fronte della *cybersecurity* e della protezione dei dati personali. Proprio sulla scarsa attenzione alle misure di sicurezza da parte di p.a., imprese e piattaforme *online,* l'Autorità ha incrementato l'attività di vigilanza e intervento, anche a seguito di casi di particolare gravità, quali i *data breach* subìti dalla Regione Lazio, dal Servizio sanitario della Regione Toscana, dalle Asl di Napoli e Padova, dall'Aifa, dalla Siae; o, in ambito internazionale, da Facebook o da Linkedin.

L'attività di informazione si è di conseguenza concentrata su vari aspetti del *cybercrime* – dal *ransomware,* al *phishing;* alle *app* pirata che rubano i dati ai *software* per

lo spionaggio – producendo e diffondendo su tali temi numerosa documentazione multimediale *ad hoc.* Uno specifico *focus* di indagine e informazione è stato dedicato ai rischi di raccolta di informazioni da parte delle *app* tramite l'uso dei microfoni inseriti negli *smartphone* (https://www.gpdp.it/temi/smartphone/microfoni).

Un'apposita campagna è stata avviata per sensibilizzare gli utenti su come impostare sicure *password* (https://www.gpdp.it/temi/cybersecurity/password).

Il Garante ha continuato a vigilare sui *social network,* con particolare attenzione ai minori. Come già in passato, sono stati oggetto di campagne di comunicazione specifiche i rischi legati ad un uso poco consapevole della rete quali: il cyberbullismo e il *revenge porn,* il *sexting,* il *deep fake,* l'*hate speech,* promuovendo in molte occasioni una vera e propria educazione digitale, per rendere tutti, e soprattutto i più giovani, consapevoli delle grandi opportunità, ma anche dei rischi che caratterizzano la sfera digitale.

Di grande rilevanza sociale anche l'attività di informazione riguardante il *telemarketing* aggressivo da parte di vari operatori; il tracciamento attraverso i *cookies* da parte dei gestori dei siti; la conservazione dei dati (*data retention*); il contrasto all'evasione fiscale e la fatturazione elettronica; la lotteria degli scontrini e il *cashback;* la carta europea della disabilità; il controllo dei lavoratori e i diritti dei *rider;* le *bodycam* e il riconoscimento facciale.

I temi dell'IA sono stati approfonditi, con il convegno "AI *Anthology.* Profili giuridici, economici e sociali dell'intelligenza artificiale" e con una serie di video in cui i componenti del Collegio dell'Autorità illustrano i possibili rischi per la *privacy* collegati all'uso di tecnologie basate sull'intelligenza artificiale (https://www.gpdp.it/temi/intelligenza-artificiale).

In seno al gruppo di comunicatori istituito presso l'EDPB per realizzare attività coordinate di comunicazione, anche con la condivisione di comunicati stampa e la gestione comune dei casi con valenza transnazionale, si sono tenute 11 riunioni a distanza e molteplici attività intermedie di coordinamento. Il Garante ha contribuito direttamente a numerose attività, quali, tra le altre: la redazione della sezione relativa al Garante italiano del "EDPB 2021 *Annual Report";* la produzione delle *news enforcement* per la sezione italiana del sito EDPB; la collaborazione alla stesura *Executive Summary* EDPB; il lavoro comune per lo sviluppo di una guida sull'art. 65 del RGPD per tutti i Paesi europei.

Nell'ambito dell'attività internazionale nel settore della comunicazione, della formazione e dell'informazione, il Garante ha partecipato al *Twinning project – Training* – con attività seminariali di formazione per l'omologa Autorità albanese nell'ambito del progetto *Institution-building for alignment with the union acquis on the protection of personal data.* Ha collaborato con le attività del GPEN, con il *Digital Education Working Group* (DEWG) della *Global Privacy Assembly* (GPA) e con altri organismi e organizzazioni internazionali (cfr. par. 23.5).

A ottobre sono stati pubblicati i risultati del *Privacy Sweep Day* 2020-21, l'indagine annuale del GPEN (*Global Privacy Enforcement Network* di cui fa parte anche il Garante italiano). Lo studio ha rilevato che tutte le autorità di protezione dati interpellate hanno svolto un ruolo attivo nel valutare le implicazioni per la *privacy* delle soluzioni e delle iniziative adottate ai fini della lotta al Covid-19.

Lo *Sweep* ha preso in esame le interazioni fra le autorità di protezione dati e i governi nazionali, attraverso le attività finalizzate a individuare e comprendere i rischi associati alle iniziative di contenimento del Covid-19 e le raccomandazioni formulate al fine di migliorare l'osservanza delle norme in materia di *privacy* e protezione dei dati. Alcune autorità, tra le quali il Garante italiano, hanno avviato interventi finalizzati a garantire il rispetto delle norme, a seguito dei reclami ricevuti.

25

L'analisi delle risposte fornite dalle autorità ha indicato che al centro dell'attenzione sono state le *app* di tracciamento dei contatti per dispositivi mobili, ma le autorità si sono confrontate anche con altre iniziative quali l'impiego di braccialetti elettronici, i registri vaccinali, e i registri nazionali dei movimenti transfrontalieri (cfr. par. 23.3).

Allo *Sweep,* oltre al Garante italiano, hanno partecipato 20 autorità di protezione dei dati dall'Europa, dalle Americhe, dall'Oceania, dall'Asia e dal Medio Oriente.

25.2. *I prodotti informativi*

Nel 2021 sono stati diffusi 85 comunicati stampa e 14 *Newsletter.*

La *Newsletter* del Garante, giunta al XXIII anno di diffusione (per un totale di 485 numeri e 1.651 notizie) è pubblicata sul sito istituzionale dell'Autorità e distribuita esclusivamente via *e-mail* a redazioni, professionisti, amministrazioni pubbliche, imprese e a singoli cittadini che ne fanno esplicita richiesta compilando il *form* presente sul sito. Al 31 dicembre la lista di distribuzione contava circa 17.300 destinatari effettivi.

Inserita in un piano periodico di invii, la *Newsletter* rappresenta – ancora oggi in tempi di *social* – uno strumento efficace per una costante condivisione di notizie e approfondimenti sui più importanti provvedimenti adottati dall'Autorità, sulla sua attività in ambito nazionale, europeo ed internazionale, e sulle molteplici iniziative legate alla protezione dei dati personali e alla tutela dei diritti fondamentali, fornendo un vasto panorama di questioni e problematiche.

La redazione opera una scelta tra i numerosi provvedimenti adottati dal Garante, e rielabora in chiave giornalistica quelli di maggiore interesse generale. Nel corpo di ciascuna notizia sono inseriti *link* che rimandano direttamente ai provvedimenti citati, facilitando così l'approfondimento dell'argomento trattato. Sul sito è possibile consultare l'archivio tematico che raccoglie i 23 anni di articoli prodotti dalla redazione nonché l'archivio dei comunicati stampa.

25.3. *Il sito istituzionale, i prodotti multimediali e le pubblicazioni*

Nel 2021 si è provveduto alla ristrutturazione e lancio del nuovo sito istituzionale; sono state ideate e sviluppate 14 campagne informative, 21 video e *teaser* informativi, 13 infografiche; create o totalmente ristrutturate con interventi su contenuti, grafica, usabilità ed organizzazione 58 pagine tematiche.

Dal marzo 2021 è stato attivato il profilo Twitter del Garante della *privacy,* @GPDP_IT. Questo nuovo canale di informazione si è dimostrato uno strumento di grande efficacia, raggiungendo a fine anno gli oltre ottomila *follower*: ha consentito una proficua e stimolante interazione con gli utenti e permesso di promuovere presso il pubblico la conoscenza delle norme e di sviluppare consapevolezza sul corretto uso dei dati personali.

A giugno è stato definitivamente attivato il nuovo sito dell'Autorità con nuovi strumenti, linguaggi, contenuti e canali per raggiungere la comunità e supportare l'azione dell'Autorità, nello spirito del nuovo Regolamento. È stato portato a termine il progetto di revisione completa del *thesaurus* tematico per aggiornare le voci alle novità normative e tecnologiche, riorganizzarle e ridurne il numero al fine di migliorare il risultato delle ricerche. Il progetto è proseguito nel corso dell'anno con l'aggiornamento o lo sviluppo di nuove sezioni di particolare interesse per gli utenti,

come quello delle FAQ, di temi come quello sul Covid-19 o il cyberbullismo, e migliorando le funzionalità del motore di ricerca.

A marzo il Garante ha lanciato il *contest* "Informative più chiare grazie alle icone? È possibile", con lo scopo di rendere le informative *privacy* più semplici, chiare e immediatamente comprensibili, utilizzando simboli e icone. L'iniziativa era rivolta a sviluppatori, addetti ai lavori, esperti, avvocati, *designer,* studenti universitari e a chiunque fosse interessato a cimentarsi nell'individuare e proporre un set di simboli o icone capaci di esemplificare gli elementi che, a norma degli artt. 13 e 14 del RGPD, devono essere contenuti nell'informativa.

I progetti vincitori sono stati resi disponibili sul sito del Garante alla pagina https://www.gpdp.it/temi/informativechiare, e sono utilizzabili da chiunque secondo i termini della licenza CC BY.

A seguito dell'approvazione delle nuove linee guida sui *cookie* (provv. 10 giugno 2021, n. 231, doc. web n. 9677876), l'Autorità ha predisposto sul tema un *booklet* che sintetizza i principali punti del provvedimento (https://www.gpdp.it/temi/cookie).

Prodotti multimediali

I numerosi prodotti multimediali progettati per le campagne informative, anche attraverso l'incremento della produzione audiovisiva e l'uso di nuove tecniche (come lo *storytelling* e nuovi formati *stories* sui *social*), hanno riguardato aspetti di vasto interesse sociale: TikTok (video); *revenge porn* (una pagina informativa e un *vademecum*); cyberbullismo (un video e un *vademecum*); Le parole dell'AI (4 video); 3 anni di GDPR (una pagina informativa e 4 video); I diritti di accesso (una pagina informativa e un *booklet*); I tuoi dati sono un tesoro (un video in due versioni declinate per la tv e i *social media*); Campagna di promozione dei risultati del *contest* "Informative chiare"; "Dalla tua parte. L'impegno del Garante in difesa dei diritti delle persone" (un video e una pagina informativa); "*Smartphone:* spegni il microfono, accendi la *privacy*" (un video e una pagina informativa); *cookie* (una pagina informativa e FAQ); assistenti digitali (aggiornamento e arricchimento del *vademecum*) "Suggerimenti per creare e gestire *password* a prova di *privacy*" (pagina informativa); "e-state in *privacy.* Informazioni utili su *selfie* e foto, protezione di *smartphone* e *tablet,* acquisti *online,* uso di *app, chat* e *social network* quando si è in vacanza" (pagina informativa e campagna informativa mirata sui *social* con *focus* su vari aspetti).

L'utilità dei prodotti realizzati e l'interesse suscitato sono stati testimoniati dall'elevato numero di visualizzazioni e interazioni (*like,* condivisioni, commenti positivi e menzioni) registrate sui profili *social* del Garante, ma anche da vari articoli di apprezzamento apparsi sui giornali o su siti di esperti nel campo della comunicazione web. Complessivamente i 5 profili (Linkedin, Instagram, Telegram, Youtube e Twitter) hanno raggiunto oltre 70.300 *followers.* Sul canale YouTube utilizzato per la promozione dei video, video *tutorial,* campagne informative e per la valorizzazione di interviste e interventi audiovisivi dei membri del Collegio, le visualizzazioni complessive hanno raggiunto quota 510.000.

Pubblicazioni

Per quanto riguarda il settore editoriale, nella Collana del Garante, "Contributi", dedicata a testi di approfondimento sulle problematiche riguardanti la protezione dati e la tutela della dignità della persona, si sono aggiunti 2 volumi: "*Privacy* e neurodiritti. La persona al tempo delle neuroscienze" e "Spazio cibernetico bene comune. Protezione dei dati, sicurezza nazionale", che raccolgono i contributi degli studiosi ed esperti intervenuti ai convegni organizzati dall'Autorità in occasione delle Giornate europee per la protezione dei dati personali del 2021 e del 2020. I volumi sono disponibili anche in formato elettronico (doc. web nn. 9697621 e 9418861).

Nel 2021 sono stati pubblicati i primi 10 numeri del magazine *online* GPDPDigest, il nuovo prodotto di informazione che raccoglie mensilmente i

25

principali interventi dell'Autorità presentando anche una sintesi delle principali attività di *European Data Protection Board* e EDPS - *European Data Protection Supervisor*. Tutti i numeri pubblicati sono consultabili sul sito web alla pagina https://www.garanteprivacy.it/home/stampa-comunicazione/gpdpdigest.

25.4. *I video istituzionali*

Nel 2021 è stata potenziata l'attività di comunicazione attraverso *spot* destinati a canali radio televisivi *social*. L'Autorità ha realizzato uno *spot* istituzionale che utilizza un linguaggio nuovo per raccontare l'attività del Garante e il ruolo svolto da quasi venticinque anni a fianco delle persone per difendere la loro riservatezza e la loro libertà, spiegando il valore dei dati personali e l'importanza della loro protezione nella vita di tutti i giorni. Nel mese di marzo 2021 una versione ridotta dello *spot* è stata trasmessa sui canali Rai utilizzando gli spazi per la comunicazione istituzionale messi a disposizione dalla Presidenza del Consiglio dei ministri (la versione televisiva dello *spot* è disponibile anche sul canale Youtube istituzionale del Garante: https://www.youtube.com/watch?v=wpEW5QAKPz4). Sia il video che lo *spot* sono stati realizzati con la collaborazione di un'agenzia specializzata.

A febbraio il Garante – in collaborazione con Telefono Azzurro – ha realizzato uno *spot* "Se non hai l'età i *social* possono attendere" (https://www.youtube.com/watch?v=9nckmslOaaU&ab_channel=Garanteperlaprotezionedeidatipersonali) realizzato con l'obiettivo principale di richiamare i genitori a svolgere un ruolo attivo di vigilanza sui loro figli al momento dell'iscrizione ai *social* a partire da Tik Tok, a cui il Garante ha imposto misure sulla *age verification* (doc. web n. 9533424) dopo il tragico caso della bambina di Palermo (doc. web n. 9524224).

La campagna informativa è andata in onda sulle reti della Rai, Sky, Mediaset, La7 dal 9 febbraio, giorno in cui Tik Tok ha iniziato a bloccare gli utenti italiani e a richiedere nuovamente l'età ai propri utenti allo scopo di evitare che si iscrivano alla piattaforma i minori di 13 anni. A completamento della campagna informativa è stato realizzato un *booklet* dal titolo "Minori e nuove tecnologie. Consigli ai grandi per un utilizzo sicuro da parte dei piccoli (https://www.gpdp.it/temi/minori).

Ad aprile il Garante ha lanciato un nuovo progetto informativo dal titolo "Le parole dell'AI" per illustrare le principali problematiche legate all'IA e il loro rapporto con la protezione dei dati. La campagna si è sviluppata sulla pagina www.garanteprivacy.it/temi/intelligenza-artificiale e sui canali *social* del Garante. Sono 4 video di approfondimento a tema nelle parole dei componenti: Etica e Intelligenza artificiale – presidente Pasquale Stanzione; *Deepfake e Deepnude* – vice presidente Ginevra Cerrina Feroni; Gli assistenti digitali nelle parole - Agostino Ghiglia; Riconoscimento facciale e sorveglianza di massa - Guido Scorza.

Nella giornata del 25 maggio 2021, a 3 anni dalla applicazione del RGPD, i componenti del Collegio del Garante mediante video divulgativi hanno spiegato e approfondito alcuni principi fondamentali e le più importanti innovazioni introdotte dal Regolamento (https://www.gpdp.it/tre-anni-di-GDPR).

I più significativi interventi adottati nel 2021 sono stati raccolti in un video intitolato "Dalla tua parte" (doc. web n. 9725322), realizzato per illustrare il ruolo e l'impegno dell'Autorità al fianco delle persone e del Paese. Al video, diffuso sui profili *social* dell'Autorità, si affianca una pagina sul sito istituzionale www.gpdp.it/dalla-tua-parte, con materiale di documentazione, utile per chiunque voglia approfondire l'attività del Garante in difesa dei diritti delle persone e le tutele garantite dalla normativa sulla *privacy*.

Infine, relativamente al contrasto del grave fenomeno del cyberbullismo l'Autorità ha realizzato il video dal titolo "Cyberbullismo: il video del Garante per spiegare ai ragazzi come difendersi" (https://www.youtube.com/watch?v=wgfq5VfKqoI&ab_channel=Garanteperlaprotezionedeidatipersonali).

25.5. *Manifestazioni e convegni*

Particolarmente intensa è stata nel 2021 l'attività di sensibilizzazione svolta dal Garante, grazie alla partecipazione a numerosi convegni ed incontri, a partire dalla XV edizione della Giornata europea della protezione dei dati, il 28 gennaio, in occasione della quale il Garante ha organizzato il Convegno "*Privacy* e neurodiritti: la persona al tempo delle neuroscienze", riguardante uno degli ambiti disciplinari più moderni e affascinanti, dove si incrociano etica, discipline giuridiche, nuove tecnologie e le frontiere più avanzate della scienza. Il Convegno si è svolto in modalità *streaming,* in ottemperanza alle misure di prevenzione del Covid-19.

I lavori sono stati aperti dal presidente dell'Autorità, Pasquale Stanzione, e conclusi da Pietro Perlingieri, professore emerito di diritto civile dell'Università del Sannio. Ha moderato l'incontro Barbara Carfagna, giornalista e autrice Rai.

Ad approfondire la questione dell'incidenza delle neuroscienze e dell'IA sul processo volitivo e, più in generale, cognitivo, delle persone, anche sotto il profilo delle responsabilità giuridiche, sono stati invitati a partecipare: Paolo Benanti, professore straordinario facoltà di teologia della Pontificia Università Gregoriana; Marcello Ienca, ricercatore *senior* presso il Politecnico federale di Zurigo; Giacomo Marramao, professore emerito di filosofia teoretica dell'Università Roma Tre; Oreste Pollicino, professore ordinario di diritto costituzionale e dei *media* dell'Università Bocconi.

Il convegno è stato anche l'occasione per proiettare il nuovo video istituzionale realizzato dall'Autorità intitolato "I tuoi dati sono un tesoro".

Significativa, nel corso dell'anno, la partecipazione del Presidente e dei Componenti del Collegio ad eventi, convegni e giornate di studio di rilievo nazionale ed internazionale.

Il *Safer Internet Day*, la giornata mondiale di sensibilizzazione per un uso più sicuro e consapevole della rete istituita nel 2004 dalla Commissione europea ha visto la partecipazione – dall'8 al 9 febbraio – ad una serie di incontri organizzati da telefono Azzurro: il presidente Stanzione è intervenuto nel *panel* "Le istituzioni a confronto: i bambini e gli adolescenti al centro della sfida digitale"; la vice presidente Cerrina Feroni in quello su "I *social network* per i bambini e gli adolescenti: potenzialità e rischi" e l'avv. Scorza nel *panel* "Essere cittadini nel XXI secolo tra sicurezza e *privacy*".

Il tema della protezione dei dati personali e del rispetto della volontà del consumatore è stato affrontato alla tavola rotonda "*Telemarketing* legale –Consumatore sicuro", organizzata da Assocontact, alla quale hanno partecipato Pasquale Stanzione e Agostino Ghiglia – tenutasi il 23 febbraio 2021 in diretta su Facebook e YouTube.

Il 26 febbraio Federprivacy ha promosso un seminario *online* dal titolo "Il *data Protection Officer* tra regole e prassi a cui ha partecipato Guido Scorza, relativo, tra l'altro, ai compiti assegnati al Garante dal Regolamento ed alle numerose sfide che i *Data Protection Officer* devono affrontare, sia nelle realtà aziendali che all'interno delle p.a.

Il 5 marzo Agostino Ghiglia ha partecipato al *webinar* organizzato da SPRINT Soluzioni Editoriali e Fairplay – "*Antitrust* Consumatori e *Privacy*", con il patrocinio del Garante *privacy* e dell'Ordine degli Avvocati di Torino dal titolo "Il *telemarketing* tra la raccolta del consenso e la tutela del consumatore".

25

Il 17 marzo il Presidente è intervenuto alla quarta edizione "*Wired Health* 2021 - La salute in dati, per tutti". L'evento è stato dedicato al tema dell'innovazione presente e futura della medicina e della salute. La discussione ha riguardato diversi temi: dalla robotica all'interoperabilità dei *big data* sanitari, tra occhi bionici, telemedicina, etica e patologie digitali. Sulle più generali attività messe in campo durante la pandemia, è intervenuto Pasquale Stanzione secondo il quale "A partire dalle attività di *contact tracing,* il tenere i dati protetti si è dimostrato presupposto irrinunciabile per creare fiducia nelle soluzioni digitali". Le questioni principali che si pongono oggi, secondo Stanzione, sono riconducibili a due grosse categorie: "una è la tutela dei dati sanitari nell'ambito delle attività di prevenzione, e poi c'è la questione *privacy* di fronte alla digitalizzazione della vita imposta dalle misure di contenimento".

Il 26 marzo si è svolto l'evento organizzato da IAPP (*International Association of Privacy Professionals*) "*Welcome to the Machine – Tra hype,* distopia e protezione dei dati". Alla tavola rotonda è intervenuto Guido Scorza – insieme a rappresentanti del mondo istituzionale, accademico, giornalistico e professionale – affrontando il sempre più complesso rapporto tra IA e tutela della protezione dei dati.

All'approfondimento del tema sull'IA è stato altresì dedicato il convegno "AI *Anthology.* Profili giuridici, economici e sociali dell'intelligenza artificiale", organizzato dalla Fondazione Cesifin in *partnership* con il Garante (19 e 20 aprile) con la partecipazione dell'intero Collegio e di alcuni funzionari dell'Autorità, insieme ad autorevoli esperti in materia di IA ed esponenti del mondo giuridico ed imprenditoriale. Numerose le tematiche: dall'impatto dell'IA sul diritto civile alla decisione politica e giudiziaria algoritmica, dalla *privacy governance* alla tutela della concorrenza, dal Fintech all'utilizzo della robotica in sanità.

I componenti del Collegio hanno illustrato con alcuni video le opportunità e i rischi connessi alla diffusione delle tecnologie di IA dando suggerimenti per conciliare sviluppo dell'IA e tutela dei dati personali.

Il convegno è stato interamente trasmesso in modalità *streaming* sul canale YouTube del Garante https://www.youtube.com/garantedatipersonaliGP.

Il 25 maggio l'Osservatorio *Digital Innovation* del Politecnico di Milano (*cybersecurity & data protection*) in collaborazione con Clusit - Associazione Italiana per la sicurezza informatica ha organizzato il *webinar:* "Il *data protection officer* all'interno delle complessità organizzative pubbliche e private" con i presidenti delle più rilevanti associazioni e strutture di studio di settore. All'evento ha partecipato Agostino Ghiglia, il quale ha sottolineato ancora una volta l'importanza del Rpd "quale figura chiave all'interno degli enti pubblici e privati".

Di IA si è parlato anche all'*executive webinar* "Intelligenza artificiale e riconoscimento facciale in *real time,* i vantaggi e i rischi del Regolamento europeo", organizzato da *Privacy* Italia, Asso Dpo e Key4biz il 4 giugno. Durante il *live streaming* Agostino Ghiglia discutendo la proposta di regolamento europeo concernente l'introduzione di nuove regole per l'utilizzo o il divieto di sistemi di IA ha ribadito la ferma opposizione alla sorveglianza di massa (sulla IA cfr. cap. 17).

Il 15 giugno, il *webinar* promosso da Confartigianato "*Privacy* a misura di micro e piccola impresa, Le linee guida di Confartigianato", ha costituito l'occasione per presentare le proposte formative per le imprese, su cui è già attivo un corso per i formatori organizzato dalla Scuola di sistema di Confartigianato. La prof.ssa Cerrina Feroni in un intervento su "L'attività del Garante per la protezione dei dati personali in favore delle PMI italiane e le linee guida di Confartigianato ha in particolare affermato che il Garante "[....] non deve essere considerato un ostacolo al mercato, ma piuttosto promotore di competitività, coerente con il tessuto produttivo del Paese nella ricerca del delicato equilibrio tra la protezione dei dati personali e dei diritti

delle persone e le esigenze dell'economia e delle imprese, tra la libera circolazione delle informazioni e la tutela della riservatezza degli individui. Siamo aperti e pronti al dialogo per difendere la nostra italianità. Confartigianato ha svolto un'azione molto utile anche per l'Autorità al fine di consentire alle imprese associate di adeguarsi al nuovo standard di trattamento dei dati personali, disegnato dal Regolamento europeo, lavorando allo stesso tempo per rendere la normativa italiana sempre più a dimensione di micro e piccole imprese".

La Luiss *Business School* il 6 luglio ha organizzato il *webinar* su: Il ruolo del *Data Protection Officer:* dagli aspetti formali alla sostanza" dove sono state illustrate le funzioni del *Data Protection Officer,* le novità introdotte dal Garante nelle recenti FAQ sul Rpd in ambito privato, le incertezze da superare per una compiuta realizzazione di questa figura. L'incontro ha messo a confronto le prospettive di attori privati e istituzionali, con un approfondimento dedicato ai rischi inerenti il trattamento dei dati in un contesto multinazionale. In un passaggio del suo intervento la vice presidente Cerrina Feroni ha messo in risalto il ruolo del Rpd indicandolo quale "figura chiave del sistema RGPD fondato sull'*accountability,* l'avamposto dell'Autorità nel variegato tessuto economico ed istituzionale nazionale, erede di una lunga tradizione di valutazione diretta dell'impatto dei trattamenti sulla protezione dei dati degli interessati operata dal Garante fino a tre anni fa e che ora spetta ai titolari". "Da maggio 2018 – ha concluso la vice presidente – non può più esistere un Garante efficiente, aggiornato, avveduto, senza questa rete di piccoli garanti che operano quotidianamente nel vivo della specificità di migliaia di trattamenti cruciali per settori strategici dell'economia del Paese. Il primo bilanciamento lo operano i Rpd. Il Regolamento cammina sulle loro gambe, il Garante vede con i loro occhi."

Il 7 settembre si è tenuta la tavola rotonda delle autorità di protezione dati dei Paesi del G7. L'incontro *Data Free Flow with Trust* è nato dall'esigenza di costruire un clima di fiducia all'interno di un sistema economico sempre più dipendente dai flussi di dati attraverso il bilanciamento nell'economia digitale, tra la tutela dei diritti individuali e la salvaguardia delle libertà del mercato. L'evento si è svolto in modalità virtuale. Hanno partecipato i Garanti *privacy* di Canada, Francia, Germania, Giappone, Italia, Regno Unito e la *Federal Trade commission* statunitense. Per l'Italia è intervenuta la vice presidente Ginevra Cerrina Feroni. "*Pandemic-Driven Tech Innovation: A Stress Test for Data Protection Rights*" il titolo dell'intervento della vice presidente Cerrina Feroni la quale ha introdotto e sviluppato due importanti questioni, recepite nel comunicato stampa finale, ovvero "la riaffermazione della centralità del ruolo delle Autorità *privacy* nella definizione di principi e criteri fondamentali per la transizione digitale ponendosi a presidio dei diritti fondamentali collegati alla protezione dati. Ruolo divenuto ancora più cruciale nell'attuale emergenza pandemica" e "la necessità di valorizzare e promuovere le competenze delle autorità *privacy* nel campo complesso e tutto in divenire dell'IA e dei futuri sviluppi e applicazioni delle tecnologie ad essa collegate".

Il principio di *accountability* è stato oggetto di attenta analisi nel convegno "Tutela della persona, gestione del rischio. Responsabilizzazione e responsabilità alla luce del GDPR" (4 ottobre). All'evento – promosso da Centro Studi Diritto Nuove Tecnologie – DNT® e dalla Fondazione Cesifin – sono intervenuti il presidente Pasquale Stanzione e la vice presidente Ginevra Cerrina Feroni. Durante il convegno si è discusso di come il RGPD abbia segnato il passaggio da un modello normativo esclusivamente sanzionatorio *a posteriori* ad un modello più maturo e consapevole di gestione del rischio *a priori.*

Sul tema Pnrr, il 20 ottobre il convegno dal titolo "Pnrr e *privacy:* tra tutela della persona e valore economico dei dati personali", organizzato dall'Università Roma Tre

25

e Hogan Lovells in occasione della giornata conclusiva del master di II livello 2021 *Data Protection Officer* e *privacy expert* è stato occasione di confronto tra istituzioni, autorità e imprese sul tema del valore economico dei dati personali nell'ambito del Pnrr nel rispetto della tutela della persona e dei diritti fondamentali dell'individuo. Per l'Autorità Guido Scorza, definendo il Pnrr, la più grande opera di riprogettazione del Paese dalle fondamenta, ha sottolineato come "questa opportunità porti con sé, anche nella dimensione della *privacy,* una delle più grandi sfide sin qui mai affrontate perché è indispensabile che il Paese, nuovo, migliore, più efficiente, più moderno, più attento al futuro che si costruirà attuando il Piano sia, innanzitutto, un Paese a prova di diritti fondamentali".

Per il 16° anno consecutivo il *Consumers' Forum*, in collaborazione con Il Sole 24 Ore, ha organizzato il 30 novembre il consueto confronto con i Presidenti delle *authority* italiane per analizzare la situazione riguardante il mercato, le imprese e i consumatori. Nell'edizione 2021sulla base di una ricerca svolta dall'Università Roma Tre, è stata approfondita la questione del Pnrr e delle ricadute che avrà in tema di tutela del consumatore.

Il presidente Stanzione ha sottolineato che "il richiamo frequente nel Pnrr all'innovazione, alla digitalizzazione, alla crescita non può essere disgiunto da una visione di lungo periodo più complessiva che coniughi sviluppo e diritti. In tale prospettiva la protezione dei dati assume un ruolo centrale, quasi di baricentro, tracciando la direzione di un'innovazione sostenibile anche in termini di diritti e di libertà". Il presidente Stanzione ha anche sottolineato come "nella complessiva azione di *governance* del processo di digitalizzazione la disciplina di protezione dei dati possa svolgere una funzione importante, al fine di garantire i presupposti di sicurezza dei flussi informativi necessari per impedire la permeabilità delle banche dati e garantire i requisiti di esattezza dei dati trattati".

Il 16 novembre è stato assegnato al presidente Stanzione il premio Dekra *Safety Award* 2021, riconoscimento attribuito per l'impegno dell'Autorità da lui presieduta nella tutela del diritto alla riservatezza dei cittadini. La premiazione è avvenuta in occasione della presentazione del rapporto internazionale DEKRA 2021 sulla sicurezza stradale. Durante la presentazione il Presidente ha sottolineato la necessità di tutelare la persona dall'invasività delle nuove tecnologie.

Il 22 novembre Guido Scorza ha ricevuto il Premio "Vincenzo Dona, voce dei consumatori"; riconoscenza ottenuta grazie alla sua intensa attività di studio e divulgazione che ha contribuito a rendere centrale il ruolo dell'Autorità e i temi della tutela della *privacy,* sia per gli addetti ai lavori che per i consumatori.

25.6. *L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi*

Nel corso del 2021 il Garante ha svolto la propria attività di assistenza al pubblico, per il tramite del Servizio relazioni con il pubblico, continuando a promuovere la conoscenza e la crescita della consapevolezza in merito alle tematiche connesse alla disciplina sulla protezione dei dati personali. Contestualmente ha svolto una funzione di filtro, ponendosi come struttura di raccordo tra il cittadino e l'Autorità al fine di agevolarne i rapporti anche attraverso, laddove possibile, il diretto riscontro delle richieste di chiarimenti. In tale ottica si è data visibilità all'attività dell'Autorità, garantendo al cittadino sia la possibilità di partecipare e di accedere alle diverse fasi procedimentali, espressamente regolamentate, sia il costante aggiornamento sulle tematiche di interesse dell'Autorità.

Nella gestione di tutte le richieste, il Servizio ha avuto cura di conciliare l'effi-

25

cienza, la professionalità e una aggiornata conoscenza giuridica delle questioni esaminate, con la cortesia e la tempestività delle risposte, provvedendo poi a informare le altre unità organizzative dell'Autorità in merito alle questioni più delicate e di maggiore interesse per gli utenti.

In particolare il Servizio ha raccolto le segnalazioni sia per il tramite della posta che del telefono, fornendo subito supporto al segnalante, spiegando la normativa di riferimento, guidando e correggendo le modalità di compilazione della modulistica e, se necessario, anche coordinandosi con il dipartimento competente, nei casi di problemi prettamente tecnici, considerati anche gli stringenti tempi previsti dalla normativa stessa.

Nel periodo in esame è stato notevole l'incremento delle richieste riferibili all'interpretazione e al coordinamento tra la normativa emergenziale e la protezione dei dati personali, in particolare in ambito sanitario, lavorativo e scolastico. L'emergenza sanitaria ha influito infatti, oltre che sull'oggetto delle istanze pervenute e sull'entità numerica, anche sulle modalità di assistenza al pubblico, che nel rispetto della normativa emergenziale, è stata fornita esclusivamente tramite i canali telefonico e telematico, essendo preclusa l'attività di ricevimento degli utenti presso la sede del Garante.

Ai fini del potenziamento degli strumenti informativi a disposizione del pubblico, alla luce delle questioni maggiormente segnalate, sono state predisposte le schede aggiornate per il risponditore automatico su videosorveglianza, cyberbullismo, esercizio dei diritti e telefonate indesiderate; sono inoltre state predisposte FAQ generali sui ruoli *privacy* sulla base delle *Guidelines* 07/2020 *on the concepts of controller and processor in the* GDPR dell'EDPB.

L'interesse degli utenti rispetto a tali temi è dimostrato dai dati numerici relativi ai contatti (quesiti, segnalazioni e reclami) con il Servizio, che ammontano in totale a 18.705 di cui 15.004 *e-mail,* 201 fascicoli e circa 3.500 via telefono (cfr. parte IV, tab. 15).

Tra le attività ordinarie e di supporto agli utenti (cittadini, aziende, scuole, enti, ecc.), vanno anche segnalate le molte istanze concernenti l'istituto del *data breach.*

Tematiche d'interesse

Tra le tematiche di carattere generale nel 2021, si segnalano in primo luogo quelle concernenti le forme di tutela (circa 1.700 *e-mail*) e gli adempimenti previsti dal RGPD (in particolare circa 1.800 *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 hanno riguardato i trattamenti di dati personali in ambito lavorativo pubblico e privato (quasi 700 *e-mail*); la videosorveglianza in ambito privato, lavorativo e scolastico (oltre 480 *e-mail*); i trattamenti di dati personali nell'ambito della rete internet, dei *social network* e delle *app,* nonché in ambito giornalistico, con particolare riferimento alle richieste di deindicizzazione dei dati personali dai motori di ricerca, volte all'esercizio del cd. diritto all'oblio di cui all'art. 17 del RGPD (circa 800 *e-mail*); il trattamento dei dati sanitari degli interessati nell'ambito delle misure adottate per il contrasto del Covid-19, nonché con riguardo alle vaccinazioni e al Fse (oltre 560 *e-mail*).

Il maggior numero delle richieste pervenute è stato afferente alla tutela dei dati personali nei diversi contesti economico-sociali interessati dalle misure previste dai decreti adottati al fine di contrastare l'emergenza da Covid-19.

Si segnalano, in particolare, le istanze concernenti l'introduzione, il funzionamento e la verifica del cd. *green pass* anche a seguito dell'evoluzione normativa, gli adempimenti riguardanti la verifica dell'obbligo vaccinale per le categorie interessate, le modalità di trattamento del certificato di esenzione vaccinale, la tenuta dei registri per il *contact tracing* (per un totale di circa 900 *e-mail*).

25

Inoltre a seguito della segnalazione di un cittadino direttamente all'attenzione del Srp, relativa alla disponibilità *online* all'interno di una nota piattaforma di *file sharing* di migliaia di *green pass* apparentemente autentici scaricabili da chiunque, il Garante ha avviato d'urgenza un'indagine, dando mandato al Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza di acquisire gli archivi *online* e accertarne la provenienza.

Anche il settore scolastico è stato oggetto di grande interesse, con particolare riguardo ai trattamenti dei dati personali di alunni, studenti, docenti e famiglie, inerenti la situazione vaccinale, la gestione dei casi di positività, le modalità di quarantena, la misurazione della temperatura dei minori e la sottoposizione degli stessi ai tamponi (circa 800 *e-mail*).

26 Studi e documentazione

Studio, documentazione e supporto giuridico

L'attività di studio e ricerca ha riguardato molteplici questioni tecnico-giuridiche sulle materie di interesse dell'Autorità, anche oggetto di rinvio pregiudiziale alla Corte di giustizia dell'Unione europea.

Particolari approfondimenti sono stati svolti in materia di finanziamento/composizione delle autorità di protezione dati e del regime di pubblicità degli atti di sindacato ispettivo presso il Parlamento, le assemblee regionali e i consigli provinciali e comunali nonché sulla sanzionabilità delle persone giuridiche e sul potere di disapplicazione da parte dell'Autorità delle norme nazionali contrastanti con quelle europee.

In ragione dei profili di interesse e delle criticità sussistenti in materia di protezione dei dati personali, è stata seguita con particolare attenzione l'evoluzione giurisprudenziale e dottrinale concernente l'istituto dell'accesso documentale anche in relazione a quello dell'accesso civico generalizzato, la cui procedura prevede la richiesta di parere al Garante da parte dei Responsabili della prevenzione della corruzione e della trasparenza (cfr. par. 4.4.3).

In continuità con il lavoro svolto da diversi anni, è stato altresì curato un Osservatorio ad uso interno con cadenza mensile quale documentazione di sintesi dell'attività di costante monitoraggio della normativa, giurisprudenza e dottrina nazionale ed eurounitaria in materia di protezione dati, unitamente ad approfondimenti su questioni o settori specifici.

Relazione annuale

In conformità alla previsione normativa nazionale ed europea (cfr. art. 154, comma 1, lett. *e*), del Codice nonché l'art. 59 del RGPD) è stata curata la redazione del testo della Relazione annuale al fine di 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 informazioni di natura statistica), agevola la rapida e sintetica consultazione di informazioni puntuali sull'attività svolta (con particolare riguardo all'attività provvedimentale, sanzionatoria e comunicativa, nonché a quella svolta in ambito europeo ed internazionale) ed aggiornamenti su specifici profili o istituti attinenti alla protezione dati. In base 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) viene trasmessa anche alla Corte dei conti, oltre ad essere a disposizione sul sito istituzionale.

PAGINA BIANCA

L'Ufficio del Garante

Relazione annuale 2021

PAGINA BIANCA

III - L'Ufficio del Garante

27 La gestione amministrativa e dei sistemi informatici

27.1. *Il bilancio e la gestione economico-finanziaria con gli obblighi derivanti dal perseguimento delle finalità istituzionali*

La gestione delle attività di natura amministrativo-contabile del Garante è stata improntata ad una prudente valutazione delle entrate ed all'osservanza dei generali principi di attenta programmazione della spesa nel rispetto delle specifiche disposizioni legislative e regolamentari in materia di contabilità pubblica che si informano ai requisiti della veridicità, pubblicità e trasparenza, nonché del pareggio di bilancio.

Nell'anno 2021 il finanziamento statale complessivo erogato al Garante è stato pari a 35,6 milioni di euro, la cui entità è stata individuata dalla legge 30 dicembre 2020, n. 178 e comprende la somma di 4 milioni di euro riferibile a rifinanziamenti e riprogrammazioni delle dotazioni finanziarie. In conseguenza dell'applicazione delle sanzioni irrogate dal Garante, nel 2021 sono affluiti direttamente al bilancio dello Stato pagamenti per complessivi 13,4 milioni di euro (12 milioni da versamenti spontanei dei contravventori e 1,4 dalla riscossione coattiva). Occorre, al riguardo, evidenziare che i proventi delle sanzioni irrogate dal Garante affluiscono direttamente al bilancio dello Stato e, nella misura del 50% del totale annuo, è previsto che debbano essere riassegnati al Garante per essere destinati alle specifiche attività di sensibilizzazione e di ispezione nonché di attuazione del RGPD, svolte dal Garante (art. 166, comma 7, del Codice).

Nel periodo considerato sono stati approvati dall'Autorità il bilancio consuntivo relativo all'anno 2020 e il bilancio preventivo relativo all'esercizio finanziario 2022. Sono stati altresì elaborati gli atti preordinati ad una variazione al bilancio di previsione 2021 approvata con la delibera 29 aprile 2021, n. 162.

Nel corso delle verifiche effettuate nell'esercizio dall'organo preposto alla verifica della regolarità amministrativo-contabile non sono emerse irregolarità, né sono stati formulati rilievi a carico dell'attività amministrativa svolta.

Sotto il profilo più strettamente contabile, il risultato finanziario dell'esercizio ha fatto registrare un avanzo di amministrazione pari ad oltre 9 milioni di euro. Tale risultato è stato determinato da una dinamica della spesa più contenuta rispetto a quanto ipotizzato in sede di previsione, sia in ragione di una politica gestionale volta a valorizzare la salvaguardia delle risorse erariali, sia per effetto delle inevitabili conseguenze che la pandemia ha determinato a carico della gestione amministrativa e delle procedure volte al rafforzamento della struttura.

Nel 2021, al netto delle partite di giro, le entrate complessivamente acquisite dall'Autorità sono state di 35,9 milioni di euro a fronte delle quali sono stati regi-

27

strati impegni di spesa per 26,2 milioni di euro.

Le risorse finanziarie acquisite al bilancio del Garante sono rappresentate, in misura largamente prevalente, da trasferimenti posti a carico del bilancio dello Stato, il cui importo è quantificato annualmente nell'ambito della legge di bilancio.

In via residuale e per importi poco significativi la gestione ha fatto registrare l'acquisizione al bilancio di ulteriori somme a titolo di meri rimborsi spese erogati da parte di amministrazioni e organismi dell'Unione europea.

Rispetto al precedente esercizio finanziario, l'incremento delle entrate registrato nel 2021 è stato di 5,5 milioni di euro, con una variazione di poco superiore al 18%.

Con riferimento alla spesa, invece, gli oneri complessivi registrati nell'anno, pari a 26,2 milioni di euro, risultano in aumento di 2,4 milioni di euro rispetto alla spesa complessiva del precedente anno 2020, corrispondente ad una variazione di circa il 10%. La spesa complessiva è da imputare in massima parte alla gestione corrente, nella misura di 25,6 milioni di euro, mentre la parte residuale di 0,6 milioni di euro rappresenta la quota delle risorse finanziarie destinate ad acquisti durevoli costituiti prevalentemente da prodotti *software* ed attrezzature informatiche utilizzate a supporto delle attività istituzionali.

Anche per il 2021 la struttura della spesa fa emergere, come per il passato ed in analogia alla generalità delle 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 ed alla relativa erogazione si è provveduto nel rispetto dei vincoli e delle prescrizioni vigenti.

Con riferimento, infine, agli oneri strettamente connessi alle esigenze gestionali, nel corso dell'anno l'Autorità ha rispettato i prescritti limiti di legge.

Si rinvia alla sez. IV, tab. 18 per una puntuale illustrazione dei valori sintetici delle entrate correnti e delle spese, suddivise tra quelle 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.

27.2. *L'attività contrattuale, la logistica e la manutenzione dell'immobile*

In materia di appalti pubblici anche l'anno 2021, come il precedente, è stato contraddistinto dalla vigenza e dall'implementazione di normative di carattere emergenziale, connesse con la perdurante situazione pandemica e finalizzate a rendere l'azione amministrativa più agile; sulla base dell'esperienza acquisita nel corso dell'anno precedente, e nel pieno rispetto delle predette normative, l'Autorità ha comunque fatto ricorso, ove possibile, a procedure di affidamento basate su comparazioni, adoperando prevalentemente le tipologie negoziali di *e-procurement* messe a disposizione da Consip spa.

Gare

Dal punto di vista del valore economico, tra gli affidamenti concretizzati nell'anno in esame risalta l'aggiudicazione ad un nuovo operatore economico della gara per la gestione del piano sanitario per il personale dell'Autorità, successiva ad altra procedura di gara bandita nel corso dell'anno precedente e risultata deserta, nonché l'aggiudicazione della gara per il servizio di assistenza in materia di amministrazione digitale e protocollo informatico; entrambe le predette procedure di gara hanno superato la soglia comunitaria.

Al di sotto di tale soglia si è collocata la procedura di gara relativa al servizio di brokeraggio assicurativo – bandita nel corso dell'anno precedente in tre distinti lotti, nella quale l'Autorità ha rivestito il ruolo di stazione appaltante nell'ambito della Convenzione sottoscritta con altre autorità amministrative indipendenti – i cui atti conclusivi, compresa la sottoscrizione del contratto, si sono concretizzati nell'anno in esame. Tra le altre procedure selettive caratterizzate da importi inferiori alla soglia comunitaria, si segnala quella relativa al servizio di cassa e quella relativa ai servizi di progettazione grafica di prodotti editoriali dell'Autorità – quest'ultima con amplissima partecipazione di concorrenti – entrambe bandite con procedure aperte sul Mepa gestito da Consip spa.

Notevole sforzo è stato profuso per l'acquisizione di ulteriori servizi di digitalizzazione dei processi (conservazione digitale, firma automatica massiva, sigillo elettronico), anche in conseguenza della necessità di adeguamento alle sopravvenienze normative intervenute; di *backup* remoto (sistemi iperconvergenti, *server*); nonché per gli appalti connessi con la remotizzazione delle attività lavorative. Parimenti cospicuo è stato l'impegno volto alla sottoscrizione di contratti derivanti dall'accresciuto impegno dell'Autorità nel campo della comunicazione e divulgazione delle proprie attività istituzionali: come premesso, anche nel caso di importi contenuti, gli affidamenti sono stati concretizzati nella quasi totalità dei casi al termine di attività di verifica della congruità dei prezzi proposti, ponendo a confronto offerte ricevute da più operatori economici oppure, laddove disponibili, paragonando le offerte pubblicate sui listini del Mepa.

È stato poi costantemente utilizzato lo strumento delle Convenzioni della Consip spa, relativamente a diverse tipologie di servizi e forniture (buoni pasto, gestione integrata della salute e sicurezza nei luoghi di lavoro, energia elettrica, forniture informatiche ecc.).

Nell'anno in esame sono stati effettuati quattro affidamenti di rappresentanza in giudizio, in presenza di controversie nelle quali, per ragioni di incompatibilità, la difesa non poteva essere assunta dall'Avvocatura dello Stato.

La manutenzione dell'immobile

La sede degli uffici del Garante è condotta in locazione e l'Autorità non detiene immobili adibiti ad abitazione o foresteria.

Per quanto attiene alla logistica e manutenzione dell'immobile, sono state effettuate attività di adeguamento funzionale, miglioramento dei locali e inventario degli arredi, di concerto con la società proprietaria e con il Responsabile del servizio prevenzione e protezione dell'Autorità, che ha coadiuvato l'Ufficio al fine di assicurare il rispetto della normativa sulla sicurezza nei luoghi di lavoro.

In particolare, si è costantemente vigilato in ordine alla corretta esecuzione delle iniziative di manutenzione e gestione dell'immobile proseguendo con le attività di adeguamento alle norme antincendio avviate in precedenza dalla società proprietaria dell'immobile.

È stata inoltre curata la realizzazione di un magazzino idoneo alla custodia dei beni librari.

27.3. *L'organizzazione dell'Ufficio*

Ha avuto avvio nel periodo di riferimento un processo di riordino complessivo dell'Ufficio per il miglior raggiungimento dei risultati programmati, secondo una linea strategica che mira, da un lato, a rafforzare l'organico, modernizzare e snellire l'attività lavorativa, dall'altro a valorizzare forme di collaborazione esterne in settori dell'ordinamento che si intersecano con la materia della protezione dei dati personali

27

(es. lotta al cyberbullismo, sviluppo dell'intelligenza artificiale). In questo quadro si colloca l'adeguamento delle tabelle retributive vigenti presso l'Autorità a quelle del personale dell'Agcm, in ottemperanza all'art. 27 del regolamento 2/2000, in base anche alle novità introdotte dal d.l. 8 ottobre 2021, n. 139 recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali, convertito con modificazioni dalla l. 3 dicembre 2021, n. 205 (G.U. 7 dicembre 2021, n. 291).

Il rafforzamento dell'Autorità

Con riguardo al reclutamento del personale, l'Autorità ha dato seguito alle attività destinate alla progressiva copertura della pianta organica, procedendo alla definizione ed alla successiva pubblicazione dei seguenti bandi di mobilità volontaria esterna: n. 1 posto di dirigente giuridico-amministrativo; n. 2 posti di funzionario con profilo area comunicazione; n. 1 posto di funzionario area comunicazione - *digital communication specialist;* n. 4 posti di funzionario con profilo informatico-tecnologico; n. 2 posti di impiegato operativo profilo informatico-tecnologico.

L'Autorità ha altresì curato la predisposizione e la pubblicazione di due bandi di concorso, rispettivamente per n. 2 posti di funzionario area comunicazione e n. 1 funzionario area comunicazione - *digital communication specialist,* nonché ha continuato a curare le attività legate alla procedura di concorso relativa a n. 1 posto di dirigente giuridico-internazionale.

Sono poi stati assunti n. 4 funzionari con profilo giuridico-amministrativo attraverso lo scorrimento della graduatoria del concorso bandito nel 2018.

L'Autorità inoltre, nel pieno rispetto della legge n. 68/1999 in tema di diritto al lavoro dei disabili, a seguito di un confronto con la direzione della Regione Lazio competente per materia, ha provveduto alla stipula di una specifica convenzione ai sensi dell'art. 11 della legge citata per il raggiungimento della quota di personale disabile prevista dalla citata normativa per tali categorie.

Lavoro agile

In conformità alla decretazione d'urgenza che si è susseguita a partire dal d.l. 17 marzo 2020, n. 18, fino alle recenti disposizioni in tema di certificazione per l'accesso ai luoghi di lavoro (cd. *green pass*), l'Autorità ha continuato a far fronte alla grave situazione emergenziale adeguando le procedure interne alle disposizioni normative succedutesi nel tempo. Si evidenziano, in particolare, tra le iniziative dell'Autorità in materia di gestione del personale, le decisioni assunte in merito alla prosecuzione dell'attività lavorativa mediante l'istituto del lavoro agile, che hanno garantito la continuità dell'azione amministrativa ed elevati standard di produttività.

Relazioni sindacali

Con riferimento alla gestione delle relazioni sindacali, anche nel corso del 2021, è stata registrata una intensa attività in relazione ai vari temi di interesse, con diversi tavoli tecnici, tra i quali quello per la definizione di un "accordo ponte" tra le parti interessate, nelle more della definizione di una specifica regolamentazione a regime ordinario dell'istituto del lavoro agile da adottare presso l'Autorità, anche in considerazione dei risultati positivi ottenuti mediante la provvisoria applicazione di detto istituto per le esigenze emergenziali già richiamate.

Sicurezza sul lavoro

In relazione alla sicurezza ed alla salute dei lavoratori, in conformità al d.lgs. n. 81/2008 in materia di tutela della salute e della sicurezza nei luoghi di lavoro, l'Autorità ha continuato ad offrire la propria consueta collaborazione nei confronti delle figure normativamente previste in tema di sicurezza dalla normativa richiamata Rspp e medico competente per l'assolvimento degli adempimenti normativamente previsti in capo al datore di lavoro, richiedendo, ove necessario, specifiche indicazioni per la corretta gestione della situazione emergenziale dovuta alla diffusione della pandemia da virus Sars-Cov-2.

Formazione

Riguardo alla formazione del personale, l'Autorità ha proseguito il proprio rapporto collaborativo con la Scuola nazionale dell'amministrazione, garantendo la costante comunicazione e pubblicizzazione, nei confronti del personale dirigente e direttivo dell'Autorità, del catalogo formativo della Scuola, ai fini della individuazione di eventuali tematiche di interesse anche in relazione all'attività svolta nei dipartimenti e servizi.

Segreteria generale

Al fine di garantire il corretto espletamento dei compiti attribuiti al Garante dalla disciplina vigente, la Segreteria generale, anche per il 2021, ha basato la propria attività su un'articolata e puntuale programmazione e sul rispetto dei principi di economicità ed efficienza dell'azione amministrativa, anche in conformità al regolamento n. 1/2000 del Garante.

L'attività di coordinamento è stata garantita dal Segretario generale, soggetto preposto all'Ufficio ai sensi dell'art. 156, comma 1, del Codice, in particolare, attraverso il costante raccordo tra le unità organizzative e il Collegio, la supervisione dell'attività istruttoria tramite l'analisi dei numerosi schemi di provvedimento oggetto di esame (per un totale di circa 37 adunanze), nonché attraverso il dialogo con le unità organizzative sulle questioni interpretative di maggiore complessità, fornendo in taluni casi indicazioni operative al fine di una più uniforme e omogenea applicazione della disciplina. In seno alla Segreteria generale si svolge anche l'attività di verbalizzazione delle adunanze del Collegio e viene curato l'invio alla Gazzetta Ufficiale dei testi da pubblicare.

La partecipazione (principalmente da remoto per le restrizioni legate alla pandemia) a diversi incontri con attori istituzionali e organismi rappresentativi di varie categorie, a livello nazionale, europeo e internazionale, ha consentito di condividere, a livello istituzionale, gli orientamenti dell'Autorità sulle questioni di maggiore criticità in materia di protezione dati, e a livello interno le novità tematiche ed interpretative di interesse frutto dell'esperienza di altri Paesi.

In tale quadro, si segnala, in particolare, la partecipazione del Segretario generale (o di funzionari facenti parte dell'Ufficio di segreteria) alle sessioni plenarie del Comitato, di cui una in presenza (28 novembre 2021), alle attività della *Global Privacy Assembly* (GPA) e ad altri eventi su profili attinenti alla protezione dei dati personali, quali la *Study Visit* organizzata presso il Garante nell'ambito del progetto di gemellaggio (*Twinning*) con l'Autorità di controllo albanese (cfr. par. 23.5).

Nel periodo di riferimento, poi, il Segretario generale si è occupato di questioni di riorganizzazione interna, anche in relazione alle criticità emerse per effetto dell'emergenza pandemica e delle ridotte dimensioni dell'Ufficio. Le soluzioni in tal senso adottate hanno garantito la puntuale osservanza della programmazione dell'attività del Garante, la gestione delle risorse interne (incluso l'incremento della pianta organica e il rinnovo degli incarichi ai dirigenti delle unità organizzative) e l'approfondimento delle problematiche riguardanti il personale (anche attraverso proficui confronti con le Organizzazioni sindacali), nonché la gestione della contrattualistica e della digitalizzazione dell'Ufficio, che in alcuni momenti hanno richiesto di intervenire anche con azioni non espressamente preventivate.

Inoltre, è proseguita l'attività, attualmente facente capo alla Segreteria generale, di mantenimento e aggiornamento del Registro delle violazioni e delle misure correttive del Garante, come previsto dal RGPD.

Controllo di gestione

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.

Rpd

Il Responsabile della protezione dei dati personali presente presso il Garante per lo svolgimento dei compiti indicati agli artt. 38 e 39 del RGPD ha puntualmente operato al fine di verificare l'osservanza delle attività di trattamento alle disposizioni del Regolamento e del Codice. Come stabilito dal RGPD ha fornito continua assistenza ai dipartimenti e al personale per assicurare la corretta applicazione della disciplina vigente in materia di protezione dei dati personali. Ha altresì partecipato alle attività svolte in seno alla rete degli Rpd delle autorità indipendenti italiane e partecipato alla rete degli Rpd delle autorità di protezione dati europee, condividendo ed armonizzando buone pratiche nelle materie di interesse.

Nel corso dell'anno, in particolare, ha dato impulso all'avvio dell'aggiornamento del registro delle attività di trattamento del Garante fornendo il necessario supporto alle unità organizzative ai fini della relativa compilazione.

27.4. *"Autorità trasparente" e adempimenti relativi alla disciplina anticorruzione*

L'Autorità ha continuato ad alimentare la sezione "Autorità trasparente" del sito web, all'interno della quale sono state tempestivamente pubblicate sia la relazione annuale del Responsabile della prevenzione della corruzione e della trasparenza (Rpct) per l'anno 2021, in conformità a quanto previsto dall'art. 1, comma 14, l. n. 190/2012 (doc. web n. 9740876) – relativa all'efficacia delle misure di prevenzione definite nel Piano triennale di prevenzione della corruzione e della trasparenza 2021-2023 – sia la griglia di rilevazione di cui all'all. 2 della delibera Anac 21 febbraio 2018, n. 141, in assenza di Oiv o strutture equivalenti presso l'Autorità, che il Rpct è tenuto a pubblicare. Dando continuità all'attuazione delle misure generali, è in via di predisposizione il nuovo Piano triennale di prevenzione della corruzione e della trasparenza: si tratta del terzo Ptpct adottato dall'Autorità il quale, sulla base delle aree di rischio previamente individuate, individua le misure di prevenzione della corruzione già attuate e quelle da continuare ad attuare. Ai fini della sua predisposizione, anche in considerazione delle ulteriori competenze attribuite all'Autorità (segnatamente, in materia di *revenge porn,* con la novella dell'art. 144-*bis* del Codice) e in ragione delle modifiche organizzative introdotte (ad es. con la costituzione di nuove unità organizzative di primo livello), si è provveduto ad una rinnovata mappatura dei processi dell'Autorità.

Con riguardo alla disciplina in materia di accesso civico, come noto prevista all'art. 5, d.lgs. n. 33/2013, gli uffici dell'Autorità hanno dato riscontro a tutte le istanze pervenute (pari a venti); non diversamente, il Rpct ha fornito riscontro a quattro istanze di riesame ex art. 5, comma 7, d.lgs. n. 33/2013 portate alla sua attenzione; è pervenuta un'unica istanza di accesso civico relativa a dati a pubblicazione obbligatoria (ex art. 5, comma 1, d.lgs. n. 33/2013), anch'essa oggetto di riscontro e della quale si è tenuto conto per rendere di più immediata fruibilità i procedimenti interni in materia di accesso (illustrati in altra sezione del sito web istituzionale), aggiornando le informazioni relative alle tipologie di procedimento in essere presso l'Autorità (cfr. doc. web n. 4541495).

27.5. *Il settore informatico e tecnologico*

Transizione al digitale

Il 2021 è stato ancora caratterizzato da intensa attività di sviluppo dei sistemi informativi, nonostante la persistente carenza di personale tecnico, a sostegno del diffuso ricorso a forme di lavoro agile e remoto a seguito della perdurante emergenza pandemica.

27

Le principali attività hanno riguardato aspetti infrastrutturali, tecnologici, funzionali ed anche applicativi, con la configurazione di sistemi in dotazione a supporto del lavoro documentale dematerializzato.

I principali interventi hanno riguardato prevalentemente la digitalizzazione della procedura di notifica all'Autorità delle violazioni dei dati personali (*data breach*) (per la quale nel 2020 era stato reso disponibile uno strumento di *self assessment*) che consente ai titolari del trattamento di compilare e trasmettere *online* il modulo di notifica. Tale procedura gestisce il processo di notifica per fasi, prevedendo l'invio di appositi avvisi (*reminder*) che segnalano ai titolari del trattamento la necessità di fornire gli elementi non disponibili all'atto della notifica iniziale.

È stata avviata la progettazione di servizi *online* per la ricezione di comunicazioni da parte di soggetti esterni che si rivolgono al Garante in qualità di interessati o segnalanti (ad es. nel caso di segnalazioni di telefonate indesiderate, segnalazioni per impedire le pratiche di *revenge porn* o di cyberbullismo).

Nel corso dell'anno è stato attivato il nuovo portale web dell'Autorità, dopo un'intensa revisione che ha reso più strutturate e più facilmente ricercabili le informazioni ed ha ottimizzato l'accessibilità con l'aggiunta di appositi servizi (tra cui il bollino blu, presente in ogni pagina, che permette una navigazione altamente personalizzata).

Per quanto riguarda altri aspetti funzionali o applicativi, sono state portate a compimento diverse attività di sviluppo e integrazione, tra cui quelle relative ai web *service* per l'integrazione nelle applicazioni *online* delle funzionalità del sistema di gestione documentale; per l'integrazione tra IndicePA e i dati registrati nel sistema di protocollo; per l'automazione delle risposte alla ricezione della corrispondenza, in ottemperanza alle linee guida AgID in tema di documento informatico.

Aggiornamenti infrastrutturali o di sicurezza

In merito ai profili infrastrutturali, sono state svolte diverse attività tra le quali, particolarmente significative, l'aggiornamento dei sistemi *on premises* con l'adozione del modello "iperconvergente" a supporto della progressiva migrazione dell'intero sistema informativo verso servizi *cloud* IaaS; la realizzazione di due sale riunioni attrezzate con dispositivi di videoconferenza; la realizzazione di una infrastruttura *cloud* per il salvataggio dei dati in modalità BaaS; la realizzazione di un sistema di autenticazione multi-fattoriale per la rete VPN (*Virtual Private Network*) e per altri servizi.

PAGINA BIANCA

1997-2022

GPDP

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

I dati statistici

RELAZIONE ANNUALE

2021

PAGINA BIANCA

IV - I dati statistici 2021

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	448
Pareri su norme di rango primario statale, delle regioni e delle autonomie	7
Pareri su atti regolamentari e amministrativi	65
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	17
Parere 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	2
Autorizzazione di accordi amministrativi ai sensi dell'artt. 46, par. 3, lett. *b*), 58, par. 3, lett. *i*) e 63, del RGPD	1
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché a seguito di accertamenti d'ufficio	112
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché a seguito di accertamenti d'ufficio con contestuale ordinanza-ingiunzione	140
Provvedimenti collegiali a seguito di notifica di violazione di dati	7
Provvedimenti collegiali a seguito di notifica di violazione di dati con contestuale ordinanza-ingiunzione	32
Provvedimenti di approvazione di codici di condotta	2
Comunicazioni di violazione dei dati	2.071
Riscontri a segnalazioni e reclami (art. 11, reg. Garante n. 1/2019)	9.184
Riscontri a quesiti (art. 11, reg. Garante n. 1/2019)	543
Risposte ad atti di sindacato ispettivo e di controllo	7
Audizioni del Presidente del Garante o memorie scritte trasmesse al Parlamento	14
Contatti Servizio relazioni con il pubblico	18.705
Accertamenti e controlli effettuati *in loco* (artt. 157-158, d.lgs. n. 196/2003)	49
Pagamenti derivanti dall'attività sanzionatoria	13.465.148
Comunicazioni di notizia di reato all'Autorità giudiziaria	12
Opposizioni (trattate) a provvedimenti del Garante	115
Ricorsi giurisdizionali trattati ex art. 152, d.lgs. n. 196/2003	58
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 1, d.lgs. n. 33/2013	1
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 2, d.lgs. n. 33/2013	20
Istanze di riesame a seguito di diniego all'accesso civico presentate al Rpct e riscontrate ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	4
Misure correttive e sanzionatorie (art. 58, par. 2, del RGPD)	388
Misure correttive e sanzionatorie (d.lgs. n. 51/2018)	1
Riunioni del Comitato europeo per la protezione dei dati personali	15
Partecipazione a sottogruppi di lavoro del Comitato europeo per la protezione dei dati personali	175
Riunioni e ispezioni autorità comuni di controllo/organismi di supervisione (Europol, SIS II, Dogane, Eurodac, VIS)	9
Conferenze internazionali	1
Riunioni presso l'OCSE e CoE	35
Altre conferenze e incontri internazionali	46

Tabella 1. Sintesi delle principali attività dell'Autorità

Tabella 2. Attività di comunicazione dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	85
Newsletter	14
Prodotti editoriali	2
Campagne informative	14
Video *spot* e *teaser* informativi	21
Infonografiche e pagine tematiche	71

Tabella 3. Pareri ex art. 36, par. 4, del RGPD su norme di rango primario statale, delle regioni e delle autonomie

Pareri ex art. 36, par. 4, del RGPD su norme di rango primario statale, delle regioni e delle autonomie	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	2
Giustizia	2
Open data	1
Sanità	1
Sanità: Covid-19	1
Totale	**7**

Tabella 4. Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi al Governo

Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi al Governo	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	9
Diritti fondamentali	1
Fisco	7
Funzioni di interesse pubblico	6
Giustizia	8
Istruzione	3
Sanità	1
Sanità: Covid-19	5
Trasporti	3
Totale	**43**

(*) inerenti anche ad affari pervenuti anteriormente al 2021

Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi ad altre Istituzioni	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	9
Fisco	7
Funzioni di interesse pubblico	2
Statistica	4
Totale	**22**

Tabella 5. Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi ad altre Istituzioni

Misure correttive e sanzionatorie	
Avvertimenti a titolare/responsabile del trattamento (art. 58, par. 2, lett. *a*), del RGPD)	23
Ammonimenti a titolare/responsabile del trattamento (art. 58, par. 2, lett. *b*), del RGPD)	55
Ingiunzioni a titolare/responsabile del trattamento a soddisfare le richieste dell'interessato concernenti l'esercizio dei diritti riconosciuti dal RGPD (art. 58, par. 2, lett. *c*), del RGPD)	28
Ingiunzioni a titolare/responsabile del trattamento di conformare i trattamenti alle disposioni del RGPD (art. 58, par. 2, lett. *d*), del RGPD)	43
Ingiunzioni a titolare del trattamento di comunicare all'interessato una violazione dei dati personali (art. 58, par. 2, lett. *e*), del RGPD)	1
Imposizioni di limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento (art. 58, par. 2, lett. *f*), del RGPD)	44
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*), del RGPD)	22
Sanzioni amministrative pecuniaria ex art. 83 (art. 58, par. 2, lett. *i*), del RGPD)	172
Totale	**388**

Tabella 6. Misure correttive e sanzionatorie (art. 58, par. 2, del RGPD)

Misure correttive e sanzionatorie (d.lgs. n.51/2018)	
Sanzioni amministrative pecuniaria (art. 42, d.lgs. n. 51/2018)	1
Totale	**1**

Tabella 7. Misure correttive e sanzionatorie (d.lgs. n. 51/2018)

Comunicazioni di notizia di reato all'Autorità giudiziaria	
Trattamento illecito dei dati (art. 167, d.lgs. n. 196/2003)	5
Violazioni in materia di controlli a distanza dei lavoratori (art. 171, d.lgs. n. 196/2003)	1
Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter*, c.p.)	3
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168, d.lgs. n. 196/2003)	1
Inosservanza di provvedimenti del Garante (art. 170, d.lgs. n. 196/2003)	2
Totale	**12**

Tabella 8. Comunicazioni di notizia di reato all'Autorità giudiziaria

(*) inerenti anche ad affari pervenuti anteriormente al 2021

Tabella 9. Pagamenti derivanti dall'attività sanzionatoria

Pagamenti derivanti dall'attività sanzionatoria	
Pagamenti spontanei dei contravventori	12.047.671
Riscossione coattiva	1.417.477
Totale	**13.465.148**

Tabella 10. Cooperazione tra autorità nazionali di protezione dei dati personali in IMI (Capo VII RGPD)*

Cooperazione tra autorità nazionali di protezione dei dati personali – procedure IMI (Capo VII RGPD)		
1) Decisioni finali adottate nell'ambito della attività di cooperazione rispetto alle quali il Garante ha agito in qualità di:		**282**
a) "autorità capofila" (LSA)	2	
b) "autorità interessata" (CSA)	280	
2) Procedure preliminari ex art. 56 del RGPD		**562**
a) Procedure preliminari pervenute rispetto alle quali l'Autorità si è dichiarata "autorità interessata"	294	
b) Procedure preliminari pervenute rispetto alle quali l'Autorità si è dichiarata "autorità non interessata"	169	
c) Procedure preliminari pervenute rispetto alle quali l'Autorità ha assunto il ruolo di "autorità capofila"	11	
d) Procedure preliminari pervenute rispetto alle quali l'Autorità ha fornito altro riscontro	19	
e) Procedure preliminari promosse dall'Autorità	6	
f) Altro	63	
3) Procedure di cooperazione ad impatto esclusivamente locale ex art. 56, par. 2, del RGPD		**1**
4) Procedure di cooperazione informale ex art. 60 del RGPD rispetto alle quali vi è stata una partecipazione dell'Autorità in qualità di:		**105**
a) "autorità interessata"	99	
b) "autorità capofila"	6	
5) Progetti di decisione ex art. 60 del RGPD rispetto ai quali l'Autorità ha cooperato in qualità di:		**126**
a1) "autorità interessata"	122	
a2) "autorità interessata" e rispetto ai quali sono state sollevate "obiezioni pertinenti e motivate" o commenti ex art. 60, par. 4, del RGPD	18	
b) "autorità capofila"	4	
6) Richieste di assistenza reciproca ex art. 61 del RGPD		**176**
a) ricevute da altre Autorità	138	
b) inviate ad altre Autorità	38	

Tabella 11. Procedure IMI nell'ambito del meccanismo di coerenza

Meccanismo di coerenza - procedure IMI (Capo VII RGDP)	
1) Procedure relative all'attività consultiva dell'EDPB ex art. 64 del RGPD	1
2) Procedure relative all'attività decisoria dell'EDPB per la risoluzione delle controversie ex art. 65 del RGPD con la partecipazione dell'Autorità	2
3) Procedure d'urgenza ex art. 66 del RGPD	6

*in relazione a procedure pervenute dal 01/01/2021

Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza	
Assicurazioni	7
Credito	72
Imprese	284
Lavoro	16
Libertà di espressione e di informazione	28
Notificazioni di violazione dei dati	133
Reti telematiche	696
RGPD	4
Trattamento dati in ambito sanitario	17
Videosorveglianza	4
Totale	**1.261**

Tabella 12. Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza

Segnalazioni e reclami		
	Pervenuti nell'anno	**Riscontri resi nell'anno (*)**
Attività ispettive	2	41
Affari legali e giustizia	159	105
Libertà di manifestazione del pensiero e cyberbullismo	854	667
Realtà economiche e produttive	3.185	3.355
Realtà pubbliche	2.672	896
Reti telematiche e *marketing*	5.356	3.179
Sanità e ricerca	626	706
Tecnologie digitali e sicurezza informatica	67	235
Totale	**12.921**	**9.184**

Tabella 13. Segnalazioni e reclami

Quesiti		
	Pervenuti nell'anno	**Riscontri resi nell'anno (*)**
Attività ispettive	4	3
Affari legali e giustizia	19	8
Libertà di manifestazione del pensiero e cyberbullismo	17	7
Realtà economiche e produttive	212	122
Realtà pubbliche	348	228
Reti telematiche e *marketing*	91	32
Sanità e ricerca	126	143
Totale	**817**	**543**

Tabella 14. Quesiti

(*) inerenti anche ad affari pervenuti anteriormente al 2021

Tabella 15. Servizio relazioni con il pubblico

Servizio relazioni con il pubblico	
E-mail esaminate	15.004
Contatti telefonici	3.500
Persone in visita al Srp (chiusura al pubblico da marzo 2020)	0
Trattazione pratiche relative a fascicoli	201
Totale	**18.705**

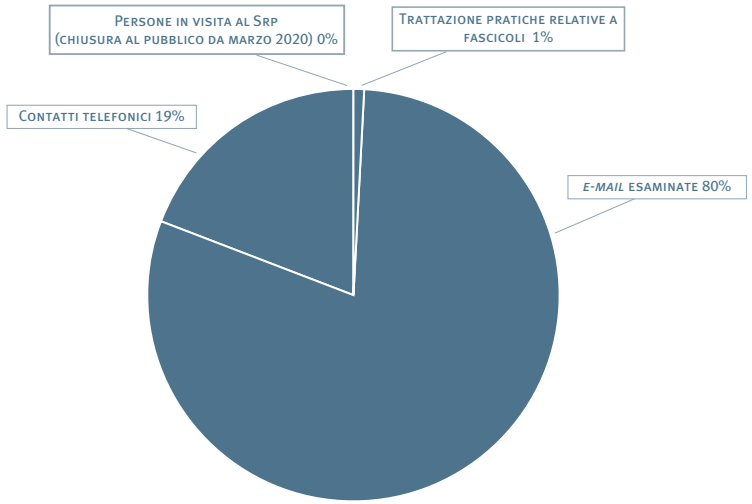
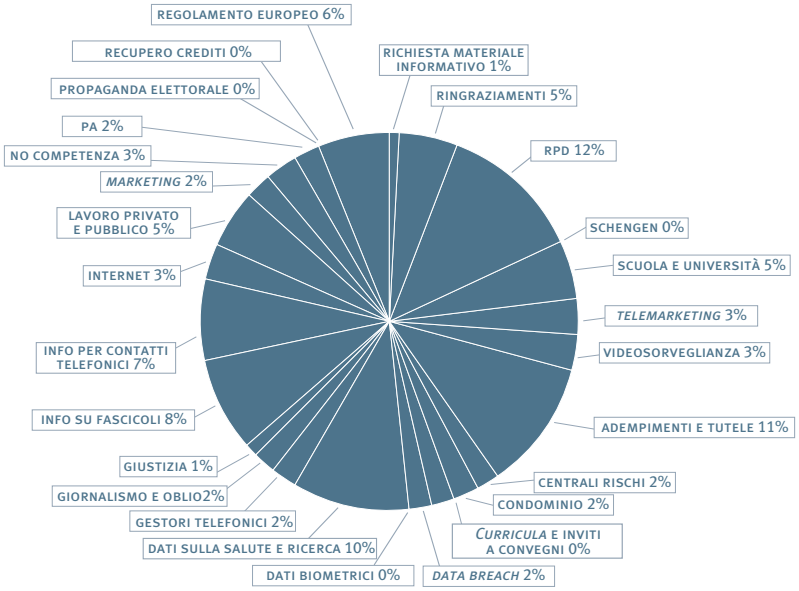


Grafico 16. Oggetto delle *e-mail* esaminate dal Servizio relazioni con il pubblico



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		1
Dirigenti	16	0	2	14
Funzionari	91	4	2	93
Operativi	24	1		25
Esecutivi	0			
Totale	**131**	**6**	**4**	**133**
Personale a contratto (art. 156, comma 5, del Codice)				20

Tabella 17. Personale in servizio

Risorse finanziarie				
Entrate accertate	**Anno 2021**	**Anno 2020**	**Variazione**	
Entrate correnti	35.969.515	30.447.905	5.521.610	18,13%
Totale entrate	**35.969.515**	**30.447.905**	**5.521.610**	**18,13%**
Spese impegnate		**Anno 2020**	**Variazione**	
Spese di funzionamento	25.280.392	22.973.973	2.306.419	10,04%
Spese in c/capitale	624.459	509.823	114.636	22,49%
Trasferimenti ad amministrazioni	333.451	330.486	2.965	0,90%
Totale spese	**26.238.302**	**23.814.282**	**2.424.020**	**10,18%**

Valori in euro

Tabella 18. Risorse finanziarie

(*) Situazione alla data del 31/12/2021

Tabella 19. Attività internazionali dell'Autorità

Unione europea			
Comitato europeo per la protezione dati	**Sessioni plenarie**		14 gennaio 20 febbraio 9 e 31 marzo 13 aprile 19 maggio 18 giugno 7, 12 e 28 luglio 14 e 24 settembre 13 ottobre 18 novembre 14 dicembre
	Riunioni dei sottogruppi	**Sottogruppo questioni strategiche e attività consultiva (SAESG)**	15 gennaio 11 e 15 febbraio 3 marzo 10 e 31 maggio 8 giugno 1-2 e 29 luglio 30 novembre
		***Border Travel Law Enforcement* (BTLE)**	21 gennaio 18 febbraio 18 e 25 marzo 22 aprile 3 maggio 1 e 24 giugno 15 luglio 2 e 28 settembre 28 ottobre 30 novembre
		Cooperation	18 gennaio 8 e 22 febbraio 23 marzo 29 aprile 6 e 27 maggio 17 e 21 giugno 15 luglio 23 settembre 29 ottobre 25 novembre 15 dicembre
		Compliance, E-Government and Health	18-19 gennaio 16-17 febbraio 4 e 22 marzo 19 aprile 5 e 12 maggio 7 e 10 giugno 6 luglio 1 settembre 18-19 ottobre 12 e 24 novembre 17 dicembre

Comitato europeo per la protezione dati	**Riunioni dei sottogruppi**	***Financial Matters***	11 gennaio 15 febbraio 18 marzo 26 aprile 18 maggio 22 giugno 20 luglio 16 settembre 12 ottobre 5 novembre 17 dicembre
		Cookie Banner Task Force	8, 29 novembre
		Key Provisions	7 e 27 gennaio 4 e 11 marzo 31 marzo 21 aprile 11 maggio 8 giugno 5-6 luglio 21 settembre 26 ottobre 15 novembre 1° dicembre
		International Transfers, BCR Session, Task Force on Supplementary Measures	6-12 e 25-29 gennaio 9-10 e 23-24 febbraio 3, 15-16 e 26-29 marzo 7-8 e 27-28 aprile 26 maggio 1-2, 9, 21 e 30 giugno 9, 13 e 27 luglio 7-8, 20 e 28 settembre 5-6 ottobre 9-10 e 9 novembre 7-8, e 13 dicembre
		Technology	21 gennaio 11-12 febbraio 4-5 marzo 6-7 maggio 3-4, 24-25 e 30 giugno 3 e 30 settembre 1° ottobre 4-5 novembre 3 dicembre
		IT *Users*	26 gennaio 4 maggio 22 giugno 22 settembre 9 dicembre
		Enforcement	2 gennaio 17 febbraio 10 e 24 marzo 5 maggio 2, 16-17 e 23 giugno 5-6 e 16 luglio 22 settembre 27 ottobre 24 novembre

Comitato europeo per la protezione dati	**Riunioni dei sottogruppi**	***Fining Task Force, Drafting Team (Guidelines on the calculation of administrative fines)***	19 gennaio 2 marzo 17 marzo 15 aprile 29 aprile 25 e 29 maggio 25 giugno 13 luglio 29 settembre 2 dicembre
		Task Force 101 Complaints	4 e 19 febbraio 31 marzo 28 aprile 28 maggio 17 giugno 5 e 30 luglio 23 settembre 14 ottobre 5 novembre 9 dicembre
		Gruppo dei coordinatori	29 ottobre
		Social Media Working Group	26 febbraio 12 aprile 17 maggio 9 luglio 17 settembre 13 dicembre
		EDPB DPO *Network*	6 dicembre
		EDPB *Communications Network*	7 e 26 gennaio 2 marzo 8 aprile 12 maggio 9 e 30 giugno 8 settembre 6 ottobre 10 novembre 8 dicembre

Unione europea	
Gruppo di coordinamento della supervisione SIS II	16 giugno, 25 novembre
Gruppo di coordinamento della supervisione VIS	17 giugno, 24 novembre
Gruppo di supervisione del sistema Eurodac	17 giugno, 24 novembre
Gruppo di coordinamento della supervisione del sistema di informazione doganale: SID	14 giugno
Europol *Coordination Board*	15 giugno, 23 novembre

Riunione presso l'OCSE e CoE		
Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	**Comitato DGP *(Data Governance and Privacy in the Digital Economy)***	7 e 13 aprile 17 settembre 16 e 22 novembre
	Gruppo di redazione sull'accesso dei governi ai dati personali del settore privato	4 e 24 febbraio 9 e 23 marzo 8 luglio
	DGP *Bureau*	17 settembre (DGP *Bureau*)
	GPA Covid-19 WP	15 e 21-22 e 26 gennaio 10 e 24 febbraio 10 e 24 marzo 7 e 21 aprile 5 maggio 2 giugno 7 luglio 24 agosto 6 ottobre
	High Level Launch of the Recommendation on Children in the Digital Environment	18 novembre
Consiglio d'Europa	**Comitato Consultivo Convenzione n. 108/1981 (T-PD)**	28-30 giugno (plenaria) 17-19 novembre (plenaria)
	T-PD *Bureau*	24-26 marzo 28-30 settembre 20-21 dicembre
	Comitato *ad hoc* in materia di intelligenza artificiale (CAHAI)	24 febbraio 27 maggio 29 settembre 30 novembre-2 dicembre

Conferenze internazionali	
GPA **(Conferenza internazionale delle autorità di protezione dati)**	18-21 ottobre 2021

Altre conferenze e *meeting*	
ICPEN ***Workshop su "Enforcement of Consumer Data Privacy"***	25 febbraio
Group of Volunteers: Cooperation among consumer and data protection authorities	19 marzo 19 novembre
Progetto Twinning con l'Albania ***Steering Committees, Rolling Work Plans, Horizontal activities, Final Event***	11-15, 18-22 e 26-29 gennaio 15-19 febbraio 2-5, 8-11 e 23-26 marzo 31 marzo-2 aprile 6-9, 13-16, 19-22 e 27-30 aprile 4-7, 18-20, 22 e 25-28 maggio 31 maggio-1,3,4 giugno 8-11 e 15-18 giugno 29 giugno-2 luglio 5-8, 13-16, 19-23 e 27-30 luglio 30 agosto-2 settembre 14-17 e 21-24 settembre 13-15 e 26-29 ottobre 2-4, 10-13, 15-16 e 22-26 novembre 2-3 e 7 dicembre
European Case Handling Workshop	16-17 novembre
Project Commitee* (PC) 317 di ISO** ***Consumer protection - Privacy by design for consumer goods and services	19-22 aprile 13-16 settembre
***Working Group* 5 del JTC 13 del CEN CENELEC** **(ex CEN/CLC/TC8)**	12 marzo
***Working Group 5* – ISO/IEC JTC1/SC27**	7-8 e 12-15 aprile
G20 *Italy* ***Multistakeholder Forum***	6 maggio

Redazione
Garante per la protezione dei dati personali

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

stampa:
Tiburtini Srl


25
1997-2022
GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PAGINA BIANCA

181360193340