SENATO DELLA REPUBBLICA

XVIII LEGISLATURA

Doc. **CXXXVI**
n. **2**

RELAZIONE

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

(Anno 2019)

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

Presentata dal Garante per la protezione dei dati personali (SORO)

Comunicata alla Presidenza il 30 giugno 2020

PAGINA BIANCA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Protezione dati, emergenza, democrazia

Discorso del Presidente

Antonello Soro

Relazione2019

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza Venezia, 11
00187 Roma
tel. 06 696771
email: protocollo@gpdp.it
www.garanteprivacy.it

Relazione2019

Discorso del Presidente

Antonello Soro

Roma, 23 giugno 2020

PAGINA BIANCA

1. Corpo, tecnica, libertà

Signor Presidente della Camera, Autorità, Signore e Signori,

un anno fa abbiamo presentato la relazione della nostra attività come conclusiva del mandato. Lo stallo nelle procedure di nomina, dovuto alla crisi di governo prima, all'emergenza sanitaria poi, ha prorogato sinora la nostra attività, non senza alcune difficoltà, dovute soprattutto all'incerto orizzonte di volta in volta prefigurato, con rinvii brevi del voto e ai limiti intrinseci del regime di ordinaria amministrazione, solo recentemente rimossi con l'intervento del legislatore.

Ciononostante, la nostra attività è stata sempre svolta con il massimo dell'impegno e della responsabilità, nella consapevolezza di dover garantire, senza soluzioni di continuità né affievolimenti sia pure momentanei, un diritto di libertà che, anche e soprattutto nel contesto emergenziale, si è dimostrato ancora più determinante. Un diritto inquieto, perché in costante evoluzione e mai tiranno, perché capace di porsi sempre in equilibrio con gli interessi giuridici che di volta in volta vengano in rilievo.

Ma la pandemia ha segnato - come in molti altri campi - un punto di non ritorno: il momento fondativo di una nuova consapevolezza.

Se fino a pochi mesi fa, nell'epoca più tecnicamente evoluta della storia umana, un timore diffuso era quello - forse ancestrale ma costantemente rinnovato - di una vera e propria sostituzione dell'uomo da parte delle macchine, oggi la paura si è materializzata nella concretezza del corpo, violato dalla malattia.

Questa rinnovata scoperta del naturale, del corporeo, del materiale, è servita, in un certo senso, a ricordarci come persino il progresso più avanzato, l'innovazione più audace - che paradossalmente l'emergenza ha appunto promosso - abbiano un fondamento umano, con cui dobbiamo fare i conti.

Ed è bene che da questa consapevolezza nasca un approccio diverso al rapporto tra uomo e tecnica, che sappia fare tesoro di tutto ciò che abbiamo vissuto, nel bene e nel male, in questi mesi.

La misura di prevenzione sanitaria più antica, ovvero la "quarantena" - che incide sulla concretezza del vivere quotidiano - si è affiancata al ricorso all'intelligenza artificiale negli studi epidemiologici e agli algoritmi quale ausilio diagnostico.

E le distanze fisiche imposte come misura, appunto la più antica, di contenimento dei contagi sono state colmate, paradossalmente, dalla prossimità offerta dalla tecnologia, capace di annullare gli spazi interposti tra i corpi e di ricostituire, nella dimensione digitale, quelle piazze svuotate nel reale.

Le distanze fisiche non sono divenute sociali grazie alla realizzazione, su innumerevoli piattaforme, di sale riunioni in cui lavorare senza rinunciare al confronto o classi dove formare ragazzi da remoto. Rispetto a tutte queste fattispecie abbiamo indicato - con strumenti agili quali linee guida e FAQ - cautele e condizioni per valorizzare al massimo l'uso della tecnologia salvaguardando l'autodeterminazione dei lavoratori, la libertà di insegnamento, la riservatezza dei minori.

Anche rispetto alla celebrazione da remoto di un processo, quale quello penale, strettamente ancorato al principio di oralità, al contraddittorio costante e alla dialettica d'aula, abbiamo segnalato l'esigenza di rafforzare le garanzie di sicurezza dei dati, delicatissimi, affidati ai canali telematici, per smaterializzare davvero - si è detto - le carte, non le persone.

Un contributo analogo ci è stato richiesto in ordine alla giustizia amministrativa, rispetto alla quale abbiamo suggerito anche un'interpretazione adeguatrice della vigente disciplina sulla pubblicità dei provvedimenti giurisdizionali.

La tecnica si è così prestata tanto alla libera esplicazione quanto al controllo della persona, esorcizzando anche la percezione di fragilità, ricostruendo legami e relazioni in un altrove divenuto, ormai, imprescindibile.

Ma come abbiamo rimosso, per decenni e anche più, la nostra vulnerabilità

fisica, ora rischiamo di ignorare quella, non meno insidiosa, del nostro io digitale.

La traslazione, mai così totalizzante, della nostra esistenza individuale e collettiva nella dimensione immateriale del web, espone infatti ciascuno di noi - in primo luogo attraverso i propri dati - alle sottili ma pervasive minacce di una realtà, quale quella digitale, tanto straordinaria quanto poco presidiata.

2. Diritti in emergenza

L'inattesa accelerazione impressa dalla pandemia alla transizione digitale impone oggi di ripensare, con altrettanta tempestività, il nostro modo di concepire questa nuova dimensione della vita, ormai sempre più indistinguibile da quella tradizionale, le cui coordinate godono tuttavia della solidità assicurata da prassi radicate.

L'epidemia ha profondamente mutato, infatti, l'allocazione dei poteri e le loro reciproche relazioni, non solo riarticolando l'equilibrio tra centro e periferia, politica e tecnocrazia, normazione e amministrazione, ma anche tracciando nuove coordinate del rapporto della nostra vita con il digitale e rendendone più urgente l'esigenza regolatoria, anche sotto il profilo della sostenibilità di sempre più incisivi poteri privati.

La devoluzione alla dimensione immateriale di pressoché tutte le nostre attività non è un processo neutro, ma comporta, se non assistito da adeguate garanzie, l'esposizione a inattese vulnerabilità in termini non solo di sicurezza informatica ma anche di soggezione a ingerenze e controlli spesso più insidiosi, perché meno percettibili di quelli tradizionali.

Particolarmente significativo è il contesto lavorativo, rispetto al quale abbiamo inteso fornire specifici chiarimenti anche in ordine alle attività di prevenzione e, più in generale, all'estensione dei poteri datoriali.

Il diffuso ricorso allo *smartworking* - generalmente necessitato e improvvisato - ha poi catapultato una quota significativa della popolazione in una

dimensione delle cui implicazioni non sempre si ha piena consapevolezza e di cui va impedito ogni uso improprio.

Potendo favorire una nuova articolazione dei processi produttivi in grado di accrescere efficienza e flessibilità, lo *smartworking* potrebbe ragionevolmente divenire una forma diffusa, effettivamente alternativa, di organizzazione del lavoro.

Per questa ragione andranno seriamente affrontati e risolti tutti i problemi emersi in questi mesi: dalle dotazioni strumentali alla garanzia di connettività, alla sicurezza delle piattaforme, all'effettività del diritto alla disconnessione, senza cui si rischia di vanificare la necessaria distinzione tra spazi di vita privata e attività lavorativa: annullando così alcune tra le più antiche conquiste raggiunte per il lavoro tradizionale.

Il ricorso intensivo alle nuove tecnologie per rendere la prestazione lavorativa non deve rappresentare l'occasione per il monitoraggio sistematico e ubiquitario del lavoratore, ma deve avvenire nel pieno rispetto delle garanzie sancite dallo Statuto a tutela dell'autodeterminazione, che presuppone anzitutto un'adeguata formazione e informazione del lavoratore.

Va, in particolare, inteso in modo rigoroso - lo abbiamo ricordato anche in sede parlamentare - il vincolo finalistico all'attività lavorativa che, rispetto ai controlli mediante strumenti utilizzati per rendere la prestazione, legittima l'esenzione dalla procedura concertativa o autorizzativa.

Per garantire, dunque, che le nuove tecnologie rappresentino un fattore di progresso, e non di regressione sociale, valorizzando anziché comprimendo le libertà affermate sul terreno lavoristico, è indispensabile garantirne la sostenibilità sotto il profilo democratico e la conformità ad alcuni irrinunciabili principi.

Lungi dal rappresentare un lusso da non potersi permettere in tempi difficili, la protezione dati ha dimostrato, da questo punto di vista, non solo di consentire tutto ciò che sia opportuno per il contrasto della pandemia, ma anche di poter fondare, attraverso le garanzie accordate ai nostri dati, quella fiducia

nel digitale senza la quale nessuna soluzione tecnica potrebbe mai avere successo.

Quale contributo utile all'attività di prevenzione sanitaria, abbiamo indicato, al Parlamento e al Governo, i principali criteri da seguire per migliorare l'efficacia delle misure adottate, in particolare rispetto al *contact tracing*, che sin da subito abbiamo richiesto tracciasse i contatti, non le persone.

Nel rilevare l'importanza dei principi di proporzionalità, necessità, adeguatezza cui devono conformarsi le scelte limitative dei diritti fondamentali, abbiamo indicato le diverse implicazioni delle varie soluzioni tecniche proposte, preferibili nella misura in cui riescano a minimizzare l'impatto sulla persona e la sua vita privata, pur garantendo l'attendibilità e l'efficacia dei risultati.

Analogo bilanciamento tra esigenze di sanità pubblica e tutela individuale abbiamo auspicato in relazione all'indagine di sieroprevalenza prevista rispetto al Covid 19, con indicazioni utili alla più efficace conduzione dello studio.

Rispetto alle varie circostanze sottoposteci abbiamo sottolineato la necessità di studiare modalità e ampiezza delle misure da adottare in vista della loro efficacia, gradualità e adeguatezza, senza preclusioni astratte o tantomeno ideologiche, ma anche senza improvvisazioni o velleitarie deleghe, alla sola tecnologia, di attività tanto necessarie quanto complesse.

3. La democrazia di fronte alla pandemia

Non è stato mai così evidente, come in questi mesi, che l'innovazione digitale abbia rappresentato un "fatto sociale totale", capace di inscrivere in nuove coordinate un'intera costruzione del mondo e la sua stessa antropologia. L'emergenza sanitaria ha evidenziato la necessità del ricorso alla tecnologia in funzione ausiliaria della scienza e la corrispettiva esigenza di valorizzare il digitale quale spazio immateriale in cui ritrovarsi.

E la protezione dati, regolando le condizioni per la circolazione di ciò che,

come il dato, rappresenta l'elemento costitutivo del digitale, in questo scenario si è rivelata un presupposto ineludibile di ogni possibile equilibrio tra l'uomo e la tecnica, la libertà e il determinismo algoritmico.

Le emergenze devono, del resto, poter contemplare anche alcune significative deroghe ai diritti, purché non irreversibili e proporzionate. Non devono essere, in altri termini, un punto di non ritorno ma un momento in cui modulare prudentemente il rapporto tra norma ed eccezione, coniugando istanza personalistica ed esigenze solidaristiche.

La duttilità del diritto, la sua capacità di adeguarsi al contesto riconoscendo gli adattamenti necessari e proporzionati alle specifiche esigenze, pur senza intaccare il "nucleo duro" dei diritti fondamentali, è la più grande forza della democrazia.

E questa forza sta dimostrando di avere il nostro Paese che, pur non nuovo a circostanze difficilissime, sta affrontando la prova più impegnativa dal secondo dopoguerra, utilizzando anche la tecnica in modo sostenibile, a fini di utilità sociale.

Il rischio che dobbiamo esorcizzare è quello dello scivolamento inconsapevole dal molto evocato modello coreano a quello cinese, scambiando la rinuncia a ogni libertà per efficienza e la biosorveglianza totalitaria per soluzione salvifica.

Così, una volta cessata questa difficile stagione, avremo forse imparato a rapportarci alla tecnologia in modo meno fideistico e più efficace, mettendola davvero al servizio dell'uomo.

Se c'è qualcosa che, forse, non tornerà più come prima, sarà il nostro rapporto con il digitale, di cui abbiamo compreso tutta l'ambivalenza e, dunque, la necessità di valorizzarne le straordinarie potenzialità "generative" contrastandone gli effetti nichilisti o anche solo regressivi.

Solo così sarà possibile fare tesoro della lezione di Tucidide, che ricordava come Atene fosse stata distrutta, più che dalla peste, dalla paura di questa.

4. Un circuito virtuoso

Ma anche in contesti diversi, nel corso di quest'anno, la protezione dei dati ha dimostrato di essere uno straordinario presupposto di democrazia, capace di coniugare personalismo e solidarismo, nascendo tra libertà e dignità, tra persona e società.

In linea generale, in questo secondo anno di applicazione della nuova disciplina, europea e di adeguamento interno, si è rivelata determinante l'interlocuzione con Parlamento e Governo, che in un circuito virtuoso ha consentito di migliorare, spesso sensibilmente, le norme proposte.

E' il caso, ad esempio, delle modifiche in tema di fascicolo sanitario elettronico, introdotte dal d.l. rilancio a seguito di un proficuo confronto con il Ministero della salute, o del reddito di cittadinanza, la cui disciplina attuativa ha concluso un percorso di collaborazione che ha contribuito a introdurre garanzie importanti per la riservatezza dei cittadini.

Rilevante si prospetta anche il confronto sul regolamento relativo agli obblighi di pubblicità inerenti i dirigenti pubblici, che dovrà conformarsi ai principi sanciti dalla sentenza 20/2019 della Corte costituzionale, in ordine al bilanciamento tra privacy e trasparenza dell'azione amministrativa.

Anche rispetto al registro pubblico delle opposizioni, il nostro parere sul regolamento attuativo della nuova disciplina ha rappresentato il punto di arrivo di un'interlocuzione - con le Camere prima e con il Governo poi - che ha consentito di rafforzare il contrasto del telemarketing selvaggio, sempre più invasivo e ramificato su plurimi rapporti commerciali.

Due tra le più elevate sanzioni irrogate quest'anno (una di oltre 27 e l'altra di oltre 11 milioni di euro) hanno, infatti, riguardato questo fenomeno, spesso indice sintomatico di una più generale negligenza rispetto agli obblighi sanciti in materia di protezione dati. Tale inosservanza è tanto più grave quanto più rilevante sia il patrimonio informativo societario che, in assenza di rigorose misure

di protezione dei dati, diviene vulnerabile terra di conquista per una sempre più abile criminalità informatica.

E' auspicabile che la consapevolezza del valore abilitante e pro-competitivo della protezione dei dati contribuisca a rendere questa disciplina parte essenziale del comune sentire.

Anche per questo è necessario completare, con gli ultimi tasselli, il quadro normativo interno emanando, in particolare, il regolamento attuativo del d.lgs. n. 51 del 2018, che dovrà definire le caratteristiche essenziali dei trattamenti svolti per fini di polizia e giustizia penale.

Un'ulteriore inerzia aggraverebbe la condizione di incertezza normativa che caratterizza aspetti, pur così rilevanti, della disciplina.

5. Equità fiscale e garanzie individuali

Le difficoltà proprie del contesto economico - già prima della pandemia - hanno reso urgente il recupero delle risorse sottratte dall'evasione: obiettivo essenziale per il nostro Paese, per garantire quell'equità fiscale "promessa" dalla Costituzione.

Per questo l'Autorità - pur assicurando il diritto dei cittadini al corretto trattamento dei loro dati - ha sempre supportato le misure volte a rafforzare l'efficacia dell'azione di contrasto dell'evasione fiscale, anche nell'ambito delle misure innovative introdotte in sessione di bilancio.

Lo sforzo con cui abbiamo tentato di promuovere un bilanciamento, il più equo possibile, tra l'efficacia delle verifiche fiscali e il diritto alla protezione dei dati personali è stato da alcuni scambiato per un ostacolo alle strategie adottate dall'amministrazione.

Quest'erronea rappresentazione - indifferente all'esigenza di mediazione propria di ogni scelta pubblica che riguardi una pluralità di interessi in gioco - stride con la lettera e lo spirito dei provvedimenti adottati dall'Autorità, in tale materia, durante l'intero mandato.

Ciascuno di essi, infatti, ha inteso garantire la sicurezza del patrimonio informativo dell'Agenzia delle entrate e l'esattezza dei dati (unitamente quindi all'affidabilità dei criteri di calcolo) sui quali si basano gli accertamenti, così migliorandone l'efficacia.

La profilazione sulla base del rischio fiscale - prevista sin dal 2011 - impone, infatti, l'adozione di garanzie volte a selezionare i dati effettivamente utili, escludendo quelli privi di rilievo e a correggere potenziali errori nel processo algoritmico conferendo così all'attività fiscale, anche nella percezione dei cittadini, quella più forte legittimazione che solo una combinazione equa di tecnologia e "fattore umano" può assicurare.

E' questo un profilo su cui abbiamo sollecitato l'attenzione del legislatore, anche relativamente al disegno di legge di bilancio.

Rispetto alla limitazione dei diritti dell'interessato prevista dalla stessa legge, abbiamo sottolineato la necessità di non escludere le possibilità di rettifica di dati inesatti, funzionale ad evitare valutazioni errate e quindi anche, in ipotesi, una falsa rappresentazione della capacità contributiva.

Tutt'altro che di ostacolo, dunque, l'azione del Garante si è rivelata semmai sinergica alla migliore efficacia degli accertamenti fiscali, nel rispetto peraltro del diritto dei cittadini a non essere erroneamente profilati come evasori.

La rappresentazione della protezione dati come ostacolo al libero dispiegamento dell'azione amministrativa (o delle indagini giudiziarie o della lotta all'evasione fiscale) è una costante del dibattito pubblico, che tuttavia mistifica in modo strumentale l'agire dell'Autorità.

6. Protezione dati e sovranità digitale

La contrapposizione, spesso insistita nel dibattito politico, tra protezione dati e interessi generali di varia natura rischia di oscurare, molto più spesso di quanto si creda, virtuose sinergie.

E' questo il caso della cybersecurity, il cui rapporto con la privacy è tutt'altro che antagonista, come abbiamo dimostrato con la proficua e consolidata collaborazione con il Copasir e con il Dis.

Questo, perché la sicurezza dello spazio cibernetico implica anzitutto, inevitabilmente, la protezione dei dati e delle infrastrutture di cui è composto l'ecosistema digitale con i suoi vari snodi.

E' la questione che abbiamo posto spesso in sede europea, da ultimo rispetto al social network Tik Tok, promuovendo accertamenti in ordine alle garanzie di sicurezza offerte, anche e soprattutto con riferimento ai dati degli utenti minorenni.

Su temi come questi, che toccano profondamente tanto la sicurezza collettiva quanto quella individuale, l'Europa deve infatti saper parlare con una voce sola, riflettendo quell'ambizione, insieme unificante e identitaria sottesa al Regolamento.

La fragilità strutturale e la scarsa consapevolezza dei potenziali bersagli di attività massive di *malware* acuisce, poi, la gravità degli attacchi, già rafforzata dal ricorso ad insidiose tecniche di intelligenza artificiale.

Gli attacchi sono ulteriormente cresciuti nello scorso anno: persino del 91,5% nel settore dei servizi on line e del cloud.

Gli atti di spionaggio/sabotaggio sono triplicati, in misura percentuale, rispetto allo scorso anno.

La pandemia ha ulteriormente acuito questo fenomeno rivoltosi, addirittura, ai danni di strutture sanitarie di eccellenza anche italiane, al punto che si è proposto di qualificare tali atti come propriamente terroristici.

Del resto, in un contesto in cui ciascun oggetto di uso quotidiano (si pensi agli assistenti vocali!) può rappresentare il canale d'ingresso di potenziali attacchi informatici, è indispensabile fare della protezione dei dati, dei sistemi e delle infrastrutture un obiettivo prioritario delle politiche pubbliche.

La crescente complessità dei sistemi genera, infatti, vulnerabilità sfruttate per paralizzare reti di servizi pubblici essenziali e canali di comunicazione di

primaria importanza, con un impatto, dunque, concretissimo sulla vita pubblica.

Sono ancora troppi e troppo importanti i sistemi informativi, soprattutto pubblici, caratterizzati da vulnerabilità suscettibili di pregiudicare tanto la sicurezza nazionale quanto la dignità dei soggetti i cui dati siano divulgati.

Il *data breach* dell'Inps, che ha determinato l'esfiltrazione di dati rivelatori anche di condizioni di fragilità economica è, in questo senso, significativo. Esso dimostra, peraltro, l'importanza della rigorosa osservanza delle regole di protezione dati, a fini tanto preventivi quanto remediali, se non altro per circoscrivere gli effetti delle violazioni, come è apparso evidente rispetto alle 1.443 notifiche di violazione dei dati personali ricevute dal Garante nel 2019, da parte di soggetti pubblici e privati.

Esse hanno riguardato tentativi di acquisizione di dati personali (credenziali di accesso, dati di contatto o relativi a strumenti di pagamento), accesso abusivo a mail e pec, perdita di dati per effetto di *ransomware* ecc..

Le implicazioni, in termini di sicurezza nazionale, di alcuni *data breach* dimostrano anche come la stretta dipendenza della sicurezza della rete da chi ne gestisca i vari snodi e "canali" induca a ripensare il concetto di sovranità digitale.

E di fronte alla delocalizzazione in *cloud* di attività rilevantissime chiediamo al Parlamento e al Governo se non si debba investire in un'infrastruttura *cloud* pubblica, con stringenti requisiti di protezione, per riversarvi con adeguata sicurezza dati di tale importanza.

In un contesto in cui le tecnologie ICT sono divenute - sempre più chiaramente con la pandemia - la principale infrastruttura di ciascun Paese, assicurarne una regolazione sostenibile e adeguata, tale da garantire sicurezza, indipendenza dai poteri privati, soggezione alla giurisdizione interna, diviene un obiettivo non più eludibile.

7. Giustizia, tecnologia, dignità

Le esigenze di giustizia e la privacy dei cittadini sono i fuochi dell'ellisse su cui si sviluppa una dinamica essenziale per la democrazia, resa inevitabilmente più complessa dalle potenzialità delle nuove tecnologie.

Uno dei campi in cui questa tensione si manifesta con maggiore urgenza è quello delle intercettazioni, rispetto alla quale, sin dalla prima fase dell'esame della riforma "Orlando", abbiamo sollecitato l'esigenza di una più puntuale selezione del materiale investigativo assicurando, nel rispetto dei diritti della difesa, che negli atti processuali non siano riportati interi spaccati di vita privata estranei al tema di prova, bilanciando privacy ed esigenze di giustizia.

Le misure, previste dalla riforma del 2017, volte a limitare la circolazione endoprocessuale delle intercettazioni eccedenti le esigenze investigative hanno segnato un'importante innovazione, che - come abbiamo rappresentato in Parlamento - è bene conservare, anche con la nuova disciplina, almeno come obbiettivo, pur modulando diversamente gli oneri di polizia giudiziaria e pubblico ministero in questa fase.

La derubricazione del divieto di trascrizione in dovere di vigilanza dell'organo requirente gli impone dunque, per non vanificare la portata innovativa della riforma, un vaglio attento sull'effettivo rispetto di questo canone di minimizzazione.

Per quanto invece concerne le intercettazioni mediante captatori, sarebbe stato opportuno cogliere l'occasione del decreto-legge per colmare le lacune normative già da noi rilevate rispetto alla riforma Orlando e ribadite con la segnalazione sul caso Exodus.

Le straordinarie potenzialità intrusive di tali strumenti impongono - come è emerso per altri versi nelle scorse settimane - garanzie adeguate per impedire che essi, da preziosi ausilii degli inquirenti, degenerino in mezzi di sorveglianza massiva o, per converso, in fattori di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio, rendendolo estremamente permeabile se allo-

cato in server non sicuri o, peggio, delocalizzati anche al di fuori dei confini nazionali.

Più in generale, abbiamo auspicato un supplemento di riflessione in ordine alla progressiva estensione dell'ambito applicativo del *trojan*, che dovrebbe invece restare circoscritto.

E' significativo che la Corte costituzionale tedesca abbia censurato la disciplina di tale tipo d'intercettazioni (sia pure preventive), per violazione non solo della riserva di giurisdizione ma anche del principio di proporzionalità.

Va infatti sottolineata l'intrinseca diversità, rispetto alle intercettazioni tradizionali, di quelle mediante captatori, propria della loro capacità invasiva e dell'attitudine a esercitare una sorveglianza ubiquitaria, con il rischio peraltro di rendere più difficile il controllo ex post sulle operazioni compiute sul dispositivo-ospite. Di qui l'esigenza di un rigoroso rispetto del principio di proporzionalità, a tutela del "generale diritto alla libertà del cittadino nei confronti dello Stato".

Questo dev'essere il parametro essenziale da osservare nella disciplina di strumenti investigativi che devono poter garantire tanto la sicurezza quanto la libertà, secondo la sinergia che richiedono la normativa costituzionale e sovranazionale.

In questo senso, è indifferibile una revisione organica della disciplina della conservazione dei dati di traffico, i cui termini - sei anni - appaiono difficilmente compatibili con la necessaria proporzionalità delle limitazioni della privacy rispetto alle esigenze investigative, posta dalla Corte di giustizia a fondamento della declaratoria di illegittimità della direttiva 2006/24/CE (basata su un termine massimo di due anni).

8. Il pendio scivoloso

Analoga proporzionalità deve caratterizzare il ricorso alle straordinarie potenzialità dell'intelligenza artificiale, tra le quali quelle connesse al riconosci-

mento facciale, che può essere o meno compatibile con i diritti fondamentali in ragione dei limiti cui soggiaccia, commisurati appunto ai rischi implicati.

A tali fini, è determinante la cognizione reale delle implicazioni di ordine individuale, sociale, persino etico della tecnologia considerata.

Per questo, avevamo guardato con favore alla proposta europea di moratoria sul riconoscimento facciale, ritenendola una lungimirante affermazione dei principi di precauzione e prevenzione, anche considerando la varietà di usi ai quali tale tecnica può prestarsi.

Se infatti, in alcuni ambiti il ricorso a tali sistemi, circoscritto e assistito da garanzie adeguate, può fornire un contributo difficilmente conseguibile altrimenti, in altri contesti esso può invece risolversi in un'ingiustificata (perché, appunto, sproporzionata) limitazione dei diritti individuali.

Il ricorso diffuso a queste tecniche in circostanze "ordinarie" e a meri fini agevolatori, rischia peraltro di indurre a sottovalutarne l'invasività: il pericolo è quello del "pendio scivoloso", fino all'acritica accettazione sociale della progressiva perdita di libertà.

E questo, tanto più in ragione dei limiti che il consenso incontra rispetto alla biometria cosiddetta facilitativa, di cui spesso si ignorano le implicazioni: dalla ubiquitaria geolocalizzazione alla sempre più penetrante profilazione.

Il tutto, in un contesto di generale asimmetria informativa tra soggetto passivo e attivo della raccolta dei dati, in cui le tradizionali diseguaglianze rischiano di ripresentarsi in forma tanto più incisiva quanto più sottile.

Sarà dunque determinante, in questo senso, il rispetto dei principi di necessità e proporzionalità nel ricorso a tali misure: criteri essenziali su cui le Corti europee hanno sinora fondato un rapporto armonico tra libertà, tecnologia e sicurezza.

E saranno importanti le scelte regolatorie che dovessero, eventualmente, legittimare l'uso del riconoscimento facciale a fini di polizia. La previsione normativa consente infatti di stabilire garanzie e limiti uniformi su tutto il territorio nazionale, come abbiamo avuto modo di sottolineare rispetto ad alcune iniziative

di enti locali, secondo uno schema destinato a riproporsi in assenza di una cornice regolatoria unitaria.

9. Il più universale dei diritti

Uno degli ambiti in cui il diritto alla protezione dati ha dimostrato di svolgere un essenziale ruolo arbitrale tra diritti fondamentali è quello dell'amplificazione dei contenuti informativi determinata dalla rete.

La giurisprudenza interna, quella della Corte di giustizia e la nostra prassi hanno contribuito a regolare un contesto, quale in particolare quello del diritto all'oblio, in cui più evidenti appaiono le vicendevoli implicazioni tra tecnica e diritto: come la prima muti lessico e semantica del secondo e come questo imponga, alla prima, soluzioni inedite a nuove tensioni.

Che, in quest'ambito, riguardano il mutamento del rapporto tra storia e biografia, giudizio pubblico e soggettività, determinato dalla capacità della rete di attribuire a ciascuno nuove identità, spesso insensibili al trascorre del tempo, ma tali da recare grave pregiudizio all'interessato. Lo dimostra il numero di istanze rivolteci anche quest'anno, che rappresentano una quota significativa delle 8.092 cui abbiamo fornito riscontro. Anche per questo abbiamo ritenuto, in alcuni casi, di accordare tutela rispetto ai profili stilati utilizzando chiavi di ricerca integrative o diverse rispetto al nome se idonee a meglio identificare, sia pur indirettamente, l'interessato.

Il profilo della persona, stilato dal motore di ricerca organizzando le notizie indicizzate - come ha sottolineato anche la Corte di giustizia - deve del resto rifletterne la condizione (anche giudiziaria) attuale.

La notizia dell'assoluzione non deve, ad esempio, essere posta in coda a una pluralità di link più risalenti, relativi all'imputazione, alle misure cautelari, persino alla condanna non definitiva.

Dev'essere, insomma, il criterio dell'esattezza e dell'aggiornamento - e non

quello del numero dei *click* - a governare l'algoritmo dei motori di ricerca i quali, titolari di un ruolo sempre più centrale rispetto all'informazione in rete, non possono affidare al solo procedimento informatico decisioni così rilevanti sui diritti fondamentali.

Significativo, in tal senso, il nostro orientamento con cui abbiamo ritenuto meritevole di deindicizzazione notizie di condanne non aggiornate al percorso, spesso complesso, successivamente compiuto dal soggetto, nel frattempo riabilitato.

La nostra prassi, così come la giurisprudenza europea e interna, mira così a responsabilizzare ulteriormente le piattaforme rispetto ad attività che hanno un impatto determinante sui diritti fondamentali, utilizzando anche la tecnica come soluzione di molte contraddizioni da essa stessa ingenerate.

E questa funzione "libertaria" della tecnica sembra, del resto, promossa da un'ulteriore sentenza della Corte di giustizia che, poche settimane dopo la pronuncia appena descritta, ha ammesso che i giudici possano - con "un'ingiunzione dinamica" - ordinare la rimozione di contenuti equivalenti a quelli già dichiarati illeciti, con effetto esteso anche a livello globale.

Tutelare la dignità limitatamente a una porzione di contenuti visibili solo su scala nazionale, infatti, sarebbe meramente velleitario in un contesto, quale quello della rete, che ha superato l'idea della frontiera.

La Corte sembra consapevole di come il diritto alla protezione dati - il più transnazionale dei diritti, in quanto si esercita su di uno spazio, quale quello digitale, che non conosce confini - necessiti di una tutela altrettanto sovranazionale ed aspiri a un riconoscimento universalistico che sembra ormai sempre più urgente.

Anche con la sentenza Google-Cnil, pur negando la sussistenza di un obbligo di deindicizzazione globale secondo la disciplina di protezione dati, la Corte ha infatti ammesso la possibilità di accordare, in ragione delle peculiarità del caso concreto, anche tale forma di tutela espansiva.

10. Tecnologie "ribelli"

In assenza di garanzie realmente uniformi a livello globale, infatti, la rete continuerà a riproporre al suo interno enclave anomiche in cui possano agire indisturbati quanti intendano sfruttare le straordinarie potenzialità del digitale per violare diritti, anziché promuoverli.

E' il problema che, ad esempio, rispetto alle fake news abbiamo discusso in sede di audizione alla Camera e su cui abbiamo istituito un tavolo di lavoro con l'Agcom.

Ma è un profilo che - ricondotto al tema più generale dell'uso distorsivo e spesso anche ritorsivo della rete (si pensi al *revenge porn*) - sollecita una riflessione avulsa da pregiudizi.

La tendenziale eliminazione, nel mondo della rete, della distinzione tra produttori e destinatari dell'informazione ha avuto, da un lato, lo straordinario pregio di espandere le possibilità di libera manifestazione del pensiero e di accesso all'informazione, da parte anche delle fasce più marginali della popolazione.

Dall'altro lato, tuttavia, ha amplificato la diffusione di notizie false e spesso diffamatorie, per la maggiore capacità aggregativa che hanno - nell'età della rabbia e della disintermediazione - i contenuti offensivi, capaci di polarizzare consensi nella lotta all'altro-da-sé.

L'autismo informativo e l'effetto "ecocamera digitale" finiscono così per produrre non già informazione ma "auto-comunicazione di massa", anche grazie alla non neutralità dell'indicizzazione e della gerarchia algoritmica. Nel conferire maggiore o minore visibilità ai contenuti, infatti, queste tecniche incidono in maniera significativa sul diritto d'informazione, con il rischio di una censura privata o comunque di una selezione informativa che non risponda più a valori socialmente condivisi, ma a un'insindacabile legge del mercato.

Le piattaforme sono oligopoliste non tanto e non solo perché detengono un potere economico rilevantissimo, quanto perché dispongono della principale

infrastruttura sociale: prima ancora di conquistare il mercato, orientano il pensiero sfruttando la potenza dei dati.

Di qui la pluralità di funzioni della protezione dati che, governando le condizioni per il legittimo uso dei dati personali, rafforza le tutele consumeristiche, regola l'esercizio del potere informativo e tutela intangibili spazi di autodeterminazione individuale, rispetto al *"nudging"* praticato a fini commerciali, ideologici, persino politici.

E quanto più si fa spazio sociale e politico, tanto più la rete deve poter garantire le sue caratteristiche di democraticità, universalità, apertura e libertà nell'accesso, che ne hanno consentito l'affermazione come il più grande spazio pubblico conosciuto dall'umanità.

La rilevanza dei poteri privati è, in tale contesto, un tema da affrontare assieme a quello della regolazione del digitale, favorendo sì la responsabilizzazione dei gestori, ma riservando la decisione sui diritti fondamentali, in ultima istanza, all'autorità pubblica, secondo il modello che la protezione dati ha offerto sul terreno dell'oblio o del cyberbullismo.

Si dovrebbe allora, forse, riflettere sulla regolazione dell'uso dell'anonimato, rendendolo realmente reversibile. Ma, pur al netto delle criticità da cui non sarebbe scevra alcuna soluzione in tal senso, anch'essa sarebbe del tutto velleitaria in assenza di uniformità, sul piano internazionale, di una tale disciplina, che, bilanciando libertà di espressione e dignità, dovrebbe rendere effettiva la tutela delle vittime di illeciti on-line.

Quell'unificazione normativa che l'Europa ha voluto promuovere - non senza un investimento identitario importante - sulla protezione dati, quale necessario presupposto di ogni regolazione possibile del digitale, dovrebbe essere quindi, oggi, un obiettivo condiviso della comunità internazionale.

E parallelamente alla cogenza e alla forza, anche simbolica, della norma, dovrebbe promuoversi una tecnologia 'ribelle' alle prevaricazioni e alle discriminazioni (per dirla con Morozov), con funzione cioè ausiliaria del progresso sociale.

In questo senso, andrebbe percorsa la strada di soluzioni tecniche volte a segnalare all'utente, in base a criteri oggettivi contenuti potenzialmente inaffidabili stimolando anche, così, il senso critico del pubblico.

Utilizzare la tecnica in funzione di promozione, anziché di limitazione, dei diritti può essere, in questo senso, una delle soluzioni migliori per contribuire a rendere la rete quello straordinario strumento pluralista che doveva e deve essere, promuovendone la sostenibilità.

11. Cronaca, storia, orizzonti

Questa è la direzione rispetto alla quale la protezione dati ha dimostrato di poter fornire un contributo essenziale, per una declinazione in chiave democratica del digitale, secondo l'auspicio già espresso da Stefano Rodotà e Giovanni Buttarelli, la cui mancanza sempre avvertiamo.

Perseguire quest'obbiettivo contribuirà a consolidare quel particolare profilo identitario che l'Europa sta progressivamente affermando sul terreno del rapporto tra diritto e tecnica, tentando di rimodularlo in chiave antropocentrica, perché il "destino dell'Occidente" non contraddica, con la cronaca, la propria storia.

E in quest'affermazione identitaria di "umanesimo digitale", la protezione dati assume una sempre più insostituibile funzione di salvaguardia dello Stato di diritto, di fronte alle continue tensioni imposte dalla sinergia di tecnica, potere e persino emergenza, essendo strumento di governo non solo dell'identità individuale, ma anche dell'umanità rispetto alla potenza di calcolo.

Questa disciplina, con la sua vocazione unitaria, ha così rappresentato il più organico tentativo di regolazione delle nuove tecnologie: una vera e propria Costituzione per il digitale, che un numero sempre crescente di ordinamenti ha assunto a modello.

Ma la sfida sarà vinta solo se e quando la protezione dei dati diverrà, fino in

fondo, cultura e sentire diffuso di tutti. Che, come tale, deve essere affidata non alla deterrenza o alla repressione sanzionatoria ma alla consapevolezza di come la sostenibilità del futuro dipenda, in larga parte, dalla tutela che sapremo accordare ai frammenti del nostro io e del nostro vissuto.

Questo è l'orizzonte che, con il Collegio che ho avuto l'onore di presiedere, riteniamo di indicare a chi avrà la responsabilità e il privilegio di guidare un'Autorità, come questa, sempre più centrale per la vita democratica del Paese e sempre più vicina alle persone.

Signor Presidente, la nostra attività è stata prorogata oltre ogni ragionevole misura.

L'invito che, con rispetto, attraverso la Sua persona, rivolgo al Parlamento è quello di procedere quanto prima all'elezione dei nuovi componenti.

Per concludere, consentitemi di rivolgere un sincero ringraziamento al Segretario generale e a tutti coloro che, nell'Ufficio, ogni giorno si impegnano con generosità e competenza per rispondere alla crescente domanda di tutela dei cittadini.

E ringrazio, ancora una volta, le Colleghe Augusta Iannini, Giovanna Bianchi Clerici, Licia Califano, componenti il Collegio del Garante: insieme abbiamo condiviso un lungo mandato e una preziosa amicizia.

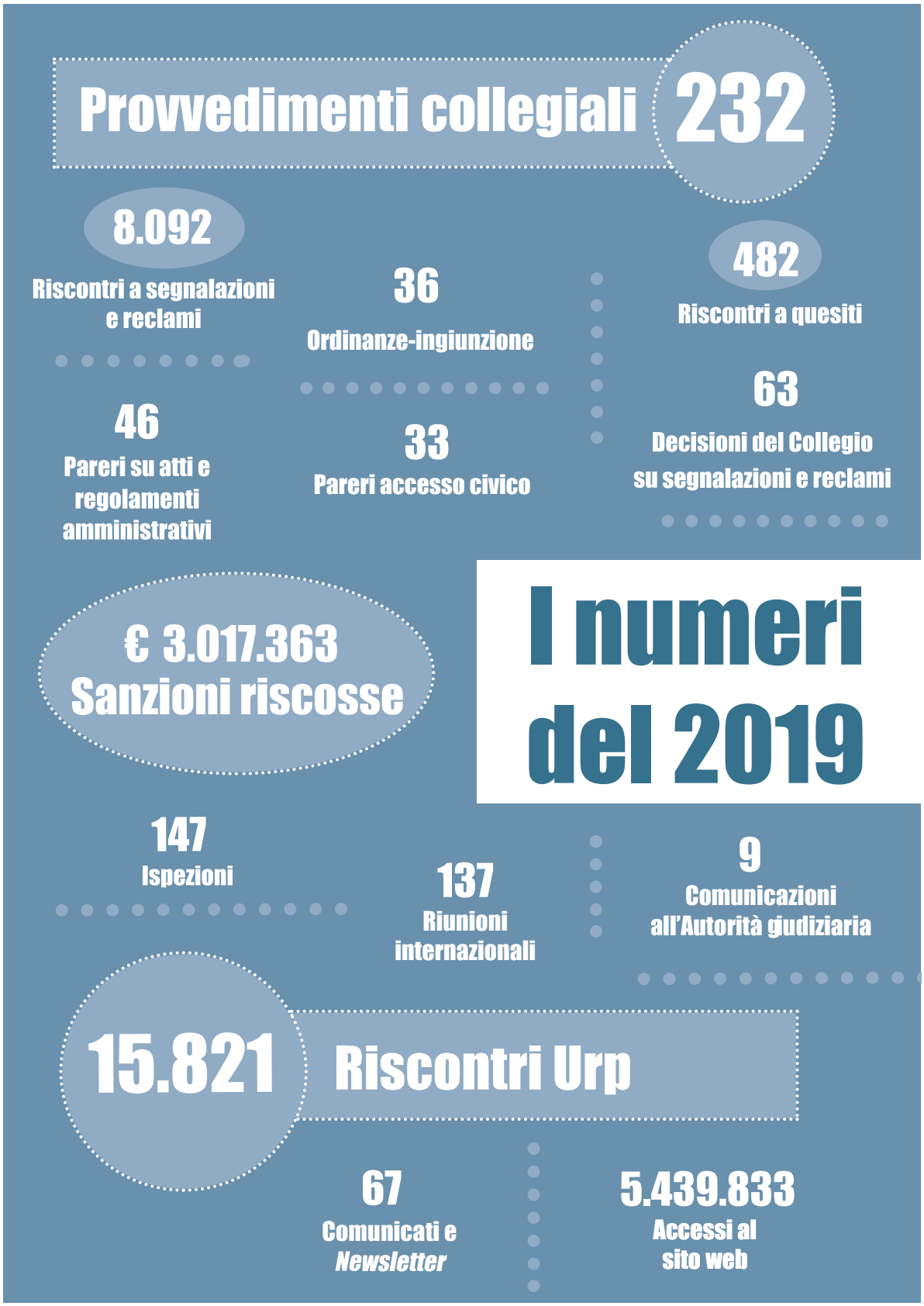
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione2019

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza Venezia, 11
00187 Roma
tel. 06 696771
email: protocollo@gpdp.it
www.garanteprivacy.it


Provvedimenti collegiali 232
8.092
Riscontri a segnalazioni e reclami
36
Ordinanze-ingiunzione
482
Riscontri a quesiti
46
Pareri su atti e regolamenti amministrativi
33
Pareri accesso civico
63
Decisioni del Collegio su segnalazioni e reclami
I numeri del 2019
€ 3.017.363
Sanzioni riscosse
147
Ispezioni
137
Riunioni internazionali
9
Comunicazioni all'Autorità giudiziaria
15.821
Riscontri Urp
67
Comunicati e Newsletter
5.439.833
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

Avvertenza ed elenco delle abbreviazioni e degli acronimi più ricorrenti

La presente Relazione è riferita al 2019 e contiene talune notizie già anticipate nella precedente edizione nonché informazioni relative agli sviluppi più recenti che si è ritenuto opportuno menzionare.

Arera	Autorità di regolazione per energia reti e ambiente
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
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	Carta europea dei diritti dell'uomo
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)
Cepd	Comitato europeo per la protezione dei dati
cons.	considerando
Consob	Commissione nazionale per le società e la borsa
Corte EDU	Corte europea dei diritti dell'uomo
Cost.	Costituzione
d.d.l.	disegno di legge
d.l.	decreto-legge
d.lgs.	decreto legislativo
d.m.	decreto ministeriale

d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica
doc.	documento
es.	esempio
Fse	Fascicolo sanitario elettronico
Gepd	Garante europeo per la protezione dei dati
G.U.	Gazzetta ufficiale della Repubblica italiana
GUUE	Gazzetta ufficiale dell'Unione europea
Gruppo Art. 29	Gruppo dei garanti europei istituto dall'art. 29 della direttiva 95/46/CE
IMI	*Internal Market Information System*
Ivass	Istituto per la vigilanza sulle assicurazioni
IWGDPT	*International Working Group on Data Protection in Telecommunications*
l.	legge
lett.	lettera
Mef	Ministero dell'economia e delle finanze
Mise	Ministero dello sviluppo economico
Miur	Ministero dell'istruzione dell'università e della ricerca
n.	numero
p.	pagina
p.a.	pubblica amministrazione
par.	paragrafo
Pec	posta elettronica certificata
provv.	provvedimento del Garante
r.d.	regio decreto
reg.	regolamento
RGPD	Regolamento (UE) 679/2016
Rdc	Reddito di cittadinanza
Rpd	Responsabile della protezione dei dati
Rpo	Registro pubblico delle opposizioni
sez.	sezione
Spid	Sistema pubblico dell'identità digitale
Ssn	Servizio sanitario nazionale
tab.	tabella
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

PAGINA BIANCA

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

PAGINA BIANCA

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

1 Introduzione Foreword

1.1. *Tra continuità e innovazione:* con questo slogan può essere riassunta l'attività svolta dall'Autorità nell'anno trascorso. Se, come è noto, dal 25 maggio 2018 il Regolamento generale sulla protezione dei dati (RGPD) ha trovato applicazione, il 2019 si è rilevato essere, per tutti gli attori, un anno di sperimentazione e di progressivo assestamento. Tale constatazione vale anche per il Garante che, inalterato nella composizione del Collegio per l'effetto di reiterati interventi legislativi, da ultimo correlati anche alla sopravvenuta emergenza sanitaria (cfr. par. 2.2, n. 1), ha operato su più livelli.

Anzitutto, privilegiando la collettività e la variegata platea di destinatari della disciplina di protezione dei dati cui sono state fornite rassicurazioni, circa le (prevalenti) linee di continuità tra il previgente regime normativo – frutto del recepimento della direttiva 95/46 – e quello introdotto a seguito del RGPD, e chiarimenti (con le più varie modalità) sugli aspetti innovativi della disciplina.

Dando seguito alle sollecitazioni provenienti da singoli e associazioni di categoria, l'Autorità ha infatti evidenziato la persistente attualità (di larga parte) delle decisioni adottate in passato. Si pensi agli orientamenti consolidati, spesso condensati in linee guida e

1.1. *Between continuity and innovation*: this slogan could sum up the activities of the Italian supervisory authority in the past year. As we all know, the General Data Protection Regulation (GDPR) has been in application since 25 May 2018; the year 2019 proved to be, for all stakeholders, a time of testing and stepwise adjustments. This also applies to the Garante: indeed, whilst the members of its collegiate panel remained in office on account of subsequent regulatory measures, which were of late also grounded in the supervening health emergency (see paragraph 2.2, No 1), the Authority as a whole worked on several levels. In the first place, the activities focused on the general public and the multifarious stakeholders impacted by personal data protection legislation, who were reassured as to the (mainly) seamless transition from the previous legal framework – based on transposition of Directive 95/46 – to the new one created by the GDPR; clarifications were provided via the most diverse channels on the innovations brought about by the EU instrument.

Following up on the requests made by individual entities and trade associations, the Garante highlighted the continued validity of a considerable portion of the decisions and measures

1

provvedimenti generali (messi alla prova ormai da una lunga esperienza applicativa), in materia bancaria (par. 14.2), come a quelli dedicati alla navigazione in internet e all'uso della posta elettronica in ambito lavorativo o alla videosorveglianza (par. 14.4) o, pure, nella materia condominiale (par. 15): come è facile intendere, si tratta di ambiti di largo impatto sulla pratica applicazione della disciplina di protezione dei dati personali nella quotidianità della vita della popolazione e sulla normale operatività di imprese e pubbliche amministrazioni. E, ancora, si sono ribaditi i criteri distintivi da tempo individuati tra il diritto di accesso ai dati personali e le altre ipotesi di accesso documentale presenti nell'ordinamento, ad esempio in ambito bancario e assicurativo, e a quest'ultimo riguardo soprattutto in relazione all'accesso ai dati personali contenuti nelle perizie medico-legali (ed ai suoi limiti), con particolare riferimento alle informazioni di tipo valutativo-soggettivo e/o ai giudizi ivi contenuti (cfr. par. 14.2); come pure sono stati ricordati i principi applicabili al trattamento dei dati personali effettuato in occasione delle operazioni di adeguata verifica della clientela prescritte dalla normativa vigente in materia di antiriciclaggio o, ancora, in occasione dell'esecuzione di servizi di consulenza effettuati da istituti di credito e imprese di investimento, per valutare l'adeguatezza e l'appropriatezza delle operazioni o dei servizi offerti alla clientela (cfr. par. 14.2).

Chiarimenti sono stati altresì forniti rispetto alle innovazioni che hanno riguardato il tema della limitazione nell'esercizio dei diritti dopo le modifiche al Codice (par. 13.7), la materia del trattamento dei dati sanitari (par. 5.4) o, nel contesto lavorativo, in merito ai compiti e alle responsabilità dei professionisti che effettuano trattamenti di dati personali su incarico del datore di lavoro (par. 13.6) come pure in relazione ai trattamenti posti in essere dal medico competente (par. 13.14).

adopted in the past years. This is the case, for instance, of benchmark indications provided by the Garante in several areas – often by way of guidelines and general application measures that have been put to test successfully in many respects – including banks (paragraph 1.4.2), use of the Internet and email at the workplace (paragraph 14.4), and even the management of condominiums (paragraph 15). It can easily be grasped that these are issues impacting substantially the implementation of personal data protection legislation in daily life as well as the standard operation of businesses and public administrative bodies. From this perspective, the criteria for distinguishing the right to access personal data from other types of access envisaged in our legal system were reaffirmed – for instance, regarding banks and insurance companies; as for the latter, the focus was placed especially on access to the personal data contained in forensic medicine reports and the relevant limitations, with particular regard to subjective evaluations and judgments as contained in those reports (paragraph 14.2). The Authority also recalled the principles applying to the processing of personal data in connection with due diligence procedures as required by the applicable anti-money laundering laws, or in the course of advisory services provided by banks and investment companies in order to assess adequacy and appropriateness of operations or services to customers (paragraph 14.2).

Clarifications were also provided regarding the innovations brought about by the amendments made to the Code (paragraph 13.7) in terms of limitations on the exercise of data subjects' rights, processing of data concerning health (paragraph 5.2), or the employment sector – such as the duties and responsibilities falling to professionals that process personal data on the employer's behalf (paragraph 13.6) or the processing activities carried out by appointed doctors (paragraph 13.14).

1.2. In quest'opera di divulgazione, che costituisce dalle origini uno dei tratti caratteristici dell'azione delle autorità di protezione dei dati personali, tutte le forme e i canali di comunicazione istituzionale sono stati valorizzati: è stata assicurata la (consueta) interlocuzione, che si caratterizza per l'immediatezza del riscontro, tramite l'Urp dell'Autorità (cfr. par. 23.5 e, per utili indicatori numerici, parte IV, tab. 12); l'attività di comunicazione ha altresì continuato a giovarsi dei prodotti informativi e multimediali realizzati dall'Ufficio oltre che del costante aggiornamento del sito web istituzionale (cap. 23 e parte IV, tab. 2). Il RGPD ha poi costituito l'occasione, nell'ambito di due progetti finanziati dall'UE (T4DATA e SMEDATA), per privilegiare l'interlocuzione con i Responsabili per la protezione dei dati (par. 21.5), figura sulla quale il legislatore dell'Unione europea fa affidamento (e così pure le autorità di controllo: cfr. par. 4.9 e 5.4.3) per incrementare l'effettività della disciplina di protezione dei dati; approfondimenti e temi di frontiera sono stati curati dal Garante e hanno visto l'attiva partecipazione dei suoi Componenti in occasione di numerose manifestazioni e conferenze (parr. 21.4 e 23.4).

1.3. Ma è nella collaborazione istituzionale che la funzione "consulenziale" del Garante assume particolare rilievo, ora incrementato in ragione dell'obbligo, introdotto dall'art. 36, par. 4, del RGPD, di consultazione dell'autorità di controllo anche nell'*iter* che conduce all'adozione di normative di rango primario suscettibili di interferire sul diritto alla protezione dei dati personali (oltre che, come già in passato, rispetto alle discipline di natura regolamentare e agli atti amministrativi di carattere generale). Nell'assolvimento di questo compito, numerose sono state le aree ed i soggetti con i quali si è instaurata (o è continuata) una feconda collaborazione istituzionale: rinviando allo svolgimento della Relazione per una compiuta map-

1.2 These dissemination activities, which have featured from the start among the key tasks of data protection authorities, have been implemented by relying on all methods and channels for official communication. Thus, the Authority's front office continued to provide upfront information and replies (see paragraph 23.5 and the helpful breakdown of the workload in Table 12 of Part IV), whilst communication activities were implemented like in the past via the information and multi-media products developed by the Office and through the continuously updated website (Chapter 23 and Table 2 of Part IV). The GDPR provided an opportunity to shed special light on the interactions with data protection officers as part of two EU-funded projects (T4DATA and SMEDATA) (paragraph 21.15), DPOs being key pillars to foster the effectiveness of data protection legislation both in the view of the EU legislator and from the perspective of supervisory authorities (see paragraphs 4.9 and 5.4.3). In-depth analyses and leading-edge issues were addressed as well including via the contributions given by the members of the collegiate panel participating in several conferences and events (paragraphs 21.4 and 23.4).

1.3 However, it is in the collaboration with other institutions where the 'advisory' role played by the Garante took on special importance, following the obligation to consult with the Authority (introduced by Article 36(4) of the GDPR) as part of the process leading to the enactment of primary legislation - if such legislation is liable to impact personal data protection rights – on top of the consultation relating, like in the past, to all types of secondary legislation. In discharging this task, the Garante set up or continued fruitful institutional relations in many areas and respects. Further details can be found in the text of the Annual Report, including the list of the opinions

1

patura dei pareri resi (v., in prima battuta, par. 3.1 e, nella parte IV, tab. 3-5), basti qui richiamare i frequenti contatti con il Ministero della salute, con riguardo alle regole di funzionamento di delicati sistemi informativi (quali il Sistema informativo trapianti, il Registro nazionale dei donatori di cellule riproduttive a scopi di procreazione medicalmente assistita di tipo eterologo, il Sistema di segnalazione delle malattie infettive), come pure in relazione all'implementazione del Fascicolo sanitario elettronico (par. 5.2) o, ancora, alle questioni connesse alla materia delle disposizioni anticipate di trattamento (par. 5.3). Non diversamente, l'attuazione del cd. Isee precompilato ed i complessi trattamenti che costituiscono le basi di fondazione del reddito di cittadinanza hanno richiesto una serrata collaborazione con il Ministero del lavoro e delle politiche sociali (par. 4.2); frequenti e positive le interazioni con le Agenzie fiscali per i delicati trattamenti effettuati negli ambiti di competenza, come avvenuto per la "lotteria dei corrispettivi" (par. 4.1.5). Di qui l'intensa produzione di pareri nel corso dell'anno nell'ambito delle materie più varie e l'interlocuzione del Garante in sede parlamentare (cfr. par. 3.1.4).

E se, con soddisfazione, va registrata un'ampia disponibilità a tenere in considerazione le valutazioni dell'Autorità e a raccoglierne i suggerimenti, sovente già all'esito di una proficua attività preparatoria nei vari tavoli di lavoro, talvolta le indicazioni fornite sono rimaste senza seguito, anche quando riferite ad aspetti fondativi della disciplina di protezione dei dati, quali il necessario rispetto del principio di proporzionalità e l'imperativo normativo sotteso al principio di minimizzazione nel trattamento dei dati personali e nella configurazione dei sistemi informativi (sempre più complessi e interconnessi, come pure si desume da queste prime note). In alcune occasioni, infatti, questi principi sono stati trascurati: si pensi al caso della memorizzazione prolungata (almeno fino al 31

rendered (see paragraph 3.1 and Tables 3-5 in Part IV). Here reference can be made to the frequent interactions with the Ministry of Health regarding the operating arrangements of highly sensitive information systems such as the Transplantation Registry, the National Registry of reproductive cells donors for medically assisted heterologous reproduction, and the Infectious diseases alerting system; the implementation of the electronic health record (paragraph 5.2); or the issues concerning the so-called 'living will' (paragraph 5.3). By the same token, implementation of the so-called pre-compiled ISEE (Equivalent Economic Situation Indication) declaration as required from candidate beneficiaries of economic aid and the complex processing operations underlying functioning of the national basic income scheme required continued cooperation with the Ministry of Labour and Welfare (paragraph 4.2). Frequent as well as fruitful interactions were held with the Revenue Agency with regard to the complex processing operations in the relevant sectors – see, in particular, those related to the so-called 'receipt lottery' (paragraph 4.1.5). This accounts for the substantial number of opinions issued in the past year concerning the most diverse areas as well as for the frequent contacts between the Garante and Parliament (paragraph 3.1.4).

Unquestionably, one has reason to be satisfied in view of the account taken of the Authority's positions and suggestions, which were taken up to a considerable extent also during the preparatory activities carried out most usefully in the various working groups; still, the guidance provided by the Garante was sometimes overlooked even when focused on key components of data protection legislation – including the need to respect the proportionality principle and the statutory obligation to minimize personal data in processing activities as well as in configuring increasingly complex and networked IT systems. These

dicembre dell'ottavo anno successivo a quello di presentazione della dichiarazione di riferimento) dei dati personali riportati nelle fatture elettroniche recanti altresì natura, qualità e quantità dei beni e servizi oggetto dell'operazione, con un'estensione delle finalità di utilizzazione dei dati di fatturazione per tutte le funzioni di polizia economica-finanziaria demandate al Corpo della Guardia di finanza (par. 4.1.7); così pure possono ricordarsi le riserve manifestate in relazione al trattamento di dati biometrici unitamente a sistemi di videosorveglianza per finalità di rilevazione delle presenze dei dipendenti pubblici (par. 13.12).

1.4. Una non meno onerosa attività "consulenziale" emerge poi dall'analisi della minuta casistica oggetto dei numerosi pareri (illustrati al par. 4.5) resi dal Garante su sollecitazione dei Responsabili della prevenzione della corruzione e della trasparenza e dei Difensori civici rispetto alla materia dell'accesso civico. Essa fa da contrappunto al tema sovraordinato del rapporto (ancora in tensione) tra le legittime esigenze di trasparenza amministrativa e il rispetto del diritto alla protezione dei dati personali, che nel 2019 ha trovato uno dei suoi punti di emersione più rilevanti nella dichiarazione di illegittimità costituzionale dell'art. 14, comma 1-*bis*, d.lgs. 14 marzo 2013, n. 33, ad opera della sentenza del 21 febbraio, n. 20 (cfr. già Relazione 2018, par. 1 e *infra* par. 20.3), rispetto alla quale va registrata la "risposta" (in qualche misura interlocutoria) fornita dal legislatore con il decreto-legge 30 dicembre 2019, n. 162 (cd. Milleproroghe) e destinata a trovare compiuto svolgimento con un apposito regolamento governativo.

1.5. Se, come si è accennato, il RGPD non ha portato a bruschi cambi di rotta o a salti nel buio, tuttavia la disciplina di adeguamento dell'ordinamento nazionale contenuta nel decreto legislativo n. 101/2018 ha posto in capo

principles were actually left out in certain cases. Reference can be made to the extended retention period (until at least the 31st of December of the eighth year following submission of the relevant income report) set out for the personal data contained in electronic bills, which also include information on nature, type and amount of the goods and services purchased; additionally, it will be possible to use the billing data for the purposes of all the financial controls carried out by the Financial Police (paragraph 4.1.7). The same applies to the concerns raised by the Garante in respect of the processing of biometrics associated with video surveillance to monitor employee attendance in the public sector (paragraph 13.12).

1.4. No less demanding was the 'advisory' role played by the Garante in connection with the numerous opinions (see paragraph 4.5) issued on FOIA-type access requests following the inquiries made by transparency and anti-corruption officials and ombudspersons. This issue actually reflects the overarching tension between the legitimate requirements of administrative transparency and the need to respect personal data protection rights. In the past year, one of the main areas where such tension surfaced was the judgment No 20 of 21 February 2019, whereby the Italian Constitutional Court found that Section 14(1-a) of legislative decree No 33 of 14 March 2013 (regulating FOIA-type access) was in breach of constitutional principles (see also the 2018 Annual Report, paragraph 1; see paragraph 20.3 below). In that respect, reference should be made to the somewhat halting 'response' provided by Parliament via decree-law No 162 of 30 December 2019, which is expected to be implemented in full through an ad-hoc governmental regulation.

1.5. As already pointed out, the GDPR did not result into sudden

1

al Garante una pluralità di rilevanti attività per assicurare un passaggio "fluido" dal vecchio al nuovo regime. Tra queste, il compito di assicurare la "trasformazione" in codici di condotta, coerenti con il disposto degli artt. 40 e 41 del RGPD, dei preesistenti codici di deontologia e di buona condotta in materia di sistemi di informazione creditizia e di informazioni commerciali (di cui già agli allegati A.5 ed A.7 del Codice previgente) nel rispetto del termine fissato al 19 settembre 2019 dall'art. 20, d.lgs. n. 101/2018 (cfr. par. 14.3); e, ancora, la necessaria individuazione, avvenuta con provvedimento di carattere generale sottoposto a consultazione pubblica, delle prescrizioni contenute nelle preesistenti autorizzazioni generali riferite ai trattamenti di dati "sensibili" compatibili con la rinnovata cornice normativa (provv. 5 giugno 2019, n. 146, doc. web n. 9124510: cfr. parr. 5.5.1 e 13.2).

1.6. Pur tenendo conto della nuova cornice normativa e consapevole della fase di adeguamento al RGPD cui i destinatari della nuova disciplina sono stati chiamati, è proseguita l'attività ispettiva, anche grazie al prezioso contributo offerto dal Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza (par. 18.2), incentrandosi parte delle verifiche su settori ormai endemici nelle segnalazioni dirette all'Autorità: con particolare riguardo a talune pratiche commerciali, irrispettose della disciplina di protezione dei dati personali (quali l'attivazione di contratti non richiesti e il *telemarketing*), si distinguono alcune decisioni adottate dal Garante per la severità delle sanzioni pecuniarie irrogate, le più alte a far data dalla sua istituzione (cfr. parr. 10.1, 11.1 e 14.5.2). Merita poi ricordare la sanzione applicata in solido nei confronti di Facebook Ireland e Facebook Italy per le violazioni emerse nell'ambito dell'istruttoria relativa all'ormai nota vicenda "Cambridge Analytica", che ha interessato anche cittadini italiani ed ha messo in luce le

U-turns or leaps in the dark; however, the provisions adapting the national legal system to the GDPR as set forth in legislative decree No 101/2018 did commit a number of major tasks to the Garante in order to enable a 'seamless' transition from the old to the new regime. One such task was bringing about the 'transformation' of the pre-existing codes of ethics and professional practice concerning business information systems and credit reporting agencies into codes of conduct in line with Articles 40 and 41 of the GDPR; that transformation was to be finalised within the 19th of September 2019 as per Section 20 of legislative decree No 101/2018 (paragraph 14.3). Yet another example in this regard is provided by the need to determine which provisions out of those contained in the pre-existing general authorisations to process 'sensitive' data were compatible with the new legal framework; this was done by way of a general application decision which was the subject of a public consultation (decision No 146 of 5 June 2019, web doc. No 9124510 – see paragraphs 5.5.1 and 13.2).

1.6. Inspection activities continued partly thanks to the valuable contribution provided by the Special Privacy Protection and Technological Fraud Unit at the Financial Police, albeit by taking account of the new legal framework and the requirements to be met by all the stakeholders in order to adjust to the GDPR (paragraph 18.2). Those activities were focused in part on areas that have become staple components of the Authority's workload over the years. As regards, in particular, certain business practices that fall short of personal data protection rights (such as the activation of unsolicited contracts) and telemarketing), special attention should be paid to a few decisions by the Garante that stand out because of the hefty fines imposed – the highest ever since establishment of the Authority (paragraphs 10.1,

possibili gravi implicazioni (non solo sulla sfera giuridica individuale) dei trattamenti *online* di dati personali rispetto alla corretta formazione della volontà popolare nel corso del processo elettorale (cfr. parr. 11.3 e 19.2).

Ma anche in altri ambiti, nei settori più vari (cfr. par. 18.4), approfondimenti istruttori (cfr., per una "fotografia" dei settori interessati da segnalazioni, reclami e quesiti riferiti al 2019, parte IV, tab. 10 e 11) e controlli dell'Autorità hanno portato all'adozione di provvedimenti del Garante con i quali, esemplificando, si è stigmatizzato l'utilizzo non consentito di dati sanitari per finalità altre rispetto a quelle di cura che ne avevano determinato la raccolta (par. 5.1.1), la comunicazione illecita degli stessi (ad es. per errori nella trasmissione della documentazione: cfr. par. 5.1) nonché, ancora, la violazione dei diritti degli interessati nello svolgimento dell'attività giornalistica (par. 8.3), profilo toccato nel corso di un incontro con il Presidente del Consiglio nazionale dell'Ordine dei giornalisti (par. 8.2). Sono state oggetto di verifica anche la corretta configurazione delle (sempre più diffuse) *app* e l'utilizzo dei dati dalle stesse generati (cfr. parr. 5.1, 11.1 nonché 4.6 e 13.8), poste peraltro al centro del *Privacy Sweep 2019* (parr. 21.3 e 23.1).

1.7. Non può poi essere sottaciuto, nella fase di passaggio attraversata nel 2019, l'impegno dell'Autorità sul versante organizzativo – in particolare con la rivisitazione e riformulazione dei regolamenti interni di attività n. 1/2019 e 2/2019 (cfr., rispettivamente, doc. web n. 9107633 e n. 9107640), che ha consentito di adeguare il *modus operandi* del Garante al nuovo quadro normativo – e, quindi, sul piano operativo, con la messa a punto dei sistemi informativi dei quali l'Autorità si avvale (circostanza che, unitamente all'impegno determinante della componente tecnologica dell'Ufficio, ha consentito la "remotizzazione" e lo "*switch* digitale" dell'Autorità, che

11.1 and 14.5.2). Reference should also be made to the fine imposed jointly on Facebook Ireland and Facebook Italy on account of the infringements found within the framework of the investigations into the notorious 'Cambridge Analytica' case, which involved Italian nationals and brought to light the possibly serious impact of the online processing of personal data not only on the individual sphere, but also on the unfettered expression of people's will in the course of electoral processes (see paragraphs 11.3 and 19.2).

However, in-depth investigations (see, for an overview of the sectors where alerts, complaints and queries were received in 2019, Tables 10 and 11 in Part IV) and inspections by the Garante led to the adoption of several decisions in many additional areas (see paragraph 18.4), for instance, on account of the unauthorised use of data concerning health for purposes other the treatment-related ones that had legitimated data collection (paragraph 5.1.1); the unlawful communication of such data due, among others, to mistakes made in forwarding the relevant documents (paragraph 5.1); and the violation of data subjects' rights in the course of journalistic activities (paragraph 8.3) – which issues were addressed in a meeting with the Chair of the National Board of Professional Journalists (paragraph 8.2). Controls were also carried out on the appropriate configuration of increasingly used apps and the use of the data generated by those apps (see paragraphs 5.1, 11.1, 4.6 and 13.8); the use of apps was actually the focus of the 2019 Privacy Sweep (paragraphs 21.3 and 23.1).

1.7. One cannot fail to mention, as part of the transition experienced in the past year, the work done by the Garante in organisational terms, in particular by revising and restructuring the internal rules of procedure No 1/2019 and 2/2019 (see web docs. No 9107633 and 9107640, respectively). This work al-

1

senza soluzione di continuità ha potuto operare "in sicurezza" anche durante il *lockdown*) (par. 25.5).

1.8. Il processo di adeguamento al nuovo quadro normativo, peraltro, non è rimasto confinato a livello nazionale; da un lato infatti il Garante ha assicurato, anzitutto per il tramite della piattaforma IMI (*Internal Market Information System*), ormai in fase avanzata di rodaggio, una partecipata cooperazione rispetto alle attività di controllo dei trattamenti transfrontalieri con le altre autorità di protezione dei dati europee, attività particolarmente onerosa per alcuni Dipartimenti dell'Autorità (cfr. parr. 11.4, 14.6 e cap. 16) e, dall'altro, ha contribuito costantemente (ed in varie forme) all'operatività del Comitato europeo per la protezione dei dati, anche mediante la partecipazione a sottogruppi di lavoro (par. 21.1 e tab. 16).

Il Comitato ha continuato a lavorare su linee guida e documenti finalizzati a chiarire concetti chiave del vecchio e del nuovo quadro europeo sulla protezione dei dati. Sono state adottate così le linee guida sul trattamento dei dati necessari all'esecuzione di un contratto di cui è parte l'interessato (art. 6, par. 1, lett. *b*), del RGPD), base giuridica che merita particolare attenzione nel caso della prestazione di servizi *online*, le linee guida relative all'ambito di applicazione territoriale del RGPD, l'aggiornamento del parere del Gruppo Art. 29 sulle nozioni di titolare e responsabile del trattamento. Non sono mancati gli interventi volti a fornire indicazioni in ordine alle novità introdotte dal RGPD (quali i pareri sulle liste di trattamenti per i quali è necessaria una valutazione di impatto sulla protezione dei dati, le linee guida in materia di codici di condotta e di certificazioni, nonché quelle in materia di protezione dei dati *by design* e *by default*) che si sono affiancate a nuovi orientamenti relativi a temi più conosciuti, quali la videosorveglianza (oggetto di un nuovo parere che tiene

lowed adjusting the Garante's *modus operandi* to the new legal framework and was translated operationally into developing the information systems relied on; this in turn made it possible to implement the Authority's 'digital switch' thanks to the key commitment shown by its technological unit and enabled the Garante to continue working seamlessly and securely also during the lockdown period (paragraph 25.5).

1.8. The adjustment to the new legal framework was actually not limited to the national arena. On the one hand, the Garante participated in the cooperation activities with other European SAs related to supervision over cross-border processing activities – first and foremost through the IMI (Internal Market Information System) platform, which has by now completed its run-in phase. Those cooperation activities increased considerably the workload of various departments in the Authority (paragraphs 11.4, 14.6, 16). On the other hand, the Garante contributed unceasingly, in many different ways, to the work of the European data protection Board including through participation in various expert groups (paragraph 21.1 and Table 16).

The Board continued working on guidance and documents intended to clarify key notions of both the old and the new European legal framework concerning data protection. This led to adoption of the guidelines on the processing of data required for performance of a contract concluded with the data subject (Article 6(1), letter b), of the GDPR) which legal basis is especially relevant in connection with the provision of online services), the guidelines on the territorial scope of application of the GDPR, and the updated WP29 opinion on the notions of data controller and data processor. The innovations introduced by the GDPR were also addressed, in particular via the opinions on the processing activities for which a

conto delle novità tecnologiche degli ultimi anni) e l'esercizio del cd. diritto all'oblio relativo ai motori di ricerca (par. 21.1), tematica che ha in più occasioni impegnato anche il Garante (cfr. par. 8.5).

Anche il Comitato, come il Garante, ha lavorato all'adeguamento delle proprie procedure interne attraverso tre revisioni delle regole di procedura e ha visto la creazione, nel suo ambito, della nuova Commissione di controllo coordinato che consentirà di rafforzare la cooperazione tra le diverse autorità di protezione dei dati in materia di controllo sugli organismi, gli uffici e le agenzie operanti nei settori delle frontiere, dell'asilo e della migrazione (SIS, EES, ETIAS e VIS), della cooperazione di polizia e giudiziaria (SIS, EPPO, Eurojust, ECRIS-TCN) e del mercato interno (IMI) (par. 21.2).

Il Comitato non ha inoltre fatto mancare il proprio contributo ai lavori della Commissione europea volti al riesame del RGPD (previsto, in base all'art. 97 del RGPD, entro il 25 maggio 2020 e, successivamente, ogni quattro anni) che in questa occasione ha riguardato in particolare l'applicazione e il funzionamento del Capo V sul trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali e del Capo VII su cooperazione e coerenza. All'esito di quello che sembra costituire un primo sommario bilancio dell'attività di cooperazione delle autorità di protezione dei dati, il Comitato ha valutato positivamente questo iniziale periodo di attuazione del RGPD e ha ritenuto prematura ogni sua modifica, considerando piuttosto necessaria, per completare il quadro normativo UE sulla protezione dei dati, una tempestiva adozione del regolamento *e-Privacy*.

Innovazione è stata una parola chiave anche per l'attività del Consiglio d'Europa e dell'OCSE: il primo, che ha visto la firma da parte di sedici nuovi Stati, tra cui l'Italia, del Protocollo emendativo della Convenzione 108 che ha dato vita

data protection impact assessment is required, the guidelines on codes of conduct and certifications and on data protection by design and be default; new guidance was provided on long-debated issues such as video surveillance – which was addressed by a new opinion taking account of the latest available technology – and the exercise of the right to be forgotten vis-à-vis search engines (paragraph 21.1), the latter being an area tackled by the Garante on several occasions as well (paragraph 8.5).

Like the Garante, the Board worked on adjusting its own Rules of Procedure, which were revised three times during 2019; additionally, a new Coordinated Supervision Committee was set up within the Board to enhance cooperation among supervisory authorities in the oversight over the bodies, agencies and offices operating in the areas related to borders, asylum and migration (SIS, EES, ETIAS, VIS), judicial and police cooperation (SIS, EPPO, Eurojust, ECRIS-TCN) and the internal market (IMI) (paragraph 21.2).

Nor did the Board fail to contribute to the review of the GDPR the European Commission is tasked with performing firstly within 25 May 2020, pursuant to Article 97 of the GDPR, and every four years thereafter. This first review concerned, in particular, the implementation and functioning of Chapter V on international data transfers to third countries or international organisations and Chapter VII on cooperation and consistency procedures. Having taken stock, albeit summarily, of the cooperation activities by national supervisory authorities, the Board issued a favourable judgment regarding this initial implementing period of the GDPR and considered it premature to put forward amendment proposals; conversely, the timely adoption of the new e-privacy regulation was found to be necessary in order to complete the EU data protection legal framework.

Innovation was key also for the

1

alla cd. Convenzione 108+, e il secondo che ha avviato il lavoro di revisione delle linee guida OCSE sulla *Privacy* adottate, nella versione attuale, nel 2013 (par. 21.3).

1.9. Nel tempo che verrà, la cooperazione sarà una delle chiavi di volta per un'efficace protezione dei diritti fondamentali, ma pure della sicurezza digitale (profilo la cui rilevanza emerge anche in relazione al fenomeno dei *data breach* notificati all'Autorità: cfr. par. 16). Leale collaborazione, nel rispetto dei distinti ruoli, anzitutto con i titolari dei trattamenti, valorizzando i molteplici strumenti di *accountability* e di interlocuzione prefigurati dal nuovo quadro normativo (codici di condotta, consultazione dell'autorità di controllo a seguito di valutazione d'impatto, certificazioni, Rpd); ma anche rinforzata cooperazione con gli organi che si occupano della normazione tecnica internazionale e nazionale (par. 22) e, ovviamente, con altre autorità di controllo. E non solo con quelle di protezione dei dati, di cui si è appena detto, ma, in prospettiva – come emerso dall'indagine condotta congiuntamente con l'Autorità per le garanzie nelle comunicazioni e l'Autorità garante della concorrenza e del mercato in materia di *Big data*, tematica dai tanti chiaroscuri, desumibili dal rapporto finale (doc. web n. 9264297) –, anche con altre autorità nazionali di settore, esse pure coinvolte dalle sfide veicolate dall'evoluzione tecno-economica, per un superamento, a vantaggio anzitutto dei destinatari delle tutele, dei limiti che una rigida compartimentazione in silos delle rispettive attribuzioni potrebbe determinare.

1.10. E la dimensione dei *Big data* – ma più in generale della *data economy*, con i rischi sempre più evidenti (per i singoli e la collettività) connessi alla *commodification* dei dati personali (cfr. par. 11.2) e amplificati dal cd. "capitalismo della sorveglianza" – schiude le

Council of Europe and OECD: the former achieved the signature by sixteen new countries, including Italy, of the Protocol amending the 108/81 Convention, which gave rise to the so-called 'Convention 108+'; the latter started revising the OECD Privacy Guidelines, whose current version was adopted in 2013 (paragraph 21.3).

1.9. In the coming years, cooperation is bound to be one the pillars to achieve effective protection of fundamental rights and digital security – as shown by the data breach notifications submitted to the Authority, see paragraph 16. This will include fair cooperation first and foremost with data controllers, leveraging on the many accountability and interaction tools that are envisaged in the new legal framework – codes of conduct, consultation of the supervisory authority following an impact assessment, certifications, DPOs. It will also entail reinforced cooperation with national and international technical standards organisations (paragraph 22) and, obviously, other supervisory bodies – including those outside the data protection area. Indeed, as shown by the joint investigation that was carried out with the Italian Authority for Communications Safeguards and the Italian Antitrust Authority regarding big data, which yielded a piebald picture as better detailed in the final report of that investigation (web doc. No 9264297), other national sector-specific authorities will have to be involved as they are also impacted by the challenges raised by technological and economic developments. This is aimed ultimately at overcoming any limitations possibly resulting from a silos mentality as applied to the discharge of the respective tasks – which would be beneficial in the first place to the stakeholders' community.

1.10 The big data dimension, more generally the issues related to the data economy and the increasingly blatant

prospettive future (anzitutto legate alla diffusione dell'intelligenza artificiale e della scansione algoritmica delle nostre vite) verso le quali le autorità di protezione dei dati sono chiamate a proiettare con urgenza la propria azione, prendendo anzitutto piena conoscenza del dato di realtà (e in questa chiave il Garante ha dedicato al tema "I Confini del Digitale. Nuovi scenari per la protezione dei dati" il Convegno organizzato in occasione della Giornata europea della protezione dei dati personali 2019, i cui atti sono raccolti nel volume disponibile al doc. web n. 9078052). In questo nuovo e accidentato percorso va tenuto a mente il monito (e l'incitamento) che Giovanni Buttarelli – al quale va il ricordo affettuoso dell'Autorità – ebbe a rivolgere (anzitutto) ai rappresentanti delle autorità di protezione dei dati in occasione del discorso di apertura della 40ª Conferenza internazionale (*Debating Ethics: Dignity and Respect in a Data Driven Life Choose Humanity: Putting Dignity Back into Digital*): "All revolutions have victims. So in the Fourth Industrial Revolution, who are the winners and losers? How can we develop a positive relationship with new technologies, which puts people and dignity at the centre? This is about defining the values of the future. And we have to do it before it is too late".

risks caused by the commodification of personal data (see paragraph 11.2) - compounded by the so-called 'surveillance capitalism' - point to the future fields of work for data protection authorities, mainly in connection with the rise of artificial intelligence and the algorithmic assessment of our lives. This is where urgent action is needed, starting from the thorough knowledge of factual reality – see, in this connection, the conference organised by the Garante on 'Digital Borders: New Scenarios for Data Protection', which was held on the occasion of the 2019 European data protection day and whose proceedings were published in a booklet available on the Authority's website as web doc. No 9078052. In pursuing this new, rocky path one should recall the warning (and the incitement) given by Giovanni Buttarelli – who will always have a place in our hearts – first and foremost to the representatives of data protection authorities in his opening speech at the 40th international data protection conference (Debating Ethics: Dignity and Respect in a Data-Driven Life / Choose Humanity: Putting Dignity Back into Digital): 'All revolutions have victims. So in the Fourth Industrial Revolution, who are the winners and losers? How can we develop a positive relationship with new technologies, which puts people and dignity at the centre? This is about defining the values of the future. And we have to do it before it is too late.'

2 Il quadro normativo in materia di protezione dei dati personali

2.1. *Le modifiche al Codice*

Prevenzione e contrasto dell'evasione fiscale

Nel 2019 l'attività del Parlamento e del Governo ha prodotto interventi normativi in diversi settori dell'ordinamento aventi impatto sulla protezione dei dati, uno dei quali, nel quadro di un più ampio intervento in materia di lotta all'evasione fiscale (profilo sul quale si tornerà *amplius* nel par. 4.1), ha apportato alcune modifiche al Codice: si tratta della legge di bilancio 2020 (legge 27 dicembre 2019, n. 160, recante il bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022) e, in particolare, dei commi da 681 a 686 dell'articolo 1.

Il comma 681, nel considerare la prevenzione e il contrasto all'evasione fiscale "rilevanti obiettivi di interesse pubblico", mediante integrazione della lett. *i*), dell'art. 2-*sexies*, comma 2, del Codice (riferita alle attività dirette all'applicazione delle disposizioni in materia tributaria e doganale), annovera fra le materie nelle quali si considera rilevante l'interesse pubblico perseguito dalle relative attività anche la "prevenzione e il contrasto all'evasione fiscale". Lo stesso comma 681, inoltre, integrando l'art. 2-*undecies*, comma 1, del Codice, con una nuova lettera (*f-bis*) rende applicabili le limitazioni dei diritti dell'interessato ivi previste anche rispetto "agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale".

Con ciò sostanzialmente si fa assurgere alle predette finalità non solo il rango di rilevante interesse pubblico tale da legittimare il trattamento di particolari categorie di dati, ma anche quello di funzioni rispondenti a interessi nazionali di tale importanza da giustificare la limitazione dei diritti degli interessati.

Le modifiche apportate al Codice fanno da cornice ad un più ampio intervento normativo volto a dotare l'Agenzia delle entrate di maggiori strumenti di verifica e di indagine in ambito fiscale o a fini di prevenzione e di contrasto dell'evasione fiscale. A tal fine il comma 682 stabilisce che per le attività di "analisi del rischio" già attribuite dall'art. 11, comma 4, d.l. 6 dicembre 2011, n. 201 (convertito dalla l. n. 214/2011), con particolare riferimento all'utilizzo dei dati contenuti nell'Archivio dei rapporti finanziari di cui all'art. 7, d.P.R. n. 605/1973, l'Agenzia delle entrate, anche previa pseudonimizzazione dei dati personali, possa avvalersi delle tecnologie, delle elaborazioni e delle interconnessioni con le altre banche dati di cui dispone, allo scopo di individuare criteri di rischio utili per far emergere posizioni da sottoporre a controllo e incentivare così l'adempimento spontaneo. Per le stesse finalità e con le medesime modalità, è consentito anche alla Guardia di finanza l'utilizzo dei dati contenuti nell'archivio dei rapporti finanziari, avvalendosi delle tecnologie, delle elaborazioni e delle interconnessioni con le altre banche dati di cui è titolare (comma 686).

Quanto alla limitazione dei diritti (oggetto di rilievi critici da parte del Garante: cfr. *amplius* par. 4.1.4), essa è prevista in relazione al trattamento dei dati contenuti nell'Archivio dei rapporti finanziari e rispetto ai diritti di cui agli artt. 14, 15, 17, 18 e 21 del RGPD. Con decreto del Mef, sentiti il Garante e l'Agenzia delle entrate, sono definite: a) le specifiche limitazioni e le modalità di esercizio dei diritti in

modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto all'obiettivo di interesse pubblico; b) le disposizioni specifiche relative al contenuto minimo essenziale di cui all'art. 23, par. 2, del RGPD; c) le misure adeguate a tutela dei diritti e delle libertà degli interessati (comma 683).

Infine, nel rispetto del principio di responsabilizzazione, il trattamento di tali dati deve essere oggetto di una valutazione unitaria di impatto sulla protezione dei dati da parte dell'Agenzia delle entrate, sentito il Garante, che deve contenere "anche le misure necessarie e ragionevoli per assicurare la qualità dei dati" (comma 684). Il Garante avrà modo di svolgere le proprie valutazioni di competenza in occasione dei provvedimenti che dovrà adottare in attuazione delle descritte norme.

La disciplina così sintetizzata e in particolare le garanzie ivi previste sono il portato del recepimento da parte del Parlamento delle indicazioni rese dal Garante in una memoria scritta inviata, a richiesta, alla competente Commissione del Senato (12 novembre 2019, doc. web n. 9184376). In tale documento il Presidente dell'Autorità ha segnalato altresì, in ragione delle finalità in concreto perseguite, l'inutilità del ricorso alla pseudonimizzazione dei dati personali che anzi potrebbe essere controproducente per l'efficacia della lotta all'evasione posto che tale finalità implica e necessita dell'individuazione delle posizioni da sottoporre a controllo e, quindi, dell'identificazione del contribuente.

2.2. *Le leggi di particolare interesse per la protezione dei dati personali*

Numerosi i provvedimenti normativi approvati nel 2019 con riflessi sulla protezione dei dati personali; fra questi, al fine di offrirne una ricognizione sintetica, ma in grado comunque di rendere conto dell'ampiezza e dell'eterogeneità delle materie che rientrano nell'area di interesse dell'Autorità, si menzionano in particolare:

Proroga funzioni del Garante

1) Il decreto-legge 17 marzo 2020, n. 18, recante misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19 (cd. Cura Italia), convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, il cui art. 118 dispone la proroga delle funzioni del Garante sino a 60 giorni dalla cessazione dello stato di emergenza decretato dal Governo per far fronte all'epidemia. Si tratta della quarta estensione della proroga dell'attività del Collegio eletto nel 2012 che avrebbe dovuto esaurire lo svolgimento delle proprie funzioni il 19 giugno 2019. A tale naturale scadenza è seguito un primo regime di *prorogatio* di 60 giorni in conformità a quanto previsto da un parere del Consiglio di Stato reso nel 2012 in riferimento ad un caso analogo; quindi il decreto-legge 7 agosto 2019, n. 75, recante misure urgenti per assicurare la continuità delle funzioni del Collegio del Garante per la protezione dei dati personali, ha prorogato i poteri e le funzioni del Presidente e dei membri del Collegio limitatamente agli atti di ordinaria amministrazione e a quelli indifferibili e urgenti, fino a "non oltre ulteriori sessanta giorni dalla data di entrata in vigore" del decreto medesimo, ossia fino al 7 ottobre 2019, termine portato poi al 31 dicembre dalla legge di conversione 4 ottobre 2019, n. 107. Successivamente l'art. 2, d.l. 30 dicembre 2019, n. 162 (cd. Milleproroghe) convertito dalla legge 28 febbraio 2020, n. 8, ha esteso la proroga al 31 marzo 2020, sino, appunto, all'ultimo intervento normativo che ha "collegato" la scadenza del periodo di *prorogatio* alla cessazione dell'emergenza sanitaria, senza però il limite dell'ordinaria amministrazione e del compimento dei soli atti indifferibili e urgenti.

"Milleproroghe"

2) Il decreto-legge 30 dicembre 2019, n. 162, recante disposizioni urgenti in materia di proroga di termini legislativi, di organizzazione delle pubbliche ammini-

2

strazioni, nonché di innovazione tecnologica (cd. Milleproroghe), convertito, con modificazioni, dalla legge 28 febbraio 2020, n. 8, contiene alcune disposizioni di interesse che di seguito brevemente si commentano:

a) l'art. 1, comma 7, che apporta modifiche al decreto legislativo n. 14 marzo 2013, n. 33, in materia di trasparenza e pubblicazione di atti, al fine di adeguare la normativa vigente alla sentenza della Corte costituzionale 21 febbraio 2019, n. 20 (cfr. par. 20.3), relativa agli obblighi di pubblicazione per i titolari di incarichi dirigenziali di cui all'art. 14 del predetto decreto. L'originaria formulazione della disposizione è stata modificata e integrata da alcuni emendamenti approvati il 10 febbraio 2020 presso le Commissioni riunite I Affari costituzionali e V Bilancio della Camera, sicché la disciplina che ne è risultata prevede che, nelle more dell'adozione dei provvedimenti di adeguamento alla sentenza della Corte costituzionale, ai soggetti di cui all'art. 14, comma 1-*bis*, d.lgs. n. 33/2013 (titolari di incarichi di direzione o di governo comunque denominati e per i titolari di incarichi dirigenziali, a qualsiasi titolo conferiti), non si applicano le misure di cui agli artt. 46 e 47 del medesimo decreto legislativo; misure che continuano invece a trovare applicazione per i titolari degli incarichi dirigenziali previsti dall'art. 19, commi 3 e 4, d.lgs. 30 marzo 2001, n. 165 (segretari generali e dirigenti generali), rispetto ai quali continua a trovare piena applicazione la disciplina di cui all'art. 14 del citato d.lgs. n. 33/2013. Con regolamento di "delegificazione", da adottarsi ex art. 17, comma 2, l. n. 400/1988, su proposta del Ministro della pubblica amministrazione, sentito il Garante, saranno individuati i dati di cui all'art. 14, comma 1, che le p.a. dovranno pubblicare con riferimento ai titolari amministrativi di vertice e di incarichi dirigenziali, comunque denominati, ivi comprese le posizioni organizzative ad essi equiparate, nel rispetto dei seguenti criteri: graduazione degli obblighi di pubblicazione dei dati di cui al comma 1, lett. *b*), ed *e*) (*curriculum* e altri eventuali incarichi con oneri a carico della finanza pubblica e compensi spettanti), in relazione al rilievo esterno dell'incarico svolto, al livello di potere gestionale e decisionale esercitato correlato all'esercizio della funzione dirigenziale e tenuto conto della complessità della struttura; previsione che i dati di cui alla lett. *f*) (documentazione attestante la complessiva situazione patrimoniale e sue variazioni, nonché la dichiarazione dei redditi) possano essere oggetto esclusivamente di comunicazione all'amministrazione di appartenenza; individuazione dei dirigenti dell'amministrazione dell'interno, degli affari esteri e della cooperazione internazionale, delle Forze di polizia, delle Forze armate e dell'amministrazione penitenziaria per i quali non sono pubblicati i dati in ragione del pregiudizio alla sicurezza nazionale interna ed esterna e all'ordine e sicurezza pubblica, nonché in rapporto ai compiti svolti per la tutela delle Istituzioni democratiche e di difesa dell'ordine e della sicurezza interna ed esterna (le amministrazioni particolari sopra citate, tuttavia, possono, nelle more dell'adozione del menzionato d.P.R., provvedere con proprio decreto all'individuazione delle figure dirigenziali, anche generali, cui non si applicano gli obblighi di pubblicazione – comma 7-*bis*); divieto di indicizzazione dei dati oggetto della disciplina del d.P.R. (art. 1, comma 7-*ter*); gli obblighi di trasparenza sono estesi ai titolari di incarichi negli organismi di cui all'art. 144 del testo unico degli enti locali (Commissione straordinaria e Comitato di sostegno e monitoraggio) (comma 7-*quater*);

b) l'art. 36 che, integrando il d.P.R. n. 462/2001, istituisce presso l'Inail una banca dati informatizzata da alimentarsi a cura dei datori di lavoro con informazioni sugli organismi deputati alle verifiche degli impianti elettrici;

c) l'art. 42, in materia di agenda digitale, che mira a potenziare l'operatività del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri e, mediante mirate modifiche al d.l. n. 135/2018, precisa i compiti della

medesima Presidenza da svolgere per il tramite della società PagoPA con riguardo allo sviluppo e all'implementazione del punto di accesso telematico di cui all'art. 64-*bis*, d.lgs. n. 82/2005 (codice dell'amministrazione digitale - Cad) e della piattaforma di cui all'art. 50-*ter* del medesimo decreto.

3) Il decreto-legge 30 dicembre 2019, n. 161, recante modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni, convertito dalla legge 28 febbraio 2020, n. 7, volto a innovare la disciplina delle intercettazioni telefoniche in funzione della necessaria tutela della riservatezza delle persone, apportando nel contempo correttivi al decreto legislativo 29 dicembre 2017, n. 216 (cd. riforma Orlando) sul piano della tutela delle garanzie difensive e della funzionalità nello svolgersi delle indagini preliminari. Su alcuni delicati aspetti, quale in primo luogo quello della ineludibile necessità di un passaggio giurisdizionale per l'acquisizione delle intercettazioni al fascicolo del pubblico ministero, si è inteso ripristinare il testo del codice di procedura penale, nella versione anteriore all'intervento normativo, conservando tuttavia le norme in materia di utilizzo del cd. captatore informatico il cui ambito di operatività è stato ampliato (le risultanze potranno essere usate come prova anche per reati diversi da quelli per i quali ne è stato autorizzato l'utilizzo). La necessaria tutela della riservatezza anche nella fase della verbalizzazione ha indotto a sostituire il meccanismo di selezione da parte della polizia giudiziaria delle intercettazioni non utilizzabili con un dovere di vigilanza del pubblico ministero. Infine, si prevede che con decreto del Ministro della giustizia, non avente natura regolamentare, adottato sentito il Garante, siano fissati i criteri a cui il Procuratore della Repubblica deve attenersi per regolare le modalità di accesso all'archivio digitale delle intercettazioni di cui all'art. 89-*bis* delle norme di attuazione del codice di procedura penale. La materia delle intercettazioni – con il difficile bilanciamento fra esigenze di indagine, riservatezza delle persone e diritto di cronaca – è da sempre oggetto di particolare considerazione da parte del Garante, che anche recentemente vi ha riservato rilevanti interventi, sia in sede di audizione sul disegno di legge di conversione del d.l. n. 161/2019, sia in sede di segnalazione, con particolare riferimento all'utilizzo del captatore informatico. Nell'audizione in Commissione giustizia del Senato, tenutasi il 4 febbraio 2020 (cfr. par. 3.1.1), il Presidente del Garante ha focalizzato il suo intervento sugli aspetti di maggior interesse dal punto di vista della protezione dei dati sottolineando i seguenti profili: la sottrazione dal verbale dovrebbe riguardare tutti i dati personali irrilevanti e non soltanto quelli sensibili o correlati ad espressioni lesive della reputazione, dal momento che la circolazione endoprocessuale di dati irrilevanti a fini investigativi è illegittima, sotto il profilo della pertinenza, indipendentemente dalla natura sensibile del dato o dal suo carattere lesivo; la disposta derubricazione del divieto di verbalizzazione dei dati irrilevanti in dovere di vigilanza del pubblico ministero impone, per non vanificare la portata innovativa della riforma, un vaglio attento, da parte dell'organo requirente, circa l'effettivo rispetto di questo canone di minimizzazione; occorre chiarire le conseguenze sanzionatorie della diffusione del contenuto delle intercettazioni non acquisite, oggetto di un generico divieto non presidiato da specifiche sanzioni, e rafforzare le garanzie di riservatezza (almeno) degli atti non acquisiti perchè, in particolare, i rilevanti o inutilizzabili, contenuti nell'apposito archivio, prevedendo misure adeguate anche con provvedimenti attuativi sui quali potrebbe essere acquisito il parere del Garante; in ordine alle intercettazioni mediante captatori, si è ravvisata l'esigenza di colmare le lacune normative già rilevate dal Garante in sede di parere sugli schemi di decreto legislativo e di decreto attuativo della "riforma Orlando", come pure nell'ambito della segnalazione rivolta al Parlamento e al Governo del 30 aprile 2019 (doc. web n. 9107773) che teneva conto dei rischi, resi palesi da recenti

2

La riforma delle intercettazioni di comunicazioni

fatti di cronaca, propri del ricorso a particolari tipologie di *software*-spia. Riprendendo alcune delle indicazioni fornite nella segnalazione, in sede di audizione il Presidente del Garante ha suggerito l'opportunità di introdurre un divieto espresso di ricorso a sistemi che presentano rischi particolari e ulteriori rispetto a quelli, già rilevanti, inevitabilmente caratterizzanti le intercettazioni mediante *trojan* (*app* o comunque *software* che non siano inoculati direttamente sul dispositivo-ospite, ma scaricati da piattaforme liberamente accessibili a chiunque, nonché archiviazione mediante sistemi *cloud*, segnatamente in *server* posti fuori dal territorio nazionale). Si è altresì sottolineata l'esigenza di escludere – con previsione suscettibile di inclusione nel decreto cui si demanda la disciplina dei requisiti tecnici dei captatori – il ricorso a *software* inidonei a ricostruire nel dettaglio ogni attività svolta sul sistema ospite e sui dati ivi presenti, senza alterarne il contenuto, per garantire la completezza della catena di custodia della prova informatica. È stata anche rilevata la necessità di chiarire le conseguenze (in termini di inutilizzabilità dei contenuti captati) del ricorso a programmi informatici non conformi ai requisiti di sicurezza previsti con il decreto ministeriale, nonché di esplicitare i termini di applicabilità della disciplina del captatore alle intercettazioni preventive, esigendo per queste garanzie non inferiori rispetto a quelle proprie delle giudiziali. Si è anche segnalato che il previsto trasferimento dei dati captati con *trojan* direttamente all'archivio e non invece al *server* della Procura, nel determinare l'accesso all'archivio da parte della polizia giudiziaria anche per fini investigativi, rappresenta un'anomalia tale da contraddire la natura stessa dell'archivio in parola, quale luogo di custodia di atti non processualmente rilevanti, da sottrarre quindi alla circolazione endoprocessuale. Si è infine sollecitato un supplemento di riflessione del Parlamento in ordine alla progressiva estensione dell'ambito applicativo di tale particolare modalità di svolgimento delle intercettazioni, che in ragione della sua intrinseca invasività e dei rischi che può comportare, dovrebbe invece restare eccezionale. Dei rilievi esposti dal Garante si è tenuto ampiamente conto in sede emendativa; tuttavia, tra le proposte accolte figura soltanto quella inerente al trasferimento dei dati captati con *trojan* esclusivamente negli impianti della Procura e non direttamente nell'archivio digitale.

Legge di bilancio 2020

4) La legge 27 dicembre 2019, n. 160, recante il bilancio di previsione dello Stato per l'anno finanziario 2020 e il bilancio pluriennale per il triennio 2020-2022, delle cui norme di interesse in materia di protezione dei dati personali si segnalano, in particolare, le seguenti:

a) i commi da 681 a 686 dell'art. 1, in materia di prevenzione e contrasto all'evasione fiscale che apportano anche modifiche al Codice, di cui si è detto al par. 2.1;

b) il comma 145 che modifica l'art. 19, d.lgs. 14 marzo 2013, n. 33, in materia di trasparenza e pubblicazione di atti, prevedendo che le p.a. debbano pubblicare, oltre al bando di concorso e i criteri di valutazione della commissione valutatrice, anche le tracce delle prove e le graduatorie finali, aggiornate con l'eventuale scorrimento degli idonei non vincitori (modifiche ai commi 1 e 2 dell'art. 19). Inoltre, tramite l'aggiunta al medesimo articolo del comma 2-*bis*, si dispone che le p.a. e gli organismi partecipati assoggettati alla normativa in materia di trasparenza pubblichino il collegamento ipertestuale di tali dati. Sul punto, nella citata memoria del 12 novembre 2019 avente ad oggetto il disegno di legge di bilancio (doc. web n. 9184376, su cui v. *amplius* par. 2.1), il Presidente del Garante ha evidenziato come l'introduzione di nuove norme in materia di trasparenza implichino il rischio di una duplicazione degli obblighi di pubblicazione già previsti dalla normativa di settore, con rilevanti ripercussioni anche in termini di proporzionalità della documentazione pubblicata;

c) i commi 288 e 289 finalizzati ad incentivare l'utilizzo di strumenti di paga-

mento elettronici, hanno previsto che le persone fisiche maggiorenni residenti nel territorio dello Stato che effettuano acquisti con strumenti di pagamento elettronici da soggetti che svolgono attività di vendita di beni e di prestazione di servizi, hanno diritto ad un rimborso in denaro (comma 288), alle condizioni e sulla base dei criteri individuati da un decreto del Ministro dell'economia e delle finanze da adottare, sentito il Garante, entro il 30 aprile 2020 (comma 289);

d) il comma 728, in materia di apparecchi da gioco, secondo cui, fatta salva la disciplina in materia di protezione dei dati personali, l'utilizzo e l'analisi dei dati registrati e trasmessi da tali apparecchi sono riservati: al Ministero della salute e all'Osservatorio per il contrasto della diffusione del gioco d'azzardo e il fenomeno della dipendenza grave, per finalità di studio, monitoraggio e tutela della salute dei cittadini; all'Agenzia delle dogane e dei monopoli, per le finalità di pubblicazione dei *report* sul proprio sito e di documentazione su richiesta del Governo e di organi parlamentari; alla suddetta Agenzia, alle Forze dell'ordine ed ai soggetti istituzionali preposti, per i compiti di controllo e verifica degli adempimenti concessori ed esigenze di prevenzione e repressione del gioco illegale. Si prevede inoltre che con decreto del Ministro dell'interno siano disciplinati i criteri e le garanzie necessarie al rispetto delle disposizioni introdotte per tutti i soggetti coinvolti nella gestione della rete telematica e nei sistemi di conservazione dei dati raccolti;

e) il comma 791 che, al fine di facilitare le attività di riscossione degli enti locali, autorizza l'accesso alle informazioni relative ai debitori presenti nell'Anagrafe tributaria degli enti creditori e, per il tramite di essi, dei soggetti ai quali gli enti hanno affidato il servizio di riscossione delle proprie entrate; a tal fine, è previsto espressamente che gli enti, nel consentire, sotto la propria responsabilità, ai soggetti affidatari l'utilizzo dei servizi di cooperazione informatica forniti dall'Agenzia delle entrate, debbano nominare tali soggetti responsabili esterni del trattamento ai sensi delle vigenti disposizioni in materia di tutela dei dati personali.

Decreto-legge in materia fiscale

5) Il decreto-legge 26 ottobre 2019, n. 124, recante disposizioni urgenti in materia fiscale, convertito dalla legge 19 dicembre 2019, n. 157, che contiene specifiche misure per esigenze fiscali e finanziarie indifferibili, anche mediante la lotta all'evasione fiscale e la pertinente disciplina penale. Tra le norme di interesse sotto il profilo della protezione dei dati personali si segnalano in particolare le seguenti:

a) l'art. 4, in materia di contrasto dell'illecita somministrazione di manodopera, che aggiunge l'art. 17-*bis* al d.lgs. 9 luglio 1997, n. 241, prevedendo, al comma 5, un obbligo di trasmissione al committente dei dati necessari per il riscontro degli importi trattenuti e la congruità del versamento dovuto. In particolare, si dispone che al fine di consentire al committente il riscontro dell'ammontare complessivo degli importi ricevuti con le trattenute effettuate dalle imprese, queste gli trasmettano – e per le imprese subappaltatrici anche all'impresa appaltatrice – un elenco nominativo di tutti i lavoratori, identificati mediante codice fiscale, impiegati direttamente nel mese precedente nell'esecuzione di opere e servizi affidati dal committente;

b) l'art. 14, relativo all'utilizzo dei *file* delle fatture elettroniche da parte dall'Agenzia delle entrate e dalla Guardia di finanza, che inserisce i nuovi commi 5-*bis*, 5-*ter* e 5-*quater* nell'art. 1, d.lgs. 5 agosto 2015, n. 127, concernente la fatturazione elettronica e la trasmissione telematica delle fatture o dei relativi dati. Il comma 5-*bis* prevede che i *file* delle fatture elettroniche, acquisiti e memorizzati fino al 31 dicembre dell'ottavo anno successivo a quello di presentazione della dichiarazione di riferimento ovvero fino alla definizione di eventuali giudizi, possono essere utilizzati dall'Agenzia delle entrate e dalla Guardia di finanza per le attività di "analisi del rischio" (cfr. par. 4.1.4). A tal fine la Guardia di finanza e l'Agenzia delle entrate

2

adottano, sentito il Garante, idonee misure di garanzia a tutela dei diritti degli interessati attraverso la previsione di apposite misure di sicurezza, anche di carattere organizzativo, in conformità con le disposizioni del RGPD e del Codice (art. 5-*ter*). Infine, l'art. 5-*quater*, introdotto durante l'esame presso la Camera, mantiene ferma l'applicazione della disciplina speciale prevista dalla legge n. 124/2007 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto) in materia di fatturazione elettronica, con riguardo alla memorizzazione, conservazione e consultazione di fatture elettroniche relative alle cessioni di beni e altre prestazioni destinate agli organismi di informazione per la sicurezza (Dis, Aise e Aisi). Nel corso dei lavori parlamentari, su richiesta dalla competente Commissione della Camera, il Presidente dell'Autorità ha inviato una memoria scritta (5 novembre 2019, doc. web n. 9178137: cfr. par. 4.1.7) evidenziando criticamente, sulla scorta di analoghi rilievi fatti dal Garante nei provvedimenti 18 novembre e 20 dicembre 2018 con riguardo allo schema di provvedimento del Direttore dell'Agenzia delle entrate in materia di fatturazione elettronica, l'eccessiva e sproporzionata memorizzazione di dati non fiscalmente rilevanti e inerenti la descrizione delle prestazioni fornite, suscettibili di comprendere anche dati idonei a rivelare lo stato di salute o l'eventuale sottoposizione dell'interessato a procedimenti penali. L'Autorità ha pertanto suggerito di selezionare la tipologia di informazioni oggetto di trattamento, posto che la memorizzazione (e potenzialmente anche l'utilizzazione) di dati personali sproporzionati – per quantità e qualità delle informazioni – rispetto alle reali esigenze perseguite avrebbe reso la norma illegittima per contrasto con il principio di proporzionalità del trattamento dei dati, assurto nella giurisprudenza della Corte di giustizia a parametro ermeneutico essenziale in materia. Le osservazioni del Garante risultano solo parzialmente recepite;

c) l'art. 15, in materia di fatturazione elettronica e Sistema tessera sanitaria, che interviene sugli obblighi in materia di fatturazione elettronica riferiti ai soggetti tenuti all'invio dei dati al Sistema tessera sanitaria ai fini dell'elaborazione della dichiarazione dei redditi precompilata;

d) gli artt. 19 e 20, che disciplinano la cd. lotteria dei corrispettivi (o degli scontrini). In particolare, l'art. 19 (Esenzione fiscale dei premi della lotteria nazionale degli scontrini ed istituzione di premi speciali per il *cashless*) riscrive il comma 542 dell'art. 1, l. n. 232/2016 (legge di stabilità per l'anno 2017), disponendo l'istituzione di premi speciali da attribuire mediante estrazioni aggiuntive a quelle ordinarie in favore di soggetti che effettuano transazioni utilizzando strumenti di pagamento elettronici al fine di incentivarne l'utilizzo. L'art. 20 disciplina più compiutamente la lotteria prevedendo che i contribuenti, per partecipare all'estrazione, debbano comunicare all'esercente al momento dell'acquisto uno specifico "codice lotteria" (la disposizione previgente riferiva l'obbligo comunicativo al codice fiscale) che sarà individuato con provvedimento del Direttore dell'Agenzia delle dogane e dei monopoli, d'intesa con l'Agenzia delle entrate (comma 1, lett. *b*). Il consumatore potrà segnalare nella sezione dedicata del portale "Lotteria" del sito internet dell'Agenzia delle entrate la circostanza che l'esercente, al momento dell'acquisto, ha rifiutato di acquisire il codice lotteria; tali segnalazioni sono utilizzate dall'Agenzia delle entrate e dalla Guardia di finanza per le analisi del rischio di evasione;

e) l'art. 21, che aggiunge nel corpo dell'art. 5, d.lgs. 7 marzo 2005, n. 82 (Cad) i commi 2-*sexies* e 2-*septies* aventi l'obiettivo di integrare le funzionalità della piattaforma tecnologica ivi prevista (dedicata ai pagamenti con modalità informatiche) e stabilire che le regole tecniche siano emanate con decreto del Presidente del Consiglio dei ministri o del Ministro delegato per l'innovazione tecnologica e la digitalizzazione, d'intesa con il Mef e l'Agenzia delle entrate. Nel corso dei lavori di

conversione presso la Camera è stato inoltre approvato un emendamento il quale apporta modifiche all'art. 2, d.lgs. n. 127/2015, in materia di trasmissione telematica dei dati relativi ai corrispettivi, aggiungendo allo stesso il comma 5-*bis*. Tale nuova disposizione prevede che i soggetti che effettuano attività di commercio al minuto o attività assimilate (come disciplinate dall'art. 22, d.P.R. n. 633/1972), per le quali non è obbligatoria l'emissione della fattura, possano assolvere agli obblighi di memorizzazione e trasmissione telematica dei corrispettivi giornalieri all'Agenzia delle entrate mediante sistemi di incasso "evoluti" che prevedano forme di pagamento elettronico (ivi comprese carte di credito o di debito) e consentano la memorizzazione, l'inalterabilità e la sicurezza dei dati. Si demanda ad un provvedimento del Direttore dell'Agenzia delle entrate la definizione dei profili attuativi di tale disposizione, con riferimento alle informazioni da trasmettere, alle regole tecniche e ai termini per la trasmissione telematica dei dati. Dovranno inoltre essere definite le caratteristiche tecniche dei sistemi evoluti di incasso per garantire sicurezza e inalterabilità dei dati. Nella già citata memoria scritta depositata in Commissione, il Presidente del Garante ha osservato che, in ragione della particolare rilevanza del flusso informativo in questione e dell'esigenza di assicurare la piena conformità di tali trattamenti alla disciplina di protezione dei dati, sarebbe stato opportuno precisare quantomeno il ruolo assunto dal gestore della piattaforma e le caratteristiche del trattamento che si intende disciplinare in relazione ai processi di certificazione fiscale, a fini di fatturazione elettronica, di memorizzazione e trasmissione dei corrispettivi giornalieri. Su tali aspetti, il Garante avrà comunque modo di esprimersi in occasione del parere da rendere sul provvedimento di attuazione;

f) l'art. 29, relativo al potenziamento dei controlli in materia di giochi, che prevede la figura del cd. agente sotto copertura al fine di prevenire il gioco da parte dei minori, impedire l'esercizio abusivo del gioco con vincita in denaro e contrastare l'evasione fiscale e l'uso di pratiche illegali in elusione del monopolio pubblico del gioco;

g) l'art. 51, che contiene disposizioni sulle attività informatiche in favore di organismi pubblici, prevedendo che, al fine di favorire la sinergia fra istituzioni pubbliche nel campo dell'*Information and Communication Technology* (ICT), la società di gestione del sistema informativo dell'amministrazione finanziaria possa offrire servizi informatici strumentali ad alto contenuto tecnologico per il raggiungimento degli obiettivi propri delle p.a. e delle società pubbliche da esse controllate;

h) l'art. 57-*bis*, in materia di Tari, che prevede che l'Arera assicuri agli utenti domestici del servizio di gestione integrato dei rifiuti urbani e assimilati in condizioni economico-sociali disagiate l'accesso a condizioni tariffarie agevolate alla fornitura del servizio. Gli utenti beneficiari sono individuati in analogia ai criteri utilizzati per i *bonus* sociali relativi all'energia elettrica, al gas e al servizio idrico integrato (comma 2). Di particolare interesse è il comma 5 il quale prevede che, a decorrere dal 1° gennaio 2021, i *bonus* sociali per la fornitura dell'energia elettrica e del gas naturale e le agevolazioni relative al servizio idrico integrato siano riconosciuti automaticamente a tutti i soggetti il cui Isee in corso di validità sia ricompreso entro i limiti stabiliti dalla legislazione vigente. L'Arera definirà con propri provvedimenti le modalità di trasmissione delle informazioni utili da parte dell'Inps al Sistema informativo integrato gestito da Acquirente unico s.p.a., nonché le modalità di condivisione delle informazioni relative agli aventi diritto ai *bonus* tra il Sistema informativo integrato e il Sistema di gestione delle agevolazioni sulle tariffe energetiche.

Contrasto del riciclaggio

6) Il decreto legislativo 4 ottobre 2019, n. 125, recante modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonché attuazione della direttiva (UE) 2018/843 che modifica

2

la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE. Il decreto legislativo contiene le integrazioni e le modifiche che si sono rese necessarie al fine di recepire le osservazioni formulate dalla Commissione europea nell'ambito della procedura di infrazione (n. 2019/2042) con la quale è stato formalmente contestato all'Italia il non completo recepimento della direttiva (UE) 2015/849 (cd. IV direttiva antiriciclaggio); il decreto contiene anche le disposizioni necessarie ad assicurare il recepimento della direttiva (UE) 2018/843 (cd. V direttiva antiriciclaggio). Tra le disposizioni di interesse si segnalano in particolare l'art.1, comma 1, lett. *i*), il quale, integrando con un nuovo comma (6-*bis*) l'art. 2, d.lgs. 21 novembre 2007, n. 231, esplicita che il trattamento dei dati personali effettuato in applicazione della normativa antiriciclaggio è considerato di interesse pubblico nell'ambito delle garanzie previste dal RGPD e della relativa normativa nazionale di attuazione; l'art. 2, comma 3, lett. *a*), che, nell'apportare modifiche all'art. 39, comma 1, del predetto d.lgs. n. 231/2007, prevede che in relazione al trattamento di dati personali connesso alle attività di segnalazione e comunicazione antiriciclaggio, i diritti di cui agli artt. da 15 a 18 e da 20 a 22 del RGPD si esercitano nei limiti previsti dall'art. 2-*undecies* del Codice. Infine, sempre all'art. 2, comma 1, si segnalano la lett. *b*), n. 1, in tema di identità digitale e le lettere da *f*) a *i*) che, nel modificare il decreto legislativo n. 231/2007, intervengono, nella sostanza, sul regime di accessibilità alle informazioni contenute nel Registro della titolarità effettiva delle imprese prevedendone l'accesso libero. A tal fine, l'art. 2, comma 1, lett. *h*), n. 5) del decreto prevede il parere del Garante sul decreto del Mef che dovrà stabilire le modalità di consultazione del predetto Registro. Sullo schema di decreto legislativo il Garante ha reso parere il 24 luglio 2019, n. 150 (doc. web n. 9126288: cfr. parr. 3.1.2 e 14.2).

Perimetro di sicurezza nazionale cibernetica

7) Il decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, che istituisce il cd. perimetro di sicurezza nazionale cibernetica (art. 1) al fine di assicurare la sicurezza di reti, sistemi informativi e servizi informatici il cui danneggiamento arrecherebbe pregiudizio alla sicurezza nazionale, allo svolgimento di funzioni o alla prestazione di servizi. Per quanto di interesse sotto il profilo della protezione dei dati personali, giova ricordare che l'art. 27, comma 1, lett. *h*), d.l. 30 dicembre 2019, n. 162 (cd. Milleproroghe), ha modificato l'art. 1, comma 6, lett. *c*), d.l. n. 105/2019, consentendo alla Presidenza del Consiglio dei ministri e al Mise di svolgere attività di ispezione e verifica anche tramite l'accesso, se necessario, a dati o metadati personali e amministrativi nel rispetto di quanto previsto dal RGPD. Il decreto n. 105/2019 demanda ad un d.P.C.M. l'individuazione dei soggetti inclusi in tale perimetro, tra i quali quelli necessari per l'esercizio di una funzione essenziale dello Stato o per l'assolvimento di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali, nonché quelli il cui malfunzionamento, interruzione o uso improprio potrebbero pregiudicare la sicurezza nazionale (art. 2). Il decreto contiene altresì norme in materia di reti di telecomunicazione elettronica a banda larga (art. 3) nonché di infrastrutture e tecnologie critiche (art. 4). Infine, in caso di "rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici", l'art. 5 attribuisce al Presidente del Consiglio dei ministri, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, il potere di disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti. Ciò per il tempo strettamente necessario all'eliminazione del rischio e secondo un criterio di proporzionalità.

8) Il decreto-legge 3 settembre 2019, n. 101, recante disposizioni urgenti per la tutela del lavoro e per la risoluzione di crisi aziendali, convertito, con modificazioni, dalla legge 2 novembre 2019, n. 128, il quale prevede una serie di interventi in materia di tutela dei lavoratori, di assunzioni, di indicatore della situazione economica equivalente (Isee) e di risoluzione di crisi aziendali. Di particolare interesse sono le norme dirette a garantire tutele lavoristiche ai cd. *riders*, contenute nell'art. 1 che apporta modifiche al decreto legislativo n. 81/2015 in materia di contratti di lavoro (introducendo un nuovo art. 2-*bis*, "Ampliamento delle tutele in favore degli iscritti alla gestione separata" e un nuovo Capo V-*bis*, "Tutela del lavoro tramite piattaforme digitali"). In sostanza, il decreto assoggetta alla disciplina dei rapporti di lavoro subordinato anche quei rapporti di collaborazione che si concretano in prestazioni di lavoro prevalentemente personali e le cui modalità di esecuzione sono organizzate dal committente anche con riferimento ai tempi e al luogo di lavoro (art. 1, comma 1, lett. *b*). L'art. 1, comma 2, lett. *c*), invece, nell'inserire nel decreto legislativo n. 81/2015 il nuovo Capo V-*bis*, introduce norme in materia di livelli minimi di tutela per i "lavoratori autonomi che svolgono attività di consegna di beni per conto altrui, in ambito urbano e con l'ausilio di velocipedi o veicoli a motore […] attraverso piattaforme anche digitali" (art. 47-*bis*), forma contrattuale e informazioni (art. 47-*ter*), compenso da definire tramite contrattazione collettiva (art. 47-*quater*). Tale nuovo Capo reca infine alcune disposizioni frutto delle proficue interlocuzioni intercorse tra l'Autorità e i competenti uffici del Ministero del lavoro con riferimento al divieto di discriminazioni (art. 47-*quinquies*) e al rispetto delle norme in materia di protezione dei dati personali (art. 47-*sexies*).

Legge di delegazione europea

9) La legge 4 ottobre 2019, n. 117, contenente delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea (cd. legge di delegazione europea 2018), che regola la partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea. Tra le direttive di cui viene disposto il recepimento se ne segnalano due di interesse: la direttiva (UE) 2017/2108 che modifica la direttiva 2009/45/CE, relativa alle disposizioni e norme di sicurezza per le navi da passeggeri (art. 17) e la direttiva (UE) 2017/2109, che modifica la direttiva 98/41/CE del Consiglio, relativa alla registrazione delle persone a bordo delle navi da passeggeri che effettuano viaggi da e verso i porti degli Stati membri della Comunità e la direttiva 2010/65/UE, relativa alle formalità di dichiarazione delle navi in arrivo e/o in partenza da porti degli Stati membri (art. 18).

Norme in materia di sicurezza pubblica

10) Il decreto-legge 14 giugno 2019, n. 53, recante disposizioni urgenti in materia di ordine e sicurezza pubblica (cd. decreto sicurezza *bis*), convertito con modificazioni dalla legge 8 agosto 2019, n. 77, che reca disposizioni per il contrasto all'immigrazione illegale, il potenziamento dell'efficacia dell'azione amministrativa a supporto delle politiche di sicurezza e il contrasto alla violenza in occasione di manifestazioni sportive. Di interesse sotto il profilo della protezione dei dati personali è l'art. 9 che ha ripristinato la vigenza – fino al 31 dicembre 2019 – dell'art. 57 del Codice sul trattamento dei dati effettuato dal Ced del Dipartimento di pubblica sicurezza del Ministero dell'interno e da organi, uffici o comandi di polizia, per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. La sua abrogazione era stata infatti prevista dall'art. 49, d.lgs. n. 51/2018, a far data da un anno dall'entrata in vigore di tale decreto legislativo: quindi dall'8 giugno 2019. Sulla base di tale disposizione il Ministero dell'interno ha redatto uno schema di regolamento su cui il Garante ha reso il proprio parere (provv. 6 maggio 2019, n. 110, doc. web n. 9116046: cfr. par. 3.1.4). Rilevante anche l'art. 5 di modifica del Testo unico delle leggi di pubblica sicurezza (Tulps)

2

in materia di soggiorni di breve durata, concernente le comunicazioni alle questure dei dati identificativi relativi alle persone alloggiate da parte dei titolari di strutture ricettive (alberghi, pensioni, *bed & breakfast*, ecc.).

Videosorveglianza all'interno delle sale destinate a pubblico spettacolo

11) Il decreto-legge 28 giugno 2019, n. 59, recante misure di sostegno del settore del cinema e audiovisivo e finanziamento delle attività del Ministero per i beni e le attività culturali, convertito, con modificazioni, dalla legge 8 agosto 2019, n. 81, che, oltre a dettare norme di specifica competenza del predetto Ministero, prevede la possibilità di installare sistemi di videosorveglianza all'interno delle sale destinate a pubblico spettacolo, in seguito ad apposita autorizzazione e con le modalità definite dal Garante. L'art. 1, comma 4-*ter*, interpolando il comma 2 dell'art. 85-*bis*, Tulps, attribuisce infatti all'Autorità il compito di indicare, con provvedimento di carattere generale ai sensi dell'art. 2-*quinquiesdecies* del Codice, le modalità di utilizzo dei sistemi di videosorveglianza, finalizzati a individuare chi effettua abusivamente registrazioni in locali di pubblico spettacolo. I dati acquisiti per effetto dell'autorizzazione del Garante sono criptati e conservati per un periodo massimo di trenta giorni decorrenti dalla data della registrazione con modalità atte a garantirne la sicurezza e la protezione da accessi abusivi. L'accesso alle registrazioni dei sistemi di cui al presente comma è vietato, salva la loro acquisizione su iniziativa della polizia giudiziaria o del pubblico ministero.

"Codice rosso" e *revenge porn*

12) La legge 19 luglio 2019, n. 69, che, apportando modifiche al codice penale e al codice di procedura penale, reca disposizioni dirette a rafforzare le tutele disposte dall'ordinamento per le vittime di violenza domestica e di genere e velocizzare l'adozione degli opportuni provvedimenti di protezione (cd. codice rosso). In particolare si prevede l'utilizzo del braccialetto elettronico per garantire il rispetto della misura cautelare del divieto di avvicinamento ai luoghi frequentati dalla persona offesa (art. 15). Di particolare interesse sotto il profilo della tutela della riservatezza è l'art. 10 della legge che introduce il "delitto di diffusione illecita di immagini o video sessualmente espliciti" (cd. *revenge porn*: art. 612-*ter* c.p.). La versione originaria del disegno di legge governativo non conteneva norme in materia di diffusione illecita di video sessualmente espliciti, disciplina invece contenuta in autonomi disegni di legge (ex *multis*, AS 1076, recante misure per il contrasto della diffusione non autorizzata di materiale sessualmente esplicito, abbinato agli atti nn. 1166 e 1134). Tale previsione è il frutto dell'emendamento n. 1.500 della Commissione giustizia della Camera, presentato in Assemblea con il parere favorevole della stessa Commissione e del governo, e approvato all'unanimità. Il nuovo art. 612-*ter* c.p. sanziona la condotta di chi pubblica o diffonde immagini o video sessualmente espliciti, originariamente destinati a rimanere privati, senza l'espresso consenso delle persone ritratte. La norma punisce inoltre la condotta di chi, avendoli ricevuti, ulteriormente condivide e diffonde i predetti video o immagini. Il reato è dunque volto a colpire il fenomeno del cd. *revenge porn*, ossia la divulgazione non consensuale, spesso associata a finalità vendicative, di immagini relative alla vita sessuale della vittima.

Decreto crescita

13) Il d.l. 30 aprile 2019, n. 34, recante misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi (cd. decreto crescita), convertito dalla legge 28 giugno 2019, n. 58. Tra le disposizioni di interesse per i riflessi sulla protezione dei dati personali si segnalano in particolare:

a) l'art. 12-*quinquies*, comma 2, relativo alla trasmissione telematica dei dati dei corrispettivi, che modifica la disciplina della cd. lotteria degli scontrini, introdotta dalla legge di bilancio 2017, disponendo un innalzamento della probabilità di vincita dei premi se le transazioni sono effettuate attraverso strumenti che consentano il pagamento con carta di debito e di credito (con riferimento al tema della lotteria degli scontrini, si veda anche l'art. 20 del decreto fiscale, al punto 4 del presente paragrafo);

b) l'art. 13-*quater*, commi 4 e 5, sul contrasto all'evasione nel settore turistico che – al fine di migliorare la qualità dell'offerta turistica e contrastare forme irregolari di ospitalità, anche ai fini fiscali – prevede l'istituzione di una apposita banca dati delle strutture ricettive e degli immobili destinati alle locazioni brevi, presenti nel territorio nazionale, identificati mediante un codice alfanumerico, (cd. codice identificativo), da utilizzare in ogni comunicazione inerente all'offerta e alla promozione dei servizi all'utenza. Le norme per la realizzazione e la gestione della banca dati, compresi i dispositivi per la sicurezza e la riservatezza dei dati, le modalità di accesso e la messa a disposizione delle informazioni in essa contenute agli utenti e alle autorità preposte ai controlli e per la conseguente pubblicazione nel sito internet istituzionale del Ministero oltre che i criteri che determinano la composizione del suddetto codice identificativo, si prevede che vengano individuate con decreto del Ministro delle politiche agricole alimentari e forestali. Il medesimo, al comma 6, affida a un altro decreto del Ministro delle politiche agricole, sentiti il Direttore dell'Agenzia delle entrate e il Garante, il compito di definire le modalità applicative per l'accesso da parte dell'Agenzia delle entrate ai dati relativi al predetto codice identificativo;

c) l'art. 18-*ter*, recante al comma 1 l'istituzione, presso il Mise, di una piattaforma telematica, denominata "Incentivi.gov", finalizzata al sostegno della politica industriale e della competitività del Paese. Nel medesimo articolo viene inoltre prevista l'istituzione di una struttura di cooperazione interorganica finalizzata a garantire il monitoraggio periodico delle informazioni che confluiscono nella piattaforma telematica. La struttura in questione, ai sensi del comma 5, definisce proposte per l'ottimizzazione della piattaforma digitale, predispone le regole tecniche per l'accesso e le modalità per la condivisione dei dati nel rispetto delle disposizioni contenute nel Cad e nel rispetto delle regole di sicurezza e trattamento dei dati di cui al RGPD e del decreto legislativo n. 101/2018;

d) l'art. 36, comma 2-*octies*, che prevede l'avvio di sperimentazioni relative alle attività di tecnofinanza (*FinTech*) volte al perseguimento, mediante nuove tecnologie, dell'innovazione di servizi e di prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati. Per tali fini viene prevista l'istituzione, presso il Mef, del "Comitato *FinTech*" al quale partecipa, quale membro permanente, anche il Garante;

e) l'art. 43 (rubricato semplificazione degli adempimenti per la gestione degli enti del Terzo settore), il quale prevede alcune modifiche all'art. 1, l. 19 gennaio 2019, n. 3, recante misure per il contrasto dei reati contro la p.a., nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici (v. *infra* n. 18). In particolare, la disposizione inserisce nell'art. 1, l. n. 3/2019, il comma 26-*bis*, il quale dispone che al fine di consentire i controlli previsti dalle norme di legge, la Commissione di garanzia degli statuti e per la trasparenza ed il controllo dei rendiconti dei partiti e dei movimenti politici può accedere alle banche dati gestite dalle amministrazioni pubbliche o da enti che, a diverso titolo, sono competenti nella materia elettorale o che esercitino funzioni nei confronti dei soggetti equiparati ai partiti e ai movimenti politici. Per i medesimi fini e per l'esercizio delle funzioni istituzionali della Commissione possono essere predisposti protocolli d'intesa con i citati enti o amministrazioni.

Contrasto dell'assenteismo nella p.a.

14) La legge 19 giugno 2019, n. 56, recante interventi per la concretezza delle azioni delle p.a. e il contrasto dell'assenteismo, mira a individuare soluzioni per garantire l'efficienza delle p.a., il miglioramento dell'organizzazione amministrativa e l'incremento della qualità dei servizi erogati dalle stesse in un'epoca di trasformazione digitale. Di particolare interesse sotto il profilo della protezione dei dati per-

2

sonali è l'art. 2 che, al fine di eliminare o comunque ridurre il deprecabile fenomeno delle false attestazioni di presenza in servizio, prevede l'applicazione generalizzata di sistemi di rilevazione delle presenze basati su sistemi di verifica biometrica dell'identità e su apparati di videosorveglianza. L'introduzione dei suddetti sistemi è prevista, obbligatoriamente e in maniera cumulativa, in sostituzione di quelli di rilevazione automatica attualmente in uso. Per rendere la legge pienamente applicabile saranno necessari più decreti attuativi: sotto quest'ultimo profilo, infatti, le modalità attuative dei sistemi di verifica biometrica dell'identità e di videosorveglianza sono demandate a un decreto del Presidente del Consiglio dei ministri e al riguardo uno schema di regolamento è stato già sottoposto al parere del Garante che si è espresso con provvedimento 19 settembre 2019, n. 167 (doc. web n. 9147290; cfr. parr. 3.1.4 e 13.12). Disposizioni specifiche sono dettate poi per il comparto scuola. Infatti il comma 4 dell'art. 2 prevede che il personale docente ed educativo degli istituti e delle scuole di ogni ordine e grado e delle istituzioni educative è escluso dall'ambito di applicazione di detto articolo e che, invece, i dirigenti dei medesimi istituti, scuole e istituzioni "sono soggetti ad accertamento esclusivamente ai fini della verifica dell'accesso", secondo modalità stabilite con decreto avente natura regolamentare del Ministro per la pubblica amministrazione, da adottare di concerto con il Ministro dell'istruzione, dell'università e della ricerca, previo parere del Garante, nel rispetto dell'art. 9 del RGPD e delle misure di garanzia definite dal Garante ai sensi dell'art. 2-*septies* del Codice. La legge, quindi, non individua la tecnologia da impiegare per attuare le misure previste dall'art. 2, in particolare per quanto riguarda i dati biometrici, ma demanda la definizione delle modalità attuative delle norme, rispettivamente, ad un decreto del Presidente del Consiglio dei ministri e a un decreto ministeriale, in entrambi i casi, previo parere del Garante. Sullo schema del disegno di legge governativo, approvato dal Consiglio dei ministri in via definitiva il 25 ottobre 2018, il Garante aveva espresso parere in data 11 ottobre 2018, n. 464 (doc. web n. 9147290) svolgendo alcune osservazioni e indicando una serie di cautele al fine di assicurare la conformità dei trattamenti ai principi di liceità, di proporzionalità e di minimizzazione dei dati (cfr. Relazione 2018, par. 3.3.1, p. 29). In particolare, il Garante aveva ritenuto assolutamente sproporzionata l'introduzione sistematica e generalizzata di sistemi di rilevazione delle presenze, tramite dati biometrici e al tempo stesso a mezzo ripresa attraverso videocamere, considerando l'invasività di queste forme di verifica e la delicatezza dei dati in questione. L'Autorità aveva perciò indicato una serie di correttivi, chiedendo che venisse evitato l'impiego simultaneo di sistemi di rilevazione di dati biometrici e di sistemi di videosorveglianza; che l'adozione delle nuove tecnologie avvenisse solo qualora altri sistemi di rilevazione non risultassero adeguati; che l'adozione di queste tecnologie fosse legata a specifici fattori di rischio o di particolari presupposti, quali, ad esempio, le dimensioni dell'ente, il numero dei dipendenti coinvolti, situazioni di criticità determinate anche dal contesto ambientale in cui si trova ad operare una p.a. Le osservazioni del Garante non sono state recepite dal Governo, il quale si è limitato a dare seguito alla sola richiesta di sostituire la locuzione "sistemi di identificazione biometrica" con la dicitura "sistemi di verifica biometrica dell'identità" che, più correttamente, si riferisce alle verifiche effettuate *one to one*. Nel corso dell'esame parlamentare del disegno di legge, vista la delicatezza della materia, sia il Senato che la Camera hanno ritenuto necessario tenere un'audizione con il Presidente del Garante che, nell'occasione, ha ribadito le criticità già evidenziate nel parere (audizioni tenutesi rispettivamente in data 27 novembre 2018, Commissione 11ª Lavoro pubblico e privato, previdenza sociale del Senato e 6 febbraio 2019, Commissioni riunite Affari costituzionali e Lavoro della Camera – cfr. par. 3.1.1).

Il Presidente ha espresso una serie di rilievi critici in merito all'introduzione di sistemi di controllo biometrici sui lavoratori, sottolineando come la previsione dell'obbligatorio impiego contestuale di due sistemi di verifica del rispetto delle presenze in servizio (raccolta di dati biometrici e videosorveglianza) ecceda i limiti imposti dalla stretta necessità del trattamento rispetto al fine perseguito. Sul punto il Garante ha evidenziato che se "presupposto per l'introduzione di un sistema di attestazione della presenza in servizio così invasivo quale quello biometrico è la sua ritenuta efficacia e affidabilità, ne consegue necessariamente l'ultroneità del ricorso contestuale alla videosorveglianza, che nulla potrebbe aggiungere in termini di contrasto di fenomeni elusivi". Inoltre, sotto un diverso profilo il Garante ha giudicato non conforme al canone di proporzionalità, come declinato dalla giurisprudenza europea, l'introduzione sistematica, generalizzata e indifferenziata per le p.a. di sistemi di rilevazione delle presenze tramite identificazione biometrica, in relazione ai vincoli posti dall'ordinamento europeo sul punto a fronte dell'invasività di tali forme di verifica e delle implicazioni derivanti dalla particolare natura del dato. Il Garante ha dunque sottolineato come per "realizzare il condivisibile fine del contrasto dell'assenteismo e della falsa attestazione della presenza in servizio dovrebbe […] farsi previo ricorso a misure meno limitative del diritto alla protezione dei dati, utilizzando i sistemi di rilevazione biometrica, in presenza di fattori di rischio specifici, qualora soluzioni meno invasive debbano ragionevolmente ritenersi inidonee allo scopo". In seguito alle audizioni sono stati presentati alla Camera numerosi emendamenti parlamentari che, al fine di mitigare i rischi paventati dal Garante, prevedevano: la facoltatività dell'introduzione dei sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi; la sostituzione della "verifica biometrica dell'identità" con la previsione di un riferimento esplicito al trattamento biometrico delle impronte digitali; la previsione dell'alternatività tra i sistemi biometrici e la videosorveglianza; il richiamo al rispetto del principio di proporzionalità di cui all'art. 52 della Carta di Nizza. Di tutti ne è stato approvato solo uno, che ha così introdotto nell'art. 2 della legge un espresso riferimento al rispetto del principio di proporzionalità previsto dall'art. 52 della Carta europea dei diritti (la norma già conteneva comunque un rinvio al principio di proporzionalità previsto dal RGPD). Come anticipato, il Garante nel settembre scorso ha reso parere sullo schema di regolamento d'attuazione, ribadendo in particolare come la previsione dell'obbligatorio impiego contestuale di due sistemi di verifica del rispetto dell'orario di lavoro (raccolta di dati biometrici e videosorveglianza) contrasti con l'esigenza di stretta necessità del trattamento rispetto al fine perseguito; esigenza tanto più rilevante rispetto ai dati biometrici, annoverati nella categoria di dati personali cui la disciplina europea accorda maggiore tutela. L'utilizzo contestuale dei due sistemi di attestazione della presenza in servizio risulta incompatibile con il canone di proporzionalità di cui all'art. 52 della suddetta Carta oltre che agli artt. 5, par. 1, lett. *c*), e – relativamente ai dati biometrici – 9, par. 2, lett. *b*) e *g*), del RGPD. Per altro verso, l'Autorità ha ribadito nel parere la non conformità della disposizione a tali principi laddove intenda configurare la rilevazione biometrica (unitamente peraltro alle videoriprese) quale obbligatoria in ogni p.a.

Finanziamento di sistemi di videosorveglianza nelle scuole dell'infanzia e in strutture per anziani

15) Il decreto-legge 18 aprile 2019, n. 32, recante disposizioni urgenti per l'accelerazione degli interventi infrastrutturali, di rigenerazione urbana e di ricostruzione a seguito di eventi sismici (cd. sblocca cantieri) convertito dalla legge 14 giugno 2019, n. 55, fra le cui disposizioni di interesse, si segnala l'art. 5-*septies* (sistemi di videosorveglianza a tutela dei minori e degli anziani), che prevede l'istituzione di un fondo di 5 milioni di euro per l'anno 2019 "finalizzato all'erogazione a favore di ciascun comune delle risorse finanziarie occorrenti per l'installazione di sistemi di

2

videosorveglianza a circuito chiuso", sia nelle scuole dell'infanzia sia nelle strutture socio-sanitarie e socio-assistenziali per anziani e persone con disabilità. Lo stanziamento di tali fondi assicura le risorse necessarie per realizzare le finalità previste dal disegno di legge in corso di esame in Parlamento, recante misure per prevenire e contrastare condotte di maltrattamento o di abuso, anche di natura psicologica, in danno dei minori negli asili nido e nelle scuole dell'infanzia e delle persone ospitate nelle strutture socio-sanitarie e socio-assistenziali per anziani e persone con disabilità, nel corso dei cui lavori parlamentari il Garante ha tenuto un'audizione il 2 ottobre 2018 (cfr. Relazione 2018, par. 3.1, p. 28) alla quale ha fatto seguito quella del 30 gennaio 2019 (cfr. audizione informale del Presidente del Garante sul d.d.l. n. 897 e connessi: prevenzione di maltrattamenti a danno di minori, anziani e disabili nelle strutture pubbliche e private: doc. web n. 9081548). Di interesse risulta inoltre l'art. 28 che, mediante l'inserimento al comma 1 dell'art. 1, d.lgs. 1° agosto 2003, n. 259, recante codice delle comunicazioni elettroniche, di alcune disposizioni (lett. da ee-*bis*) a ee-*sexies*) prevede un sistema di allarme pubblico agli utenti finali interessati da gravi emergenze e catastrofi imminenti o in corso; sistema che può utilizzare servizi mobili di comunicazione interpersonale basati sul numero di telefono, servizi di diffusione radiotelevisiva, applicazioni mobili basate su un servizio di accesso a internet, prevedendo anche un servizio di *Cell broadcast service* che consente alla Protezione civile la diffusione di messaggi cd. IT-*alert* a tutti i terminali presenti all'interno di una determinata area geografica individuata dalla copertura radiomobile di una o più celle. Il comma 2 dell'art. 28 prevede che con d.P.C.M., di concerto con il Mise, sentiti il Garante e l'Agcom, vengano individuate le modalità e i criteri di attivazione del suddetto servizio IT-*alert*, da realizzarsi secondo gli standard applicabili; le modalità di definizione dei contenuti e di gestione della richiesta di attivazione dei messaggi IT-*alert*; i criteri e le modalità da utilizzare al fine di garantire che l'utilizzo e il trattamento dei dati eventualmente raccolti nell'ambito del funzionamento del sistema IT-*alert* avvenga nel rispetto della normativa in materia di protezione dei dati personali e che sia escluso l'utilizzo dei medesimi dati per finalità diverse.

Legge europea

16) La legge 3 maggio 2019, n. 37, recante disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - legge europea 2018. Tra le disposizioni di interesse si segnala in particolare l'art. 1, il quale, nell'ambito delle disposizioni in materia di riconoscimento delle qualifiche professionali, prevede alla lett. *e*) che le autorità interne competenti devono prestare piena collaborazione con i centri di assistenza degli Stati membri ospitanti – centri che forniscono l'assistenza necessaria in favore dei cittadini europei che intendano ottenere il riconoscimento di una qualifica professionale nello Stato ospitante – e, se richiesto, devono trasmettere ai medesimi centri tutte le informazioni pertinenti ai singoli casi, fatte salve le disposizioni in materia di protezione dei dati personali. Di interesse è inoltre l'art. 15, recante la delega per l'attuazione della direttiva (UE) 2017/1564 relativa a taluni utilizzi consentiti di determinate opere e di altro materiale protetto da diritto d'autore e da diritti connessi a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa; la disposizione aggiunge all'art. 71-*bis*, l. 22 aprile 1941, n. 633 (legge sul diritto d'autore) il comma 2-*undecies*, il quale dispone che, nel rispetto delle disposizioni vigenti in materia di trattamento dei dati personali, le entità autorizzate stabilite nel territorio dello Stato – vale a dire, ai sensi dell'art. 2-*sexies*, entità, pubbliche o private, riconosciute o autorizzate secondo le norme vigenti a fornire ai beneficiari, senza scopo di lucro, istruzione, formazione, possibilità di lettura adattata o accesso alle informazioni – devono: a) distribuire, comunicare e rendere disponibili le

copie in formato accessibile unicamente ai beneficiari o ad altre entità autorizzate; b) "prendere opportune misure per prevenire la riproduzione, la distribuzione, la comunicazione al pubblico o la messa a disposizione del pubblico non autorizzate delle copie in formato accessibile;" [*sic*] c) prestare la dovuta diligenza nel trattare le opere o altro materiale e le relative copie in formato accessibile e nel registrare tutte le operazioni effettuate; d) pubblicare e aggiornare, se del caso nel proprio sito web, o tramite altri canali *online* o *offline*, informazioni sul modo in cui le entità autorizzate rispettano gli obblighi descritti.

Reddito di cittadinanza

17) Il decreto-legge 28 gennaio 2019, n. 4, recante disposizioni urgenti in materia di reddito di cittadinanza e di pensioni, convertito dalla legge 28 marzo 2019, n. 26, del quale rileva particolarmente, per i profili di protezione dei dati, il Capo I (artt. 1-13), volto a realizzare un primo livello di tutela mediante l'introduzione del reddito di cittadinanza (Rdc) quale misura sociale ed economica preordinata a realizzare una ridefinizione del modello di benessere collettivo con un minimo di sussistenza ed incentivare la scelta di un lavoro (in tema v. anche par. 4.2.1). In particolare, l'art. 2 prevede la tipologia dei beneficiari del Rdc ed i relativi requisiti per accedere al beneficio economico che è riconosciuto per un periodo continuativo non superiore a diciotto mesi. L'art. 5 stabilisce le modalità di erogazione del beneficio prevedendo che il Rdc possa essere richiesto presso il gestore del servizio integrato (Poste italiane s.p.a.) o presso i centri di assistenza fiscale (Caf) utilizzando un modello di domanda reso disponibile in un provvedimento dell'Inps che rimanda alla corrispondente dichiarazione sostitutiva unica (Dsu) a fini Isee, a cui la domanda è successivamente associata dall'Inps. Il Rdc viene riconosciuto dall'Inps, che potrà acquisire dall'Anagrafe tributaria, dal Pubblico registro automobilistico e da altre amministrazioni pubbliche, le informazioni rilevanti ai fini del suddetto riconoscimento (art. 5, comma 3). L'art. 6 prevede poi l'istituzione di due apposite piattaforme digitali dedicate al Rdc al fine di attivare e gestire i Patti per il lavoro e i Patti per l'inclusione sociale. Si tratta di una piattaforma che si inserisce nel Sistema informativo unitario delle politiche del lavoro (Siupl) per il coordinamento dei centri per l'impiego e di un'altra piattaforma che si inserisce nel Sistema informativo unitario dei servizi sociali (Siuss) per il coordinamento dei comuni. Le piattaforme rappresentano strumenti di condivisione delle informazioni sia tra le amministrazioni centrali e i servizi territoriali sia, nell'ambito dei servizi territoriali, tra i centri per l'impiego e i servizi sociali. Altre disposizioni riguardano le modalità operative delle citate piattaforme che costituiranno il portale delle comunicazioni dai centri per l'impiego, dai soggetti accreditati e dai comuni all'Agenzia nazionale per le politiche attive del lavoro (Anpal), al Ministero del lavoro e delle politiche sociali e all'Inps. L'art. 7 dispone che i centri per l'impiego e i comuni comunichino alle piattaforme, al fine della messa a disposizione dell'Inps, le informazioni sui fatti suscettibili di dar luogo a sanzioni (art. 7, comma 12). L'Inps a sua volta, per il tramite delle piattaforme, mette a disposizione dei centri per l'impiego e dei comuni gli eventuali conseguenti provvedimenti di decadenza dal beneficio. L'art. 10 prevede che il Ministero del lavoro e delle politiche sociali sia responsabile del monitoraggio del Rdc e debba predisporre, sulla base delle informazioni fornite dall'Inps e dall'Anpal, nonché delle altre informazioni disponibili in materia rilevate anche dalle piattaforme digitali, il rapporto annuale sull'attuazione del Rdc da pubblicare sul sito internet istituzionale. L'art. 11, comma 2, infine, reca modifiche alla disciplina dell'Isee e, in un'ottica di semplificazione, subordina la precompilazione della Dsu alla manifestazione del consenso (revocabile in ogni tempo) che ogni componente il nucleo familiare, se maggiorenne, potrà manifestare presso le sedi Inps, sul sito dell'Istituto o dell'Agenzia e presso i Caf (cfr. il nuovo comma 2-*bis*

dell'art. 10, d.lgs. n. 147/2017). Si prevede, inoltre, che anche in contrasto con la predetta manifestazione di volontà dell'interessato, in caso di presentazione della Dsu in modalità cartacea da parte di un componente il nucleo familiare, debbano comunque essere restituite al dichiarante (e quindi anche al Caf) al momento del rilascio dell'attestazione Isee, informazioni di dettaglio relative a eventuali omissioni o difformità riscontrate negli archivi dell'Inps e dell'Agenzia delle entrate, di tutti i componenti il nucleo familiare, incluse quelle relative ai saldi e alle giacenze medie del patrimonio mobiliare (cfr. nuovo comma 2-*ter* dell'art. 10, d.lgs. n. 147/2017). Nel corso dell'esame parlamentare del provvedimento, il Garante ha depositato presso le competenti Commissioni di Camera e Senato il 19 febbraio 2019 (Commissione Lavoro pubblico e privato, previdenza sociale del Senato) e il 6 marzo 2019 (Commissioni riunite Lavoro pubblico e privato e Affari sociali della Camera) una memoria scritta nella quale ha evidenziato numerose criticità. Esse riguardano, tra l'altro, talune previsioni generiche inidonee a definire con sufficiente chiarezza le modalità di svolgimento delle procedure di consultazione e verifica delle varie banche dati; la disciplina del "monitoraggio" sull'utilizzo della carta Rdc; le disposizioni sul rilascio delle attestazioni Isee (suscettibili di pregiudicare la sicurezza dei dati contenuti nell'Anagrafe tributaria e, soprattutto, nell'Archivio dei rapporti finanziari dell'Agenzia delle entrate); infine, l'architettura del sito web del Governo dedicato al Rdc. Nel corso dell'esame parlamentare del disegno di legge si sono tenuti alcuni incontri di lavoro tra rappresentanti dell'Autorità e del Ministero del lavoro, nell'ambito dei quali sono state analiticamente rappresentate le criticità presenti nel testo, già ampiamente evidenziate dal Presidente nella memoria trasmessa alle Commissioni. Le indicazioni rese nelle suddette interlocuzioni sono state in parte recepite nell'ambito di emendamenti presentati dal Governo durante l'esame del disegno di legge. La legge necessita di numerosi provvedimenti di attuazione, tra i quali – oltre a quello dell'Inps sul modello di domanda, sopra citato (art. 5, comma 1) – si segnalano: 1) il decreto del Ministro del lavoro recante le modalità del monitoraggio degli importi spesi e prelevati sulla carta Rdc da adottarsi entro 3 mesi dalla data di entrata in vigore del decreto-legge (art. 3, comma 15); 2) il decreto del Ministro del lavoro recante le modalità di presentazione della richiesta di Rdc con Dsu a fini Isee (art. 5, comma 2); 3) il provvedimento Inps recante le modalità di acquisizione dei dati da banche dati pubbliche a fini della concessione del Rdc (art. 5, comma 3); 4) il decreto del Ministro del lavoro recante il piano tecnico di attivazione ed interoperabilità delle piattaforme (art. 6, comma 1), da adottare entro 60 giorni; 5) il decreto del Ministro del lavoro sull'eventuale integrazione dell'all. A relativo a banche dati trattate dall'Inps cui può accedere l'Ispettorato del lavoro per fini di vigilanza Rdc (art. 7, comma 15-*ter*); 6) il provvedimento del Direttore dell'Ispettorato del lavoro sull'individuazione delle modalità di accesso ai dati (art. 7, comma 15-*ter*), da adottarsi entro 60 giorni; 7) il decreto del Ministro del lavoro recante l'individuazione a campione di beneficiari per valutazioni del Rdc (art. 10, comma 1-*bis*); il decreto Ministro del lavoro sulla compilazione Dsu in tema di Isee (art. 11, comma 2, lett. *d*).

Rete nazionale del registro tumori

18) La legge 22 marzo 2019, n. 29, recante l'istituzione e la disciplina della Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza nonché del referto epidemiologico per il controllo sanitario della popolazione. Più in dettaglio, gli artt. 1 e 2 prevedono l'istituzione di una Rete nazionale relativa sia ai registri dei tumori sia ai sistemi di sorveglianza, individuati ai sensi del d.P.C.M. 3 marzo 2017 con riferimento ai singoli sistemi sanitari regionali (o delle province autonome). L'art. 4 istituisce il "referto epidemiologico", che non riguarda singoli pazienti (come il termine "referto" potrebbe indurre a ritenere) ma si riferisce allo stato di salute complessivo

di una comunità. Esso è definito dal comma 2 come "il dato aggregato o macrodato corrispondente alla valutazione dello stato di salute complessivo di una comunità che si ottiene da un esame epidemiologico delle principali informazioni relative a tutti i malati e a tutti gli eventi sanitari di una popolazione in uno specifico ambito temporale e in un ambito territoriale circoscritto o a livello nazionale, attraverso la valutazione dell'incidenza delle malattie, del numero e delle cause dei decessi, come rilevabili dalle schede di dimissioni ospedaliere e dalle cartelle cliniche". La stessa disposizione demanda ad un decreto del Ministro della salute, previo parere del Garante ed intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome, l'istituzione e la disciplina del referto epidemiologico. Il decreto deve individuare i soggetti preposti alla raccolta e all'elaborazione dei dati che confluiscono nel referto epidemiologico, disciplinare il trattamento, l'elaborazione, il monitoraggio continuo e l'aggiornamento periodico dei medesimi dati e prevedere la pubblicazione, con cadenza annuale, del referto epidemiologico, "in particolare per quanto riguarda i dati relativi all'incidenza e alla prevalenza delle patologie che costituiscono più frequentemente causa di morte"; la pubblicazione è effettuata nei siti internet delle regioni e delle province autonome, alle quali spetta il controllo quantitativo e qualitativo dei flussi di dati che alimentano il referto epidemiologico.

Come fatto rilevare nella Relazione 2018 (p. 28), in sede di esame parlamentare dei disegni di legge che attengono a tale disciplina (n. 535 e abbinati), il Presidente dell'Autorità ha fatto pervenire il 15 ottobre 2018 una memoria presso la Commissione Igiene e sanità del Senato nella quale ha, tra l'altro, invitato il legislatore a definire con chiarezza l'ambito di operatività della Rete nazionale e il suo rapporto con il Registro tumori e gli altri sistemi di sorveglianza "di rilevanza nazionale" già istituiti presso il Ministero della salute (doc. web n. 9065528). Ciò, al fine di evitare la duplicazione di banche dati e archivi sanitari, in ottemperanza ai principi di proporzionalità e di *data protection by design* e *by default* previsti dal RGPD che richiedono di ridurre al minimo il trattamento di dati personali, considerata la natura, il contesto e le finalità del trattamento (v. artt. 5 e 25 del RGPD). Il Garante ha altresì sottolineato i rischi connessi alla proliferazione degli obblighi informativi in capo agli organismi sanitari e alle strutture sanitarie regionali, non solo in termini di aggravio degli oneri imposti a tali enti, ma anche di accresciuto pericolo per la riservatezza degli interessati, specie con riferimento alle esigenze di esattezza e aggiornamento dei dati.

Sostegno e semplificazione per le imprese e la p.a.

19) Il decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la p.a., convertito dalla legge 11 febbraio 2019, n. 12, del quale si segnala l'art. 8, rubricato "piattaforme digitali", rivolto a promuovere la capillare e più efficace diffusione dell'utilizzo della piattaforma digitale per i pagamenti alle pubbliche amministrazioni di cui all'art. 5, comma 2, del Cad. La disposizione prevede anche la costituzione di una società, interamente partecipata dallo Stato, che ne industrializzi lo sviluppo tecnologico e la diffusione. Sono inoltre attribuite al Presidente del Consiglio dei ministri le funzioni di indirizzo, di coordinamento e di supporto tecnico alle p.a. centrali e territoriali, al fine di assicurare la diffusione del sistema di pagamento digitale tramite la piattaforma, nonché lo sviluppo, tra l'altro, della Piattaforma digitale nazionale dati di cui all'art. 50-*ter* del Cad.

Trasparenza di partiti e movimenti politici

20) La legge 9 gennaio 2019, n. 3, che introduce misure in materia di contrasto ai reati contro la p.a., di prescrizione e di trasparenza dei partiti e dei movimenti politici e delle fondazioni, con particolare riferimento al loro finanziamento. Per quanto riguarda la disciplina di trasparenza relativa ai partiti politici, che ha un notevole impatto sulla protezione dei dati, le nuove disposizioni sono volte a raf-

2

forzare gli obblighi di trasparenza sia in ordine ai contributi ricevuti, sia alla presentazione delle candidature. In particolare si prevede, per i partiti e i movimenti politici nonché per le liste e per i candidati alla carica di sindaco che partecipano alle elezioni nei comuni con più di 15.000 abitanti, l'obbligo di annotare in un apposito registro, entro il mese successivo a quello della riscossione, rispetto ad ogni contributo ricevuto, l'identità dell'erogante, l'entità del contributo o il valore della prestazione o di altra forma di sostegno e la data dell'erogazione. Di particolare interesse sono le disposizioni che prevedono l'obbligo di pubblicare sul sito istituzionale dei partiti i dati identificativi dei sostenitori che abbiano corrisposto contributi nonché, in occasione delle competizioni elettorali, il certificato penale dei candidati. L'obbligo di trasparenza è riferito alle elargizioni di contributi in denaro complessivamente superiori nell'anno a euro 500 per soggetto erogatore, o di prestazioni o altre forme di sostegno di valore equivalente. Inoltre, in occasione di competizioni elettorali (con l'eccezione delle elezioni comunali sotto i 15.000 abitanti) è previsto per i partiti, movimenti politici e liste che si presentano alle elezioni l'obbligo di pubblicare sul proprio sito internet il *curriculum vitae* fornito dai propri candidati ed il relativo certificato penale, rilasciato dal casellario giudiziale non oltre 90 giorni prima della data fissata per le elezioni. I medesimi documenti sono pubblicati in apposita sezione denominata "Elezioni trasparenti" del sito internet dell'ente cui si riferisce la consultazione elettorale. Alcune disposizioni del provvedimento normativo sono state modificate nel corso dell'esame parlamentare in parziale conformità alle indicazioni rese dal Garante nell'audizione richiesta dalle Commissioni Affari costituzionali e Giustizia della Camera e tenuta il 10 ottobre 2018 (cfr. Relazione 2018, par. 2.3 e 3.1). In tale occasione il Presidente del Garante aveva, da un lato, richiamato il Regolamento (UE) 2014/1141 sul finanziamento dei partiti politici europei e la graduazione delle soglie oltre le quali scattano gli obblighi di pubblicazione ivi individuata e, dall'altro, espresso forti perplessità sulla generalizzata pubblicazione del certificato penale dei candidati, ritenendola sproporzionata e richiedendo perciò un raccordo tra tale previsione e la disciplina dell'incandidabilità a competizioni elettorali, con una rimodulazione dell'ampiezza della pubblicazione in ragione delle diverse caratteristiche della predetta disciplina per ciascun tipo di elezione. Tali ultime indicazioni non sono state recepite. Sotto altro profilo, mentre l'Autorità aveva richiesto di individuare termini di pubblicazione obbligatoria dei dati strettamente commisurati e non eccedenti le finalità perseguite, è stato previsto un periodo di conservazione non inferiore a 5 anni per la pubblicazione dei dati sul sito internet del partito o movimento politico che non appare assolutamente adeguato, stante peraltro la sua indeterminatezza. Quanto all'obbligo di pubblicare il *curriculum vitae* e il certificato penale dei candidati – aspetto quest'ultimo di particolare criticità – anche sul sito del Ministero dell'interno, in caso di elezione del Parlamento nazionale o dei membri del Parlamento europeo, e di quello dell'ente cui si riferisce la consultazione elettorale, l'Autorità aveva segnalato l'opportunità di stabilire, anche tramite un regolamento attuativo, modalità di assolvimento di tale obbligo con misure appropriate e specifiche finalizzate a prevedere un accesso selettivo a tali dati (con credenziali rilasciate a chiunque ne abbia interesse e dietro specifica richiesta) ed a renderli disponibili in formato protetto dal rischio di copia o alterazione, per un tempo proporzionato alle esigenze perseguite (ad es. quello della campagna elettorale). Al riguardo, il testo di legge approvato si limita a stabilire che la pubblicazione deve consentire all'elettore di accedere alle informazioni ivi riportate attraverso apposita ricerca per collegio o nominativo del candidato e demanda ad un decreto del Ministro dell'interno la definizione delle modalità tecniche di "acquisizione dei dati su apposita piattaforma informatica".

2.3. *Norme di rango secondario*

Sono stati infine pubblicati i seguenti atti di rango secondario aventi impatto sulla protezione dei dati sui cui schemi il Garante ha reso parere (cfr. par. 3.1.4):

a) decreto del Ministro della salute 10 dicembre 2019, n. 168, recante il regolamento concernente la banca dati nazionale destinata alle disposizioni anticipate di trattamento - Dat (parere 29 maggio 2019, n. 123, doc. web n. 9117770);

b) decreto del Ministro della salute 20 agosto 2019, n. 130, recante il regolamento recante disciplina degli obiettivi, delle funzioni e della struttura del Sistema informativo trapianti (Sit) e del Registro nazionale dei donatori di cellule riproduttive a scopi di procreazione medicalmente assistita di tipo eterologo (parere 30 luglio 2019, n. 158, doc. web n. 9131111);

c) decreto del Ministro dell'interno 21 agosto 2019, n. 127, recante il regolamento volto a dare attuazione alle disposizioni del d.lgs. n. 81/2008 in materia di tutela della salute e della sicurezza nei luoghi di lavoro, nell'ambito delle articolazioni centrali e periferiche della Polizia di Stato, del Dipartimento dei vigili del fuoco, del soccorso pubblico e della difesa civile, del Corpo nazionale dei vigili del fuoco, nonché delle strutture del Ministero dell'interno destinate per finalità istituzionali alle attività degli organi con compiti in materia di ordine e sicurezza pubblica (parere 19 luglio 2018, n. 423, doc. web n. 9040242);

d) d.P.R. 28 marzo 2019, n. 54, recante modifica dell'articolo 331 del decreto del Presidente della Repubblica 16 dicembre 1992, n. 495, concernente i certificati medici attestanti l'idoneità psicofisica dei conducenti di veicoli a motore (parere 15 febbraio 2018, n. 78, doc. web n. 8043000).

3 I rapporti con il Parlamento e le altre Istituzioni

3.1. *L'attività consultiva del Garante*

Il nuovo quadro normativo europeo prevede il parere obbligatorio dell'autorità nazionale di controllo anche in relazione alla normativa di rango primario, includendo quindi le iniziative legislative – sia del Parlamento, che del Governo – aventi impatto sulla protezione dei dati personali nel novero dei provvedimenti per la cui elaborazione è necessario consultare il Garante (artt. 36, par. 4, e 57, par. 1, lett. *c*), cons. 96, del RGPD; art. 28, par. 2, direttiva (UE) 2016/680; art. 24, comma 2, d.lgs. n. 51/2018).

L'art. 36, par. 4, del RGPD non chiarisce con quali modalità e con che tempistica l'obbligo debba essere assolto, sia da parte del Parlamento che del Governo, limitandosi a prevedere che la consultazione avvenga "durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali". Analoga previsione è contenuta nell'art. 28 della direttiva 2016/680, mentre nessuna indicazione specifica al riguardo si rinviene nell'art. 24, d.lgs. n. 51/2018 che dà attuazione al predetto art. 28 in ordine alla consultazione sugli schemi di provvedimenti adottati per finalità di giustizia o di polizia o nel Codice novellato.

3.1.1. La consultazione del Garante su atti normativi statali di rango primario: le audizioni in Parlamento su progetti di legge

Consolidando una prassi già avviata nel 2018 durante il primo scorcio di legislatura, il Parlamento ha consultato il Garante nel corso dell'esame di proposte o disegni di legge aventi rilevanza sotto il profilo della protezione dei dati, richiedendo all'Autorità audizioni informali presso le competenti Commissioni di merito oppure, in altri casi, l'inoltro di una memoria scritta su eventuali profili di criticità delle disposizioni normative in discussione.

Ciò è avvenuto nel corso dei lavori su progetti di legge relativi a temi di notevole importanza, che spaziano dalle intercettazioni di comunicazioni elettroniche mediante captatore informatico, ai poteri di indagine e di verifica dell'Agenzia delle entrate in ambito fiscale mediante "analisi dei rischi"; e ancora all'utilizzo da parte della medesima Agenzia e della Guardia di finanza dei *file* delle fatture elettroniche, al reddito di cittadinanza, alla prevenzione dell'assenteismo mediante utilizzo di dati biometrici e di strumenti di videosorveglianza, alla videosorveglianza negli asili nido o in luoghi di cura per finalità di prevenzione di maltrattamenti ai danni di bambini o di altre persone vulnerabili (cfr. par. 2.2).

La delicatezza e l'importanza dei temi trattati testimoniano il fatto che, al di là delle forme prescelte per consultare l'Autorità, il Parlamento ha dimostrato una forte sensibilità sui temi aventi impatto sul diritto alla protezione dei dati personali, coinvolgendo comunque il Garante nel corso del procedimento legislativo.

Le audizioni si sono tenute in relazione a progetti di legge che riguardavano le seguenti materie:

- disciplina delle intercettazioni di conversazioni o comunicazioni (audizione 4 febbraio 2020, Senato - 2ª Commissione giustizia, doc. web n. 9260158);
- interventi per la concretezza delle azioni delle p.a. e la prevenzione dell'assen-

teismo (audizione 6 febbraio 2019, Camera - Commissioni riunite I Affari costituzionali e XI Lavoro pubblico e privato, doc. web n. 9080870);
- misure per prevenire e contrastare condotte di maltrattamento o di abuso, anche di natura psicologica, in danno dei minori negli asili nido e nelle scuole dell'infanzia e delle persone ospitate nelle strutture socio-sanitarie e socio-assistenziali per anziani e persone con disabilità (audizione 30 gennaio 2019, Senato - 1ª Commissione Affari costituzionali, doc. web n. 9081548).

Nei seguenti casi, invece, sono stati forniti contributi scritti con osservazioni:
- bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022 (Legge di bilancio 2020) (memoria 12 novembre 2019, Senato - 5ª Commissione Bilancio, doc. web n. 9184376);
- conversione in legge del decreto-legge n. 124/2019, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili (cd. decreto fiscale) (memoria 5 novembre 2019, Camera - VI Commissione Finanze, doc. web n. 9178137);
- conversione in legge del decreto-legge 28 gennaio 2019, n. 4, recante disposizioni urgenti in materia di reddito di cittadinanza e di pensioni (memoria trasmessa l'8 febbraio 2019, Senato - 11ª Commissione permanente Lavoro pubblico e privato, previdenza sociale, doc. web n. 9081679; memoria 6 marzo 2019, Camera - Commissioni riunite XI Lavoro pubblico e privato e XII Affari sociali, doc. web n. 9089070).

3.1.2. La consultazione del Garante su atti normativi statali di rango primario: i pareri su schemi di decreto legislativo

Per quanto riguarda l'attività normativa di rango primario del Governo, il Garante ha reso il parere di competenza su due schemi di decreto legislativo.

In un caso si è trattato dello schema di decreto legislativo recante integrazioni e modifiche ai decreti legislativi 25 maggio 2017, nn. 90 e 92, concernente l'attuazione della direttiva (UE) 2015/849 del 20 maggio 2015 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che si rendevano necessarie per recepire le osservazioni formulate dalla Commissione europea nell'ambito dell'avviata procedura di infrazione nei confronti dell'Italia (n. 2019/2042), con cui veniva contestato il non completo recepimento di suddetta direttiva (cd. IV direttiva antiriciclaggio).

Il medesimo schema conteneva, altresì, le disposizioni necessarie ad assicurare il recepimento della direttiva (UE) 2018/843 del 30 maggio 2018 (cd. V direttiva antiriciclaggio), *medio tempore* adottata.

Il Garante, che era già intervenuto in sede di parere sul precedente schema di decreto legislativo con il quale si era fornita la prima attuazione della direttiva (UE) 2015/849 in tema di riciclaggio e di finanziamento del terrorismo (parere 9 marzo 2017, n. 125, doc. web n. 6124534), ha formulato una serie di osservazioni che tengono conto, ribadendole, di quelle già rese nel provvedimento del 2017.

Nel parere reso (24 luglio 2019, n. 150, doc. web n. 9126288) il Garante si è pronunciato sugli obblighi di adeguata verifica della clientela e conservazione documentale di cui all'art. 18, d.lgs. n. 231/2007, tornando ad affermare l'opportunità che il trattamento – nel rispetto delle finalità previste dalla direttiva – venga effettuato solo sui dati necessari e con modalità proporzionate tanto per l'identificazione del cliente o del titolare effettivo quanto per la valutazione del rischio di riciclaggio e di finanziamento del terrorismo.

L'Autorità ha ribadito il rilievo, avanzato nel parere del 2017, con il quale veniva richiesta l'introduzione di un rinvio a un atto di natura regolamentare che discipli-

3

nasse la consultazione del sistema pubblico per la prevenzione del furto di identità di cui al d.lgs. 11 aprile 2011, n. 64 (sistema Scipafi), al fine di effettuare il riscontro sulla veridicità dei dati identificativi forniti dal cliente per adempiere agli obblighi di adeguata verifica. Tale atto si rende infatti necessario per specificare le tipologie di dati, le categorie di soggetti che vi possono accedere, le procedure di abilitazione dei soggetti obbligati e i dati oggetto di riscontro per la verifica della veridicità dei dati forniti, a maggior ragione sulla base del nuovo quadro giuridico, secondo cui la base giuridica richiesta è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 6, par. 3, lett. *b*), del RGPD e art. 2-*ter* del Codice).

Con riguardo invece alle misure di sicurezza per la comunicazione e la conservazione dei dati – rispetto alle quali il Garante ha ritenuto inadeguato il termine di 10 anni e ne ha proposto la riduzione – si è ritenuto opportuno richiedere l'adozione di meccanismi di cifratura e di sicurezza finalizzati a proteggere le informazioni contenute nei *file* e ad assicurare l'integrità del contenuto, prevenendone il pericolo di alterazioni. L'accesso alle informazioni (anche dopo la cifratura) deve essere assicurato ad un numero il più possibile limitato di persone sottoposte all'autorità del titolare e i dati devono essere loro forniti già cifrati, se il trattamento viene affidato a soggetti esterni.

Il decreto adottato ha tenuto conto solo in parte delle osservazioni del Garante: in particolare, è stata recepita l'indicazione di precisare la disciplina della limitazione dei diritti rispetto a trattamenti effettuati per finalità di contrasto del riciclaggio, finalità riconosciute di particolare interesse pubblico, in relazione alle attività di segnalazione e comunicazione antiriciclaggio, che riguarda i diritti di cui agli artt. da 15 a 18 e da 20 a 22 del RGPD (cfr. par. 14.2).

Un parere è stato altresì reso su uno schema di decreto legislativo in materia di nautica da diporto, adottato su proposta del Ministro delle infrastrutture e dei trasporti, (parere 2 ottobre 2019, n. 178, doc. web n. 9162642); già intervenuto sul precedente decreto del 2017 (provv. 19 ottobre 2017, n. 420, doc. web n. 7273618), il Garante ha formulato una serie di osservazioni volte a segnalare la necessità di maggiori tutele per il trattamento dei dati personali in tale settore. Scopo del decreto è aggiornare i procedimenti amministrativi in materia di nautica da diporto alle previsioni del Sistema telematico centrale ad essi riferito (Siste), istituire l'Ufficio di conservatoria centrale delle unità da diporto (Ucon), completare e chiarire le disposizioni del codice della nautica da diporto attraverso una maggiore sistematicità e semplificazione del quadro dei decreti attuativi. Con riferimento agli istituti di maggiore interesse sotto il profilo della protezione dei dati personali, l'analisi del Garante si è soffermata sull'Elenco nazionale degli istruttori di vela, l'Anagrafe nazionale delle patenti, l'Archivio nazionale dei prodotti delle unità da diporto e i dati riportati sulla patente nautica. L'Autorità ha così suggerito al Ministero di integrare lo schema prevedendo l'utilizzo di codici comunitari armonizzati o di codici nazionali per annotare sulla patente nautica le limitazioni e le prescrizioni nei confronti di soggetti che si trovino in particolari condizioni psico-fisiche, impedendo in tal modo la diretta conoscibilità delle informazioni sullo stato di salute. Rispetto all'Anagrafe nazionale delle patenti nautiche, completamente informatizzata, il Garante ha chiesto di chiarire, nel rispetto dei principi di trasparenza e correttezza del trattamento, quali dati debbano essere forniti dai vari soggetti interessati. Particolare attenzione infine è stata rivolta all'ambito del trattamento di particolari categorie di dati personali e di dati personali relativi a condanne penali e reati di cui agli artt. 9 e 10 del RGPD, al fine di completare la base giuridica del trattamento, individuando gli elementi

minimi necessari previsti dal quadro normativo generale in materia di protezione dei dati personali (art. 6, par. 3, lett. *b*), del RGPD e artt. 2-*sexies* e 2-*octies* del Codice).

3.1.3. La consultazione del Garante su atti normativi delle regioni e delle autonomie

Il Garante ha poi reso parere su alcuni progetti di legge in ambito regionale o delle Province autonome riferiti, in particolare, ai seguenti ambiti:

- una disposizione integrativa della legge della Provincia di Trento 31 maggio 2012, n. 10, recante interventi urgenti per favorire la crescita e la competitività del Trentino (parere 12 giugno 2019, n. 128, doc. web n. 9123419);
- il progetto di legge della Regione Molise concernente test antidroga casuali e periodici per i consiglieri e assessori della Regione Molise (parere 10 ottobre 2019, n. 188, doc. web n. 9206457);
- il disegno di legge della Provincia autonoma di Trento concernente disciplina dell'agriturismo e modificazioni della legge provinciale 19 dicembre 2001, n. 10 e della legge provinciale 13 dicembre 1996, n. 6 (parere 31 ottobre 2019, n. 202, doc. web n. 9207836);
- il disegno di legge della Regione Lombardia istitutivo del Registro regionale per la gestione coordinata degli accessi dei veicoli alla Ztl (parere 11 dicembre 2019, n. 219, doc. web n. 9232560).

3.1.4. I pareri sugli atti regolamentari e amministrativi del Governo

Nel quadro dell'attività consultiva concernente norme regolamentari ed atti amministrativi generali suscettibili di incidere sulla protezione dei dati personali, il Garante ha reso il parere di competenza su numerosi schemi di decreto o di altri provvedimenti, alla stregua della normativa di riferimento (artt. 36, par. 4, e 57, par. 1, lett. *c*), del RGPD; art. 154, comma 5, del Codice). Ci si riferisce, in particolare, agli schemi relativi al:

- decreto del Mef relativo all'estensione alle strutture militari della rilevazione delle spese sanitarie (parere 17 gennaio 2019, n. 7, doc. web n. 9084299);
- decreto del Mef sullo schema di decreto della Ragioneria generale dello Stato relativo all'estensione alle strutture militari della rilevazione delle spese sanitarie (parere 31 gennaio 2019, n. 30, doc. web n. 9084311);
- decreto del Ministro dell'istruzione, dell'università e della ricerca recante modifiche al regolamento 8 febbraio 2013, n. 45 sulle modalità di accreditamento delle sedi e dei corsi di dottorato e criteri per la istituzione dei corsi di dottorato da parte degli enti accreditati (parere 14 febbraio 2019, n. 43, doc. web n. 9102022);
- decreto recante modifiche al d.P.R. 19 settembre 2000, n. 358 che ha introdotto lo sportello telematico dell'automobilista (parere 14 marzo 2019, n. 59, doc. web n. 9106322);
- decreto del Ministro per la pubblica amministrazione recante le modalità di digitalizzazione delle procedure dei contratti pubblici (*e-procurement*) ai sensi dell'art. 44 del d.lgs. 18 aprile 2016, n. 50 (parere 19 marzo 2019, n. 66, doc. web n. 9113870);
- regolamento recante la disciplina delle modalità di iscrizione in via telematica degli atti di ultima volontà nel registro generale dei testamenti su richiesta del notaio o del capo dell'archivio notarile, ai sensi dell'art. 5-*bis*, l. 25 maggio 1981, n. 307 (parere 28 marzo 2019, n. 86, doc. web n. 9113929);
- decreto del Ministero della salute che disciplina il Sistema di segnalazione delle malattie infettive (Premal) (parere 18 aprile 2019, n. 105, doc. web n.

3

9124009);
- regolamento che sostituisce il d.P.R. 7 settembre 2010, n. 178, recante disposizioni in materia di iscrizione e funzionamento del Registro pubblico delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato (parere 30 aprile 2019, n. 109, doc. web n. 9109315);
- decreto di attuazione dell'art. 57 del Codice recante regolamento sulla disciplina delle procedure di raccolta, accesso, comunicazione, correzione, cancellazione ed integrazione dei dati e delle informazioni registrati nel Ced del Dipartimento di pubblica sicurezza del Ministero dell'interno (parere 6 maggio 2019, n. 110, doc. web n. 9116046);
- regolamento per l'attuazione della banca dati nazionale delle dichiarazioni anticipate di trattamento (Dat) (parere 29 maggio 2019, n. 123, doc. web n. 9117770);
- regolamento recante modifiche al decreto del Ministro dell'interno 15 febbraio 2012, n. 23, concernente l'istituzione dell'elenco dei revisori dei conti degli enti locali e modalità di scelta dell'organo di revisione economico-finanziario (parere 12 giugno 2019, n. 129, doc. web n. 9123427);
- decreto del Mise relativo alle procedure di consultazione e accesso al sistema informativo nazionale federato delle infrastrutture (parere 20 giugno 2019, n. 132, doc. web n. 9123563);
- decreto del Ministero del lavoro e delle politiche sociali attuativo in materia di Isee precompilata (parere 20 giugno 2019, n. 136, doc. web n. 9124390);
- decreto del Ministro del lavoro e delle politiche sociali in materia di Sistema informativo del reddito di cittadinanza (parere 20 giugno 2019, n. 138, doc. web n. 9122428);
- d.P.C.M. concernente l'individuazione dei criteri, delle condizioni e degli adempimenti per richiedere l'anticipo Tfs/Tfr, nonché le modalità di funzionamento dell'istituendo Fondo di garanzia (parere 30 luglio 2019, n. 156, doc. web n. 9126584);
- decreto del Mef per le prestazioni del fondo indennizzo risparmiatori (Fir) in applicazione delle disposizioni di cui all'art. 1, commi da 493 a 507, l. 30 dicembre 2018, n. 145 (parere 30 luglio 2019, n. 155, doc. web n. 9126476);
- regolamento del Ministro della salute recante la disciplina degli obiettivi, delle funzioni e della struttura del Sistema informativo trapianti (Sit) e del Registro nazionale dei donatori di cellule riproduttive a scopi di procreazione medicalmente assistita di tipo eterologo (parere 30 luglio 2019, n. 158, doc. web n. 9131111);
- d.P.C.M. concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56, recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo (parere 19 settembre 2019, n. 167, doc. web n. 9147290);
- d.P.C.M. concernente disposizioni in materia di misure di protezione dei minori stranieri non accompagnati (parere 19 settembre 2019, n. 172, doc. web n. 9162562);
- decreto del Ministero del lavoro e delle politiche sociali su proposta di Dichiarazione sostitutiva unica (Dsu) e istruzioni per la compilazione (parere 19 settembre 2019, n. 176, doc. web n. 9163393);
- decreto del Mef per l'estensione della rilevazione delle spese sanitarie attraverso il sistema TS a ulteriori categorie di esercenti le professioni sanitarie (parere 26 settembre 2019, n. 174, doc. web n. 9162444);

- decreto del Ministero dell'infrastrutture e dei trasporti concernente la disciplina delle modalità semplificate di trasmissione dei certificati medici attestanti l'idoneità psicofisica dei conducenti dei veicoli a motore (parere 17 ottobre 2019, n. 192, doc. web n. 9207176);
- schema di d.P.C.M. recante le modalità e criteri di attivazione e gestione del Servizio IT-*alert* (parere 17 ottobre 2019, n. 193, doc. web n. 9207188);
- regolamento del Ministro per i beni e le attività culturali e per il turismo in tema di criteri e modalità di attribuzione e di utilizzo della Carta elettronica per i diciottenni (cd. *bonus* cultura) (parere 14 novembre 2019, n. 207, doc. web n. 9195252);
- decreto del Ministro del lavoro e delle politiche sociali, di concerto con il Mef in materia di fruizione, mediante Carta Rdc, del beneficio economico spettante ai beneficiari del reddito di cittadinanza (parere 11 dicembre 2019, n. 214, doc. web n. 9232574).

Il Garante si è inoltre espresso sui seguenti atti e provvedimenti non aventi natura regolamentare:

Atti non regolamentari

- contratto tra il Ministero per i beni e le attività culturali e Sogei in attuazione dell'art. 2, d.P.C.M. n. 16/2017 (parere 17 gennaio 2019, n. 6, doc. web n. 9082272);
- provvedimento del Ministero per i beni e le attività culturali e per il turismo recante le modalità e i tempi della gestione e conservazione dei dati personali raccolti in attuazione della disciplina in materia di attribuzione e di utilizzo della Carta elettronica prevista dall'articolo l, comma 604, della legge 30 dicembre 2018, n. 145 (cd. *bonus* cultura) (parere 18 dicembre 2019, n. 224, doc. web n. 9220734).

3.1.5. I pareri sugli atti regolamentari e amministrativi resi ad altre Istituzioni

Il Garante ha reso il parere di competenza su numerosi atti regolamentari e amministrativi di altre Istituzioni che di seguito si riportano:

- tre schemi di provvedimento del Direttore all'Agenzia delle entrate in tema di comunicazione all'Anagrafe tributaria di informazioni per l'elaborazione della dichiarazione dei redditi precompilata relativa all'anno d'imposta 2018 (parere 24 gennaio 2019, n. 13, doc. web n. 9082720);
- schema di provvedimento del Direttore dell'Agenzia delle entrate recante modalità tecniche di utilizzo dei dati delle spese sanitarie ai fini della elaborazione della dichiarazione dei redditi precompilata, a decorrere dall'anno d'imposta 2018 (parere 31 gennaio 2019, n. 35, doc. web n. 9084331);
- schema di regolamento predisposto dall'Istituto nazionale per la valutazione del sistema educativo di istruzione e di formazione, concernente le modalità di svolgimento delle prove Invalsi dell'ultimo anno della scuola secondaria di secondo grado (parere 14 febbraio 2019, n. 44, doc. web n. 9102421);
- schema di provvedimento del Direttore dell'Agenzia delle entrate relativo alla sperimentazione di una procedura di selezione basata sull'utilizzo delle informazioni fornite dall'Archivio dei rapporti finanziari e dai dati presenti in Anagrafe tributaria per l'individuazione di profili di evasione rilevanti (parere 14 marzo 2019, n. 58, doc. web n. 9106329);
- schema di linee guida AgID relative all'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) (parere 14 marzo 2019, n. 64, doc. web n. 9113862);
- schema di provvedimento Inps attuativo dell'art. 5, comma 1, d.l. 28 gennaio 2019, n. 4, di approvazione del modulo di domanda del reddito di cittadi-

nanza e della pensione di cittadinanza (parere 29 marzo 2019, n. 82, doc. web n. 9106306);
- schema di provvedimento del Direttore dell'Agenzia delle entrate recante comunicazioni per la promozione dell'adempimento spontaneo nei confronti dei contribuenti che non hanno dichiarato, in tutto o in parte, le attività finanziarie detenute all'estero nel 2016, come previsto dalla disciplina sul monitoraggio fiscale, nonché gli eventuali redditi percepiti in relazione a tali attività estere (parere 4 aprile 2020, n. 44, doc. web n. 9106360);
- schema di provvedimento del Direttore dell'Agenzia delle entrate per l'accesso alla dichiarazione 730 precompilata (parere 11 aprile 2019, n. 89, doc. web n. 9113901);
- scheda identificativa dell'indagine europea sulla salute (EHIS) predisposta dall'Istat (parere 11 aprile 2019, n. 94, doc. web n. 9113830);
- schema di linee guida AgID contenenti le regole tecniche e raccomandazioni afferenti la generazione di certificati qualificati, firme e sigilli elettronici qualificati e validazione temporale elettronica qualificata (parere 12 giugno 2019, n. 142, doc. web n. 9123455);
- schema di provvedimento del Direttore dell'Agenzia delle entrate concernente la disciplina relativa ai sistemi di biglietterie automatizzate (parere 20 giugno 2019, n. 35, doc. web n. 9122419);
- schema di deliberazione Arera recante l'istituzione del Portale dei consumi di energia elettrica e di gas naturale (parere 20 giugno 2019, n. 131, doc. web n. 9123551);
- schema di decreto del Direttore dell'Agenzia delle dogane e dei monopoli in tema di regole tecniche per la produzione dei sistemi di gioco VLT (parere 24 luglio 2019, n. 151, doc. web n. 9126407);
- schema di provvedimento dell'Agenzia delle entrate inerente alle modalità tecniche di utilizzo dei dati delle spese sanitarie e delle spese veterinarie (parere 17 ottobre 2019, n. 191, doc. web n. 9207155);
- schema di linee guida AgID relative all'accessibilità degli strumenti informatici (parere 17 ottobre 2019, n. 194, doc. web n. 9207804);
- schema di provvedimento del Direttore dell'Agenzia delle entrate recante disposizioni in materia di memorizzazione elettronica e trasmissione telematica dei dati dei corrispettivi validi ai fini della lotteria di cui all'articolo 1, commi da 540 a 544, della legge 11 dicembre 2016, n. 232 (parere 31 ottobre 2019, n. 197, doc. web n. 9175238);
- schema di linee guida Anac in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro (cd. *whistleblowing*) (parere 4 dicembre 2019, n. 215, doc. web n. 9215763);
- schema di provvedimento del Direttore dell'Agenzia delle entrate in tema di memorizzazione elettronica e trasmissione telematica dei dati dei corrispettivi giornalieri attraverso i registratori telematici (parere 18 dicembre 2019, n. 221, doc. web n. 9217337);
- schema di provvedimento congiunto del Direttore dell'Inps e del Direttore dell'Agenzia delle entrate volto a disciplinare le specifiche tecniche per l'accesso alla Dsu precompilata (parere 18 dicembre 2019, n. 225, doc. web n. 9220741).

3.2. *Le attività di sindacato ispettivo e di indirizzo e controllo del Parlamento*

L'Autorità ha curato il monitoraggio degli atti di sindacato ispettivo e di indirizzo del Parlamento riguardanti possibili aspetti di interesse in materia di protezione dei dati, in relazione ai quali non si segnalano, in questo primo scorcio di legislatura, richieste al Garante di elementi informativi da parte del Governo ai fini della risposta da fornire agli interroganti.

Tra gli atti di sindacato di interesse, quelli di seguito riportati si sono conclusi con la risposta del rappresentante del Governo:

- interrogazione a risposta orale in tema di installazione di sistemi di videosorveglianza cd. intelligenti nel Comune di Roma (Camera n. 2-00352);
- interrogazione a risposta orale in tema di tutela degli autori di segnalazioni di reati (cd. *whistleblowing*) (Camera n. 3-01204) dove la Ministra per la pubblica amministrazione ha sottolineato i progressi delle Istituzioni per garantire la tutela del segnalante, rilevando però la necessità di rafforzare l'effettiva applicazione della legge. Ha ricordato inoltre la recente approvazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, volta ad assicurare un livello di protezione adeguato anche mediante la previsione di canali sicuri per la segnalazione;
- interrogazione a risposta scritta relativa alla pubblicazione su Facebook di immagini e nominativi di stranieri occupanti alloggi popolari di Bologna da parte di due esponenti di un partito politico (Camera n. 4-04099) in cui il rappresentante del Governo, in attesa dei provvedimenti del Garante, ha condannato le iniziative idonee a generare fenomeni di intolleranza ed un clima di contrapposizione tra cittadini e di discriminazione;
- interpellanza urgente in materia di intercettazioni mediante inserimento di captatore informatico, in particolare in relazione alle osservazioni del Garante per la protezione dei dati personali (Camera n. 2-00553), con riguardo alla quale il Sottosegretario di Stato per l'interno ha dato informazioni sull'avvio di un tavolo presso il Ministero della giustizia che si occuperà della definizione di una nomenclatura delle tipologie di intercettazioni. Il rappresentante del Governo ha affermato anche l'impegno per incrementare il livello di sicurezza di tali sistemi e l'avvio di una riforma che miri a far sì che i programmi funzionali alle operazioni di videosorveglianza siano conformi agli standard tecnici predefiniti a livello ministeriale;
- interrogazione a risposta immediata in materia di operatività del Fascicolo sanitario elettronico (Camera n. 3-01029).

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

È proseguita l'attività di esame delle leggi regionali approvate e sottoposte al vaglio di costituzionalità del Governo ai sensi dell'art. 127 della Costituzione, al fine di fornire alla Presidenza del Consiglio dei ministri eventuali elementi di valutazione circa la compatibilità di esse con le disposizioni in materia di protezione dei dati personali e con il dettato costituzionale (art. 117, comma 2, lett. *l*), Cost.).

Nel periodo considerato ne sono state esaminate 4 e per 3 di esse l'Autorità ha ritenuto di dover trasmettere alla Presidenza del Consiglio le pertinenti osservazioni:

a) legge della Regione Lombardia 6 dicembre 2018, n. 18, recante iniziative a favore dei minori che frequentano nidi e micronidi. L'Autorità, con nota 28 gen-

3

naio 2019, nel rilevare che il tema della videosorveglianza in asili nido o comunque in altri luoghi di ospitalità di persone "vulnerabili" non trovava ancora disciplina nella legislazione statale pur essendo all'esame del Parlamento un progetto di legge *ad hoc* sul quale si è espresso più volte il Garante in audizione, ha sottolineato la dubbia compatibilità della legge regionale con il dettato costituzionale sul riparto della potestà legislativa tra Stato e regioni. Al riguardo ha sottolineato la complessità del quadro normativo della materia accresciuto dall'intersezione di due distinte discipline di protezione dati: il RGPD (con l'integrazione, sul piano nazionale, del Codice, come novellato dal d.lgs. n. 101/2018), applicabile all'installazione e alla tenuta dei sistemi di videosorveglianza, e la direttiva (UE) 2016/680 (recepita dal d.lgs. n. 51/2018), applicabile alla fase dell'accesso ai dati acquisiti dalle telecamere e al relativo trattamento da parte degli organi inquirenti. Il bilanciamento dei diversi interessi sottesi in questo settore con il diritto alla protezione dei dati personali è devoluto allo Stato. E la conferma della delicatezza e complessità di questo compito sta proprio nell'impegno che il legislatore nazionale stava proprio allora profondendo nell'esame della proposta di legge citata. La legge regionale non è stata impugnata dalla Presidenza del Consiglio dei ministri;

b) legge della Regione Puglia 21 gennaio 2019, n. 1, recante disposizioni per l'attuazione della legge 22 dicembre 2017, n. 219 (Norme in materia di consenso informato e di disposizioni anticipate di trattamento). L'Autorità, con nota 25 febbraio 2019, ha segnalato alla Presidenza del Consiglio dei ministri profili di dubbia conformità della legge regionale con il quadro normativo di riferimento, sia con riguardo alla disciplina europea e nazionale in materia di protezione dei dati personali, sia rispetto alla normativa statale in materia di Dat (legge n. 219/2017) e l'opportunità di mettere a conoscenza delle criticità segnalate la Regione interessata, la quale ha poi comunicato di voler sottoporre al Consiglio regionale mirate proposte di modifica della legge nel senso suggerito dal Garante;

c) legge della Regione Marche 18 aprile 2019, n. 19, recante disposizioni di semplificazione e aggiornamento della normativa regionale, con la quale la Regione ha introdotto numerose disposizioni di semplificazione e aggiornamento della normativa regionale, in diverse materie. Le osservazioni dell'Autorità, inviate con nota 17 giugno 2019, hanno riguardato gli articoli 31 e 24, comma 4, rispettivamente in tema di pubblicità e trasparenza della situazione patrimoniale dei componenti gli organi della Regione, materia come è noto disciplinata a livello nazionale dal decreto legislativo n. 33/2013, e in tema di stato di salute e vaccinazioni dei giovani. Sotto il primo aspetto, il riferimento è al novellato art. 6, l.r. 17 dicembre 2012, n. 41 (Diffida e sanzioni amministrative), in base al quale il Presidente dell'Assemblea regionale diffida gli interessati alla presentazione entro 15 giorni dei documenti destinati alla pubblicazione che non siano stati presentati entro i termini previsti dalle pertinenti disposizioni della medesima legge, con la conseguenza che dell'eventuale inosservanza della diffida è data notizia anche tramite "avviso pubblicato sul sito istituzionale" dell'Assemblea per 30 giorni (art. 6, comma 2, l. n. 41/2012). La pubblicazione sul sito di tale atto di diffida rappresenta un obbligo ulteriore rispetto a quelli previsti dal decreto legislativo n. 33/2013 e ciò ha indotto l'Autorità a ritenere dubbia la compatibilità di tale previsione con il quadro normativo nazionale, soprattutto in ragione della legittima possibilità di adottare atti normativi in materia di trasparenza in deroga alla normativa nazionale. Da questo punto di vista si è fatto rinvio a quanto già rappresentato dal Garante nella nota 20 luglio 2015 indirizzata al Sottosegretario di Stato con delega agli affari regionali e le autonomie e al Presidente della Conferenza delle Regioni e delle Province autonome (doc. web n. 4758997), laddove venne evidenziato che, circa l'eventuale estensione dell'obbligo

di pubblicazione dei documenti, "il predetto decreto n. 33 prevede che le pubbliche amministrazioni possano disporre la pubblicazione nel proprio sito istituzionale di dati, informazioni e documenti che non hanno l'obbligo di pubblicare a norma di legge, a condizione però che rendano anonimi i dati". Quanto all'art. 24, comma 4, della legge (il quale prevede che la partecipazione dei giovani di età inferiore ai diciotto anni ai previsti campeggi è subordinata alla presentazione di idonea documentazione rilasciata dal medico curante che attesti lo stato di salute del giovane e le vaccinazioni), l'Autorità ha richiamato l'attenzione sulla necessità che tale previsione normativa sia conforme ai requisiti previsti dal RGPD ovvero che ogni base giuridica legittimante un trattamento di dati personali (cfr. art. 6, par. 3, lett. *b*), del RGPD) contenga l'indicazione del periodo di conservazione dei dati contenuti nella documentazione raccolta;

d) la legge della Regione Lombardia del 6 agosto 2019, n. 15, recante disposizioni di assestamento del Bilancio 2019-2020 con modifiche di leggi regionali, che, all'art. 22, ha aggiunto il comma 3-*bis* all'art. 3, l.r. n. 22/2018, istitutiva del Garante regionale per la tutela delle vittime di reato, ai sensi del quale, per lo svolgimento delle proprie attività di tutela in sede amministrativa e giudiziaria, detto Garante può trattare anche le categorie di dati personali di cui agli articoli 9 e 10 del RGPD, entro i limiti ivi previsti e nel rispetto delle disposizioni normative a tutela dei diritti fondamentali dell'interessato, fermo restando il rinvio ad un regolamento per l'individuazione di ulteriori misure a garanzia dei diritti dell'interessato. L'Autorità, con nota 30 settembre 2019, ha formulato alla Presidenza del Consiglio dei ministri alcune osservazioni volte a conformare pienamente l'intervento normativo della Regione ai principi e alle garanzie previste dall'aggiornato quadro normativo e, in particolare, ai requisiti di legittimità delle basi giuridiche su cui si fondano i trattamenti (artt. 6, 9 e 10 del RGPD; artt. 2-*sexies* e 2-*opties* del Codice). Al riguardo l'Autorità, in attuazione delle disposizioni relative ai dati rientranti nelle "categorie particolari" e "relativi a condanne penali e reati" – secondo cui i trattamenti di tali categorie di dati "sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento 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" (art. 2-*sexies*, comma 1, del Codice) –, ha richiamato l'attenzione della Presidenza del Consiglio e della Regione sulla necessità di rendere conforme il testo normativo regionale in esame con il regolamento di attuazione ex art. 2-*sexies* del Codice cui la norma regionale fa espresso rinvio e il cui schema dovrà essere sottoposto al parere del Garante (art. 36, par. 4, del RGPD). Le legge regionale non risulta essere stata impugnata dalla Presidenza del Consiglio, né risulta che la Regione abbia modificato l'articolo nel senso indicato dall'Autorità.

PAGINA BIANCA

L'attività svolta dal Garante

PAGINA BIANCA

II - L'attività svolta dal Garante

4 Il Garante e le amministrazioni pubbliche

4.1. *L'attività fiscale e tributaria*

Particolarmente intensa è stata, nel corso del 2019, la trattazione di una pluralità di tematiche di rilievo con riguardo ai trattamenti effettuati in ambito fiscale e tributario, rispetto ai quali, come emerge dalle informazioni di sintesi di seguito riportate, criticità sono state rilevate dall'Autorità in particolare in relazione all'osservanza del principio di pertinenza e non eccedenza.

4.1.1. La cd. dichiarazione dei redditi precompilata

Entro l'ampio perimetro delle aree di sovrapposizione con la materia fiscale, numerosi sono stati i pareri espressi nell'ambito della realizzazione della cd. dichiarazione dei redditi precompilata, aventi ad oggetto sia schemi di decreti del Mef che schemi di provvedimenti dell'Agenzia delle entrate, tutti adottati ai sensi dell'art. 3, commi 4 e 5, d.lgs. 21 novembre 2014, n. 175. In particolare, il Ministero ha inteso adottare un decreto, sul quale il Garante ha reso parere favorevole (provv. 17 gennaio 2019, n. 7, doc. web n. 9084299), per estendere il novero delle informazioni da trasmettere telematicamente all'Agenzia delle entrate, a fini di deduzioni dal reddito o detrazioni dall'imposta, a quelle concernenti le spese sanitarie sostenute presso strutture sanitarie militari.

In attuazione di questo provvedimento, la Ragioneria generale dello Stato ha quindi sottoposto all'Autorità uno schema di decreto volto a definire le specifiche tecniche e le modalità operative relative alla predetta trasmissione telematica, sul quale il Garante si è espresso in modo favorevole, in quanto le misure e garanzie previste sono risultate conformi a quelle contenute nel d.m. 31 luglio 2015 e in decreti ministeriali successivi (su cui pure il Garante aveva già reso parere favorevole). In particolare, alla luce dei tempi di attuazione di tale trasmissione, è stato assicurato agli interessati un termine sufficiente per poter effettuare l'opposizione al trattamento mediante la dichiarazione precompilata (provv. 31 gennaio 2019, n. 30, doc. web n. 9084311).

Il Garante ha espresso parere favorevole anche sul conseguente schema di provvedimento del Direttore dell'Agenzia delle entrate che ha disciplinato le modalità tecniche di utilizzo dei medesimi dati concernenti le spese sanitarie militari (provv. 31 gennaio 2019, n. 35, doc. web n. 9084331).

In seguito, al fine di consentire a un maggior numero di soggetti la possibilità di trasmettere le spese sanitarie sostenute dai contribuenti attraverso il sistema TS, è stato predisposto uno schema di decreto del Mef che estendeva tale possibilità a professionisti iscritti in albi professionali, quali l'Albo della professione sanitaria di

assistente sanitario, l'Albo dei biologi e gli Albi afferenti all'Ordine dei tecnici sanitari di radiologia medica e delle professioni sanitarie tecniche, della riabilitazione e della prevenzione; anche rispetto ad esso è stato espresso parere favorevole (provv. 26 settembre 2019, n. 174, doc. web n. 9162444).

Sul conseguente schema di provvedimento del Direttore dell'Agenzia delle entrate, che si occupa delle modalità tecniche di utilizzo dei predetti dati, il Garante non ha formulato osservazioni, rilevando come le misure e garanzie a tutela degli interessati già precedentemente individuate fossero rimaste inalterate (provv. 17 ottobre 2019, n. 191, doc. web n. 9207155).

Analogamente, il Garante, con un unico parere, non ha ritenuto di formulare rilievi sugli schemi di provvedimenti che disciplinavano la trasmissione, all'Agenzia stessa, di una serie di dati (quelli relativi agli interventi di recupero del patrimonio edilizio e di riqualificazione energetica effettuati su parti comuni di edifici residenziali, quelli relativi ai contratti assicurativi e ai premi assicurativi e quelli relativi agli interessi passivi per contratti di mutuo), in quanto modificativi di provvedimenti già vagliati dall'Autorità, senza alcuna alterazione circa i canali di trasmissione e le relative misure di sicurezza (provv. 24 gennaio 2019, n. 13, doc. web n. 9082720).

Il Direttore dell'Agenzia delle entrate, infine, ha ritenuto di aggiornare il proprio provvedimento del 2018 concernente l'accesso alla dichiarazione precompilata da parte del contribuente e degli altri soggetti autorizzati, integrandolo con l'elenco degli oneri detraibili e deducibili a partire dal 2019. Tale schema di provvedimento ha inteso prolungare il periodo sperimentale in cui i Caf potevano accedere alle dichiarazioni dei redditi precompilate e alle informazioni relative a singoli contribuenti, in cooperazione applicativa, con le medesime modalità tecniche già individuate. Ritenuto adeguato il livello di sicurezza delle misure previste nello schema di provvedimento, il Garante ha espresso il proprio avviso favorevole, e ha autorizzato l'Agenzia delle entrate ad effettuare il trattamento proposto, ai sensi dell'art. 58, par. 3, lett. *c*), del RGPD, e dell'art. 2-*quinquiesdecies* del Codice, ingiungendole altresì di trasmettere l'esito dei controlli a campione effettuati (provv. 11 aprile 2019, n. 89, doc. web n. 9113901).

4.1.2. Controlli antievasione: l'utilizzo dell'Archivio dei rapporti finanziari

Anche nel 2019 il Garante è stato chiamato a pronunciarsi sulla prosecuzione della sperimentazione della procedura di selezione basata sull'utilizzo delle informazioni comunicate all'Archivio dei rapporti finanziari, ai fini dell'analisi del rischio di evasione ai sensi dell'art. 11, comma 4, d.l. 6 dicembre 2011, n. 201, che l'Agenzia delle entrate ha voluto estendere agli anni di imposta 2014 e 2015. Il Garante ha subordinato il proprio parere favorevole alla condizione che venissero richiamate nel relativo provvedimento del Direttore le misure di garanzia a tutela degli interessati già stabilite nel provvedimento del 20 luglio 2017, con cui si era espresso sull'avvio della sperimentazione. In particolare, sono state richieste specifiche misure di sicurezza per la minimizzazione del rischio di accessi non autorizzati e adeguati controlli sulla qualità dei dati e sulle elaborazioni logiche, con garanzie specifiche per i trattamenti automatizzati, assicurando la puntuale valutazione della coerenza complessiva della posizione di ciascun contribuente selezionato da parte di operatori qualificati. È stato inoltre richiesto che al contribuente convocato in contraddittorio venissero fornite adeguate informazioni.

Con il medesimo parere il Garante ha autorizzato, ai sensi dell'art. 58, par. 3, lett. *c*), del RGPD, e dell'art. 2-*quinquiesdecies* del Codice, l'estensione di suddetta sperimentazione, prescrivendo altresì all'Agenzia di trasmettere all'Autorità, non appena disponibili, le risultanze della stessa, relative anche ai successivi anni di

imposta, ai fini della valutazione in concreto dell'idoneità delle procedure e delle garanzie in vista degli ulteriori utilizzi del modello di analisi sperimentato (provv. 14 marzo 2019, n. 58, doc. web n. 9106329).

4.1.3. L'utilizzo di dati derivanti dallo scambio automatico obbligatorio tra autorità fiscali estere aderenti agli accordi internazionali

Sempre in materia di controlli di carattere fiscale, il Direttore dell'Agenzia delle entrate, con proprio schema di provvedimento, ha inteso utilizzare, nell'ambito dello scambio automatico obbligatorio tra autorità fiscali estere aderenti agli accordi internazionali (DAC2/CRS e FACTA), informazioni di fonte estera al fine di consentire all'amministrazione di verificare il corretto adempimento degli obblighi dichiarativi da parte dei contribuenti residenti in Italia che non hanno dichiarato, in tutto o in parte, le attività finanziarie detenute all'estero nel 2016 ed i relativi redditi percepiti. Anche questa attività rientra, infatti, nelle finalità di controllo per contrasto all'evasione, come fissate dal citato art. 11, d.l. n. 201/2011, in merito al quale il Garante, con provvedimento 15 novembre 2012, aveva prescritto all'Agenzia di sottoporre all'Autorità i casi di trattamento dei dati oggetto della comunicazione integrativa annuale ai fini dell'individuazione di procedure e garanzie a tutela degli interessati. Pur a fronte di una valutazione di impatto focalizzata su aspetti meramente tecnici del trattamento, il Garante, ritenendo che i rischi per i diritti e le libertà degli interessati fossero stati adeguatamente considerati, ha fornito parere favorevole e ha autorizzato l'Agenzia, ai sensi dell'art. 58, par. 3, lett. *c*), del RGPD, e dell'art. 2-*quinquiesdecies* del Codice, ad effettuare il trattamento, a condizione che venissero richiamate le misure di garanzia a tutela degli interessati e venissero individuati puntualmente i tipi di dati messi a disposizione della Guardia di finanza e le relative modalità di comunicazione (provv. 4 aprile 2019, n. 84, doc. web n. 9106360).

4.1.4. Analisi del rischio per la lotta all'evasione fiscale: la legge di bilancio 2020

Come riferito nelle pagine introduttive (par. 2.1), in relazione all'analisi del rischio per finalità di prevenzione e contrasto dell'evasione fiscale, il Presidente dell'Autorità ha presentato una memoria alla Commissione V (Bilancio) del Senato della Repubblica sul disegno di legge di bilancio 2020 (memoria del 12 novembre 2019, doc. web n. 9184376). Con riferimento ai dati contenuti nell'Archivio dei rapporti finanziari e ai fini di cui all'art. 11, comma 4, d.l. n. 201/2011, l'art. 86 di tale disegno di legge legittimava l'Agenzia delle entrate, previa pseudonimizzazione dei dati personali, ad avvalersi delle tecnologie, delle elaborazioni e delle interconnessioni con le altre banche dati di cui dispone, per elaborare criteri di rischio utili a far emergere posizioni da sottoporre a controllo e incentivare l'adempimento spontaneo. Analoghe facoltà erano riconosciute, dal comma 3 dell'articolo, relativamente agli stessi dati, alla Guardia di finanza, pur in assenza di un'adeguata specificazione del ruolo assunto, anche in rapporto alle attività dell'Agenzia delle entrate, nonché del coordinamento tra l'Archivio dei rapporti finanziari e le altre banche dati con cui esso si interconnetta, con evidenti rischi di disallineamenti o duplicazione delle informazioni, nonché di attenuazione della qualità dei dati.

Il Presidente del Garante ha ritenuto necessario evidenziare che la prevista interconnessione delle banche dati, funzionale all'elaborazione dei parametri di rischio fiscale, non pare particolarmente innovativa, dal momento che tale possibilità era già sottesa alla riforma di cui al d.l. n. 201/2011, convertito, con modificazioni, dalla l. n. 214/2011, senza che peraltro il Garante avesse sul punto sollevato obiezioni né richiesto la pseudonimizzazione dei dati, come rilevabile anche dai provve-

4

dimenti sopra menzionati.

Il riferimento all'art. 23 del RGPD contenuto nelle disposizioni esaminate, relativo alle limitazioni dei diritti degli interessati – non all'intera disciplina di protezione dati che, comunque, l'Agenzia e la Guardia di finanza sono tenute a rispettare – è risultato, ad avviso dell'Autorità, probabilmente fuorviante in assenza delle precisazioni, di cui si dirà, alle modifiche proposte al comma successivo. Si è invece ritenuto più utile che la norma prevedesse un richiamo all'art. 22, par. 2, lett. *b*), del RGPD, nella parte in cui, per le decisioni fondate su trattamenti automatizzati normativamente previsti, impone di introdurre anche misure adeguate a tutela dei diritti e delle libertà degli interessati. In tal senso, l'Autorità ha ritenuto adeguato anche un rinvio a disposizioni attuative della stessa Agenzia delle entrate che, previo parere del Garante, prevedano – come peraltro rappresentato anche nella stessa relazione illustrativa – apposite misure di sicurezza, controlli sulla qualità dei dati e sulle elaborazioni logiche, nonché cautele relative al trattamento automatizzato, in modo da ridurre i rischi per gli interessati, con particolare riguardo ad erronee rappresentazioni della capacità contributiva. Tali accorgimenti, lungi dal depotenziare l'efficacia dell'azione di contrasto dell'evasione, potrebbero invece promuoverla – correggendo potenziali errori o distorsioni nel processo decisionale automatizzato – e conferirle, anche nella percezione dei cittadini, quella più forte legittimazione che una combinazione equa di tecnologia e "fattore umano" può assicurare all'azione amministrativa.

Con riferimento, invece, alla prevista pseudonimizzazione, è stato ricordato anzitutto che i dati personali sottoposti a tale processo non perdono la loro caratteristica di "dati personali", appunto, riferendosi comunque a persone fisiche identificabili, sia pur in via indiretta, con conseguente applicazione della disciplina di protezione dati (cfr. art. 4, nn. 1) e 5) e cons. 26 del RGPD). Il ricorso alla pseudonimizzazione in relazione al patrimonio informativo dell'Agenzia delle entrate, che, in costante incremento, già contiene miliardi di informazioni di dettaglio relative ad ogni aspetto della vita privata di tutta la popolazione, ivi compresi i minori, non costituisce infatti una garanzia in assoluto efficace. E ciò, anzitutto, perché l'interessato risulterebbe comunque identificabile, in ragione del dettaglio delle informazioni che, presso il titolare del trattamento, sarebbero associate allo pseudonimo, in luogo del codice fiscale. In secondo luogo, perché le finalità per le quali verrebbe effettuato il trattamento di dati pseudonimizzati, ovvero l'individuazione delle posizioni da sottoporre a controllo e per incentivare l'adempimento spontaneo, sono di per sé volte all'identificazione del contribuente, sicché in sostanza la misura prevista contrasterebbe con la finalità perseguita e si risolverebbe in un inutile aggravio per l'Agenzia.

Con riferimento alle previste limitazioni dei diritti dell'interessato è stato evidenziato che la modifica potrebbe risultare, paradossalmente, disfunzionale rispetto agli stessi interessi perseguiti, oltre che di dubbia legittimità se non adeguatamente circoscritta. Le stesse ragioni sottese alla modifica non appaiono di immediata evidenza dal momento che, per come è formulata, la disposizione non pare introdurre elementi di reale utilità rispetto all'azione di prevenzione e contrasto dell'evasione fiscale. Del resto, non sono risultati all'Autorità casi di esercizio dei diritti da parte dei contribuenti tali da aver arrecato pregiudizio all'efficacia dell'azione dell'amministrazione finanziaria. Peraltro, lungi dal delineare specifiche misure volte a potenziare l'efficacia dell'azione di contrasto dell'evasione, il disegno di legge introduce una generale limitazione dei diritti esercitabili dal cittadino in ogni procedimento, anche soltanto amministrativo, attinente genericamente alla materia della prevenzione e del contrasto dell'evasione fiscale, escludendo anche la possibilità

di proporre un reclamo al Garante. La preclusione dell'esercizio in via diretta, da parte degli interessati, dei diritti in relazione ai dati a sé riferiti, appare peraltro in contrasto con lo Statuto dei diritti del contribuente (l. n. 212/2000), che ha inteso regolare i rapporti tra amministrazione finanziaria e contribuenti secondo principi di massima trasparenza. Il diritto d'accesso alle informazioni in possesso dell'amministrazione finanziaria, oltre a essere stato riconosciuto dalla giurisprudenza amministrativa, anche in favore dei terzi, secondo i canoni della legge n. 241/1990 – anche in relazione ai dati presenti nell'Archivio dei rapporti finanziari – è, infatti, funzionale alla correttezza dei rapporti con il contribuente, chiamato a dichiarare al fisco le informazioni rilevanti per l'assolvimento degli obblighi tributari. E questo, soprattutto con l'introduzione della dichiarazione precompilata, fondata sulla messa a disposizione del contribuente delle informazioni nella disponibilità dell'amministrazione finanziaria. Precludere poi (o anche solo limitare) l'esercizio, direttamente da parte degli interessati, del diritto di rettificare dati inesatti, rischia di ostacolare la rilevazione di errori nelle valutazioni prodromiche alle verifiche fiscali, con una possibile conseguente falsa rappresentazione della capacità contributiva, depotenziando così l'efficacia dell'azione di contrasto dell'evasione fiscale. Anche la limitazione del diritto a richiedere in via diretta la cancellazione dei dati, ad esempio illegittimamente acquisiti, lungi dall'agevolare l'azione di contrasto, rischia invece di protrarre condotte illecite, esponendo così l'amministrazione al rischio di ingenti richieste risarcitorie oltre che di rilevanti sanzioni amministrative. Risulta pertanto ingiustificatamente gravoso consentire l'esercizio di tali diritti unicamente, tramite il Garante, ai sensi dell'art. 2-*undecies*, comma 3, del Codice, in quanto ciò comporta tempi e procedure ben diversi rispetto all'istanza diretta del singolo al titolare del trattamento.

In ogni caso, l'Autorità ha ribadito che, fermi restando questi dubbi sulla stessa funzionalità ed efficacia della proposta, le limitazioni dei diritti dell'interessato possono ammettersi, per espressa previsione della disciplina di protezione dati, solo se l'esercizio di tali diritti possa determinare un pregiudizio effettivo e concreto alle esigenze pubbliche perseguite e nei limiti di quanto "necessario e proporzionato in una società democratica" (artt. 23 del RGPD e 2-*undecies* del Codice).

Per impedire valutazioni eccessivamente disomogenee quando non addirittura decisioni scorrette, sarà necessario delineare, con la stessa legge, casi e presupposti che consentano di ravvisare il suddetto "pregiudizio effettivo e concreto". E questo, a maggior ragione se si deciderà di mantenere il riferimento alla prevenzione (oltre che al contrasto) dell'evasione fiscale tra gli obiettivi di interesse pubblico che legittimano tali limitazioni, considerando che mentre il contrasto include almeno, in parte, illeciti penali, la prevenzione per definizione allude a un novero ben più ampio di comportamenti, non necessariamente di per sé soli *contra legem* o comunque prodromici a più gravi illeciti. Andrà quindi adeguatamente circoscritta la portata delle limitazioni disposte per rendere la norma conforme (almeno *in parte qua*) all'art. 23 del RGPD che costituisce, peraltro, parametro di legittimità della normativa interna anche ai sensi dell'art. 117, comma primo, della Costituzione, disciplinando, in particolare, le categorie di dati coinvolti, le garanzie per prevenire vari tipi di illeciti, i rischi per i diritti e le libertà. Qualsiasi limitazione, ancorché legislativamente imposta, non può infatti intaccare – per espressa previsione del citato art. 23 – l'essenza dei diritti e delle libertà considerati e deve rispettare i principi di necessità e proporzionalità.

Soprattutto su questo aspetto il legislatore è stato invitato a valutare con rigore la modifica proposta, anche per evitare profili di incompatibilità con la disciplina europea di riferimento, che renderebbe la norma illegittima. Nella sua generalità,

infatti, la modifica proposta rischia di introdurre una limitazione eccedente le reali necessità perseguite, ostacolando l'esercizio dei diritti dei cittadini anche in ipotesi nelle quali esso non pregiudichi realmente le attività funzionali al contenimento del rischio di evasione fiscale. Il raffronto con la disciplina delle limitazioni dell'esercizio dei diritti degli interessati, prevista in tema di riciclaggio (cui la modifica proposta accosta, anche a livello testuale, la materia degli illeciti fiscali, all'interno dell'art. 2-*undecies*), è in tal senso significativo. Sarebbe, quindi, necessario circoscrivere adeguatamente l'ambito oggettivo di applicazione della norma derogatrice indicando almeno, ai sensi dell'art. 23 del RGPD e della disciplina generale di cui all'art. 2-*undecies* del Codice: i trattamenti (ed auspicabilmente anche i titolari) rispetto ai quali si prevede la possibilità di limitazione dell'esercizio dei diritti, gli specifici diritti oggetto di limitazione, i parametri in base ai quali ritenere sussistente, in caso di esercizio dei diritti da parte dell'interessato, il pregiudizio effettivo e concreto alle esigenze indicate, al fine di meglio orientare, nella prassi, l'applicazione della norma, evitando ingiustificate disparità di trattamento.

4.1.5. La lotteria dei corrispettivi

Interlocuzioni con l'Agenzia delle dogane e dei monopoli e l'Agenzia delle entrate sono state avviate per la realizzazione della lotteria dei corrispettivi prevista dall'art. 1, commi 540 ss., l. 11 dicembre 2016, n. 232, e ss.mm. (legge di bilancio 2017) nel rispetto del RGPD e del Codice. Al fine di attuare in modo efficace i principi di protezione dei dati fin dalla progettazione (*privacy by design:* cfr. art. 25 del RGPD), ai fini della partecipazione è stato stabilito che, in luogo del proprio codice fiscale, i contribuenti comunichino agli esercenti al momento dell'acquisto un cd. codice lotteria (pseudonimo del codice fiscale). Tale codice lotteria consiste in un codice alfanumerico, composto da otto caratteri generati in modo casuale, univocamente associato al codice fiscale del consumatore finale, e rilasciato dall'Agenzia delle dogane e dei monopoli, senza obbligo alcuno di identificazione del consumatore. Il consumatore ha la facoltà di generare più codici, tutti ugualmente validi ai fini della lotteria.

Il Garante ha quindi reso parere favorevole sul primo provvedimento del Direttore dell'Agenzia delle entrate attuativo della lotteria, recante memorizzazione elettronica e trasmissione telematica dei dati dei corrispettivi validi ai fini della lotteria di cui all'art. 1, commi da 540 a 544, l. 11 dicembre 2016, n. 232, nel quale si sono individuati i dati che gli esercenti devono memorizzare nei registratori telematici e trasmettere all'Agenzia delle entrate ai fini della lotteria. Nel parere è stato rilevato che l'utilizzo del codice lotteria costituisce un'efficace misura di garanzia per gli interessati, fermo restando che i dati oggetto di memorizzazione elettronica e di trasmissione telematica all'Agenzia delle entrate, seppur sottoposti a pseudonimizzazione, debbono essere considerati dati personali in quanto rappresentano informazioni su persone fisiche identificabili (cfr. cons. 26, e art. 4, nn. 1) e 5), del RGPD). È stato invece rinviato al successivo provvedimento dell'Agenzia delle entrate in tema di sicurezza l'esame delle misure tecniche e organizzative che gli esercenti dovranno adottare per il trattamento dei dati effettuato attraverso i registratori telematici (provv. 31 ottobre 2019, n. 197, doc. web n. 9175238).

Il Garante si è quindi espresso favorevolmente sullo schema di provvedimento del Direttore, recante modifiche al provvedimento del Direttore dell'Agenzia delle entrate n. 182017 del 28 ottobre 2016, e successive modificazioni, in tema di memorizzazione elettronica e trasmissione telematica dei dati dei corrispettivi giornalieri e il relativo documento di specifiche tecniche. In tali atti sono state indi-

viduate adeguate misure di garanzia riferite, in particolare, al trattamento dei dati conservati presso gli esercenti nella cd. memoria permanente dei registratori telematici o nei cd. *server* RT. Lo schema esaminato ha tenuto conto delle indicazioni fornite nelle interlocuzioni intercorse con i rappresentati dell'Agenzia delle entrate al fine di assicurare, in vista dell'avvio della lotteria dei corrispettivi, la conformità al RGPD del trattamento effettuato dagli esercenti nell'ambito della memorizzazione elettronica e trasmissione telematica degli stessi all'Agenzia delle entrate, tenuto conto del fatto che, come detto, seppur sottoposti a pseudonimizzazione, i dati oggetto di trattamento debbono essere considerati come dati personali e quindi, come ribadito anche nel documento contenente le specifiche tecniche, l'esercente in quanto titolare del trattamento dei dati presenti nelle memorie del registratore telematico (o del *server* RT) deve mettere in atto adeguate misure tecniche e organizzative al fine di garantire la conformità del trattamento al RGPD (art. 24).

Anche a fronte della prevista conservazione decennale da parte degli esercenti delle cd. memorie permanenti di riepilogo e di dettaglio ai sensi dell'art. 2220 c.c. (nelle quali sono memorizzati, tra gli altri, i dati dei corrispettivi), le misure di garanzia – individuate nel documento contenente le specifiche tecniche, dirette, oltre che ai produttori dei registratori telematici, anche agli esercenti – prevedono che il registratore telematico (o il *server* RT) sia configurato in modo da permettere all'esercente di disciplinare l'accesso, anche da remoto, ai dati contenuti nelle memorie permanenti di riepilogo e di dettaglio, nonché da inibire o abilitare, in qualunque momento, la lettura, l'esportazione e la ristampa, anche virtuale, dei dati contenuti nelle memorie; con un superamento, quindi, della disciplina precedente che non consentiva modalità di accesso riservato ai dati contenuti all'interno delle memorie. Inoltre, la trasmissione dei *file* dei corrispettivi all'Agenzia delle entrate deve avvenire mediante API REST su canale cifrato esclusivamente con protocollo TLS 1.2 e, per essere validi, gli aggiornamenti del *firmware* fiscale (effettuati sia localmente che da remoto dai tecnici abilitati) del registratore telematico (o del *server* RT) devono essere firmati elettronicamente dal produttore e approvati dall'Agenzia. Infine, le operazioni di lettura delle memorie e di chiusura giornaliera, di definizione e modifica della mappa dei punti cassa connessi a un *server* RT nonché quelle di modifica del *firmware* fiscale devono essere registrate nel registratore telematico (o nel *server* RT).

Il Garante, rilevando i maggiori rischi insiti nei trattamenti effettuati dagli esercenti nei possibili utilizzi impropri dei dati, soprattutto nei casi di utilizzo di registratori telematici accessibili o gestibili da remoto o di *server* RT, ha sottolineato perciò la necessità che esercenti e produttori, in conformità ai principi di *privacy by design* e *by default*, valutino adeguatamente l'idoneità dei prodotti e dei servizi in uso a soddisfare i requisiti del RGPD (provv. 18 dicembre 2019, n. 221, doc. web n. 9217337).

4.1.6. Le biglietterie automatizzate

L'Agenzia delle entrate ha sottoposto all'Autorità uno schema di provvedimento del Direttore in materia di contrasto al fenomeno del cd. *secondary ticketing* (espressione con la quale si identifica il fenomeno della ricollocazione in vendita di titoli di accesso ad attività di spettacolo parallelo al mercato ufficiale), volto ad individuare le specifiche tecniche che disciplinano le modalità di realizzazione di biglietterie automatizzate in grado di identificare l'acquirente e di rimessa in vendita dei titoli di accesso nominativi o del cambio di nominativo, in attuazione dell'art. 1, commi 545-*bis* ss., l. 11 dicembre 2016, n. 232 (legge di bilancio 2017).

Il Garante, che aveva ricevuto al riguardo una segnalazione, ha ritenuto proporzionato il trattamento rispetto ai fini perseguiti di contrasto all'elusione e all'eva-

sione fiscale, di tutela dei consumatori e di garanzia dell'ordine pubblico, poiché la necessità di biglietti di accesso nominativi e la conseguente verifica dell'identità dei fruitori è stata limitata ad alcune tipologie di attività di spettacolo per impianti con capienza superiore a 5000 spettatori e lo schema di provvedimento ha individuato misure atte a garantire il rispetto del RGPD e del Codice. La disciplina introdotta dall'Agenzia delle entrate consente di assicurare un trattamento di dati personali lecito e corretto, prevedendo modalità informative adeguate nei confronti degli interessati nonché il rispetto del principio di minimizzazione dei dati. In particolare, è stato previsto che i dati personali stampati sul titolo di accesso siano esclusivamente il nome e il cognome, indispensabili per consentire il riconoscimento personale (*de visu*) tramite l'esibizione di un documento di identità al momento dell'accesso all'area dello spettacolo.

In sede di acquisto dei titoli di accesso *online*, l'acquirente dovrà conferire i dati indispensabili per assicurare la sua identificazione univoca, secondo quanto stabilito dal d.m. 12 marzo 2018, nonché il numero del telefono cellulare, al fine di asseverare l'identità dell'acquirente e impedire gli acquisti multipli. Minori sono i dati raccolti in sede di acquisto dei titoli di accesso presso i *box office* autorizzati, attribuendo all'acquirente, su base volontaria e previa informativa, la facoltà di fornire al venditore il proprio nominativo allo scopo di consentirgli di richiederne il successivo cambio e la rimessa in vendita del titolo.

Anche la cd. lista unica dei titoli di accesso all'evento dovrà contenere solo nome e cognome dei partecipanti, in modo da consentire il previsto controllo *de visu* da parte degli addetti al controllo degli accessi. L'Agenzia, invece, non tratterà alcun dato personale relativo all'intestatario o all'acquirente del titolo oggetto di vendita o a qualsiasi altra forma di collocamento, di rimessa in vendita o di cambio nominativo, poiché ai fini dell'attività di controllo tributario, l'Agenzia riceve dalla Società italiana autori ed editori (Siae) i dati aggregati relativi ai proventi di ciascun organizzatore/distributore per ciascuna manifestazione.

Sono state altresì previste misure di sicurezza adeguate e l'Agenzia si è impegnata a valutare, d'intesa con le altre amministrazioni competenti, l'adozione di eventuali misure migliorative, al fine di incrementare l'efficacia delle regole tecniche (provv. 20 giugno 2019, n. 135, doc. web n. 9122419).

4.1.7. La fatturazione elettronica

A seguito dei provvedimenti adottati dal Garante (provv. 18 novembre e 20 dicembre 2018, doc. web nn. 9059949 e 9069072), l'Agenzia delle entrate ha dato corso alle prescrizioni ivi contenute, informando l'Autorità delle attività svolte e chiedendo di prorogare il periodo transitorio di conservazione integrale delle fatture per ragioni tecniche oltre che al fine di consentire ai contribuenti di valutare pienamente l'eventuale adozione del sistema di consultazione offerto facoltativamente dall'Agenzia delle entrate.

Al riguardo, è però intervenuto il legislatore prevedendo la memorizzazione integrale di tutte le fatture elettroniche emesse e ricevute, misura ritenuta non conforme al RGPD dal Garante nel predetto provvedimento. La questione è stata quindi trattata nell'ambito della memoria del Presidente del Garante avente ad oggetto il disegno di legge C. 2220, di conversione in legge del decreto-legge n. 124/2019, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili, in Commissione VI (Finanze) della Camera dei deputati (memoria del 5 novembre 2019, doc. web n. 9178137); nel novellare l'art. 1, d.lgs. 5 agosto 2015, n. 127, si dispone infatti la memorizzazione dei *file* delle fatture elettroniche fino al 31 dicembre dell'ottavo anno successivo a quello di presentazione della dichiarazione di riferimento, ovvero

fino alla definizione di eventuali giudizi (art. 14). I dati da memorizzare includono, così, quelli inerenti alla natura, qualità e quantità dei beni e servizi oggetto dell'operazione, di cui all'art. 21, comma 2, lett. *g*), d.P.R. n. 633/1972, resi accessibili, secondo quanto previsto dal comma 1 della disposizione in esame, alla Guardia di finanza nell'assolvimento delle funzioni di polizia economica e finanziaria, nonché all'Agenzia delle entrate e alla stessa Guardia di finanza per le attività di verifica e analisi del rischio fiscale, disponendo, dunque, l'estensione dell'ambito di utilizzazione dei dati di fatturazione a tutte le funzioni di polizia economica-finanziaria demandate al Corpo della Guardia di finanza dal d.lgs. n. 68/2001 e non soltanto – come a legislazione vigente – al solo scopo dell'effettuazione delle verifiche fiscali. La norma estende, quindi, tanto l'oggetto della memorizzazione quanto l'ambito di utilizzazione dei dati di fatturazione, senza peraltro escluderne alcune categorie, quali i dati non fiscalmente rilevanti o quelli inerenti alla descrizione delle prestazioni fornite (suscettibili di comprendere anche dati idonei a rivelare lo stato di salute o l'eventuale sottoposizione dell'interessato a procedimenti penali, come per le fatture relative a prestazioni in ambito sanitario o forense): profili rispetto ai quali il Garante aveva già espresso perplessità, alla luce del principio di proporzionalità, in relazione allo schema di provvedimento del Direttore dell'Agenzia delle entrate in materia di fatturazione elettronica.

Annualmente risultano infatti essere emesse complessivamente circa 2,1 miliardi di fatture che, di regola, contengono dati anche particolarmente analitici nell'individuazione dei beni e i servizi ceduti – spesso a fini di garanzia, assicurativi o per prassi commerciali –, con la descrizione puntuale delle prestazioni rese, dei rapporti fra cedente e cessionario e altri soggetti, riferiti anche a sconti applicati, fidelizzazioni, abitudini di consumo, oltre a dati obbligatori imposti da specifiche normative di settore, con particolare riguardo ai trasporti, alle forniture di servizi energetici o di telecomunicazioni (tipologie dei consumi, fatturazione dettagliata, regolarità dei pagamenti, appartenenza a particolari categorie di utenti). La presenza, all'interno dei *file* delle fatture elettroniche (ad es. anche di documenti allegati), di informazioni non rilevanti a fini fiscali – che, come detto, possono riguardare anche categorie particolari di dati personali e dati personali relativi alle condanne penali e ai reati di cui agli artt. 9 e 10 del RGPD, potenzialmente riferibili ad ogni aspetto della vita quotidiana – è, peraltro, espressamente contemplata nel provvedimento dell'Agenzia.

Con specifico riferimento all'utilizzo delle fatture elettroniche a fini di controllo da parte dell'Agenzia delle entrate e della Guardia di finanza, le attività di controllo fiscale effettuate possono essere ricondotte a due tipologie: la prima basata su trattamenti automatizzati e di analisi del rischio (ad es., quelli volti a rilevare le incongruenze tra i dati dichiarati e quelli a disposizione dell'Agenzia nonché quelli relativi all'analisi del rischio evasione) e l'altra, più analitica, fondata sull'esame puntuale della posizione fiscale del contribuente e della documentazione fiscale.

I controlli automatizzati e l'analisi del rischio richiedono, per loro natura, la memorizzazione e l'elaborazione massiva dei dati estratti dai *file* XML delle fatture (cd. dati fattura), tra i quali non dovrebbe rientrare però il campo contenente la descrizione dell'operazione oggetto di fatturazione che, oltre a poter contenere i significativi dati personali di dettaglio (sopra esemplificati) e presentare, quindi, rischi elevati per gli interessati, non si presta ad elaborazioni massive, essendo un campo a testo libero e non strutturato (che richiede quindi un esame puntuale, caso per caso, del contenuto). Con riferimento, invece, ai controlli puntuali talora necessari per l'esame analitico delle fatture, dalla documentazione fornita dall'Agenzia dell'entrate in occasione dei suddetti pareri del 2018 risulta che, negli anni 2016

4

e 2017, sono stati effettuati, rispettivamente, 121.849 e 163.339 accertamenti nei confronti di contribuenti Iva, a fronte di circa 4,7 milioni di soggetti che hanno presentato la dichiarazione Iva.

Alla luce di tali elementi, l'archiviazione integrale di tutte le fatture emesse e ricevute, comprensiva dei dati non fiscalmente rilevanti (oltre che, naturalmente, dei destinatari delle prestazioni fatturate) e di quelli inerenti alla descrizione delle prestazioni fornite, ai fini dell'esecuzione di controlli puntuali nell'ambito di accertamenti fiscali e verifiche, anche da parte della Guardia di finanza, appare quindi sproporzionata. Come già rilevato, gli obblighi di memorizzazione dei *file* XML delle fatture elettroniche a cura degli operatori economici, anche presso l'Agenzia delle entrate, possono invece agevolare i controlli a distanza da parte dell'Agenzia e della Guardia di finanza previsti dall'art. 1, comma 5, d.lgs. n. 127/2015, mediante le nuove modalità di acquisizione delle fatture che dovranno essere individuate con il decreto ministeriale da emanarsi ai sensi della medesima disposizione. L'autenticità e l'integrità di ciascun *file*, indispensabile ai fini dei controlli, è peraltro garantita dalla memorizzazione, da parte dell'Agenzia, di una cd. impronta univoca della fattura (*hash*).

La previsione di un obbligo di memorizzazione (e potenzialmente anche di utilizzazione) di dati personali sproporzionato – per quantità e qualità delle informazioni – rispetto alle reali esigenze perseguite renderebbe, infatti, la norma illegittima per contrasto con il principio di proporzionalità del trattamento dei dati, assurto nella giurisprudenza della Corte di giustizia a parametro ermeneutico essenziale in materia (v. sentenze 20 maggio 2003, nelle cause riunite C-465/00, C-138/01 e C-139/01, Österreichischer Rundfunk e altri, e 9 novembre 2010, nelle cause riunite C-92/09 e 93/09, Volker und Markus Schecke e Eifert, 8 aprile 2004, C- 203/12 e C-594/12, Digital Rights Ireland; 21 dicembre 2016, Tele2 Sverige, C-203/15 e 698/15; in ordine al canone di proporzionalità in via generale, v. pure, per quanto concerne la Corte europea dei diritti umani, sez. II, sent. 28 novembre 2017, Antović and Mirković v. Montenegro, ric. n. 70838/13; Grande Camera, 5 settembre 2017, Bărbulescu c. Romania, ric. n. 61496/08).

Quello della necessità delle misure limitative del diritto alla protezione dati è, peraltro, un principio che la Corte di giustizia (ma anche la Corte EDU) ha più volte valorizzato, ammettendo le misure più invasive solo a fronte della dimostrata inidoneità allo scopo di sistemi meno limitativi del diritto, dal momento che "deroghe e restrizioni" ai diritti fondamentali devono intervenire "entro i limiti dello stretto necessario" (cfr., ex *plurimis*, CGUE, C-362/14, Maximillian Schrems c. Data Protection Commissioner [GC], 6 ottobre 2015).

La stessa Corte costituzionale, con la sentenza n. 20/2019, ha attribuito a tali principi una rilevante funzione etero-integrativa del canone di ragionevolezza di cui all'art. 3 Cost., fondandovi la declaratoria di illegittimità parziale, per violazione appunto del parametro interno così integrato, degli obblighi di pubblicità previsti per i dirigenti pubblici dall'art. 14, comma 1-*bis*, d.lgs. 14 marzo 2013, n. 33.

Il Garante ha pertanto espresso l'invito a vagliare, in sede di conversione, l'effettiva necessità dell'archiviazione integrale dei dati di fatturazione, per la durata prevista, rispetto alla realizzazione delle varie attività di indagine, nei settori tributario ed extratributario, in vista delle quali si consente l'utilizzazione di tali informazioni.

Tuttavia, nonostante le numerose osservazioni formulate, la disposizione normativa non è stata modificata in fase di conversione.

4.2. *La previdenza e l'assistenza sociale*

4.2.1. Il reddito e la pensione di cittadinanza

Con il d.l. 28 gennaio 2019, n. 4, sono stati introdotti il "reddito di cittadinanza" (Rdc) e la "pensione di cittadinanza" (Pdc) quali misure di politica attiva a garanzia del diritto al lavoro e di contrasto alla povertà, alla disuguaglianza e all'esclusione sociale (cfr. in merito anche par. 2.2, n. 17). Il contributo del Garante è stato preordinato a far sì che l'implementazione di tali istituti – che comportano il trattamento, su larga scala, di dati personali, relativi alla salute, alla condizione sociale e alla situazione economica e finanziaria, elaborati anche in esito alla valutazione dello stato di bisogno dei beneficiari del Rdc, relativi principalmente a soggetti vulnerabili (disabili, anziani, persone in cerca di occupazione), anche minori d'età, in grado di condizionare l'accesso a servizi e prestazioni sociali – abbia luogo nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati. Preoccupazione, questa, espressa dal Presidente del Garante anche nel corso di due audizioni presso le competenti Commissioni parlamentari di Senato e Camera in sede di conversione del citato decreto legge (cfr., rispettivamente, la memoria dell'8 febbraio 2019, doc. web n. 9081679 e del 6 marzo 2019, doc. web n. 9089070).

Con la prima memoria il Garante ha sottolineato che il meccanismo, così come delineato dal legislatore nelle norme del decreto-legge, presentava rilevanti criticità, alcune delle quali suscettibili di superamento nell'ambito dei provvedimenti attuativi (inizialmente non previsti), altre invece in sede di conversione. La realizzazione del Rdc presuppone, infatti, un patrimonio informativo complesso e articolato, fondato sull'interconnessione di molteplici banche dati, la circolazione di delicatissime informazioni tra una pluralità di soggetti pubblici, nonché il monitoraggio e la valutazione dei consumi e dei comportamenti dei singoli familiari del beneficiario. Il trattamento dei dati personali, anche se effettuato da amministrazioni pubbliche e preordinato (come in relazione al Rdc) al perseguimento di motivi di rilevante interesse generale, non può comunque eludere le garanzie dei diritti e delle libertà sancite dalla disciplina di protezione dati, anzitutto a vantaggio delle persone che tale beneficio intende tutelare. In questa prospettiva, il legislatore nazionale deve prevedere le condizioni e i limiti necessari, secondo il canone di proporzionalità, a coniugare la dignità e i diritti fondamentali della persona con esigenze di interesse generale, quali il contrasto di frodi e abusi, nonché la realizzazione di percorsi di inclusione sociale e altri obiettivi di politica attiva del lavoro.

Non essendo stato richiesto sul decreto-legge il parere di cui all'art. 36, par. 4, del RGPD, che prevede la consultazione preventiva dell'Autorità, non è stato possibile evidenziare nel dettaglio *ab origine* i rischi derivanti dalle diverse attività di trattamento (che incidono su un numero elevato di cittadini, ivi inclusi coloro i quali non sono interessati a richiedere il Rdc), né individuare preventivamente misure idonee a mitigarli, così da evitare limitazioni dei diritti degli interessati sproporzionate ed ingiustificate rispetto al legittimo obiettivo di interesse pubblico perseguito. Le disposizioni esaminate non hanno individuato con sufficiente precisione, come richiesto dai principi di trasparenza nei confronti degli interessati, minimizzazione dei dati trattati e protezione dei dati personali per progettazione e impostazione predefinita, i titolari del trattamento, le tipologie di dati trattati, i soggetti ai quali essi possono essere comunicati e le rispettive finalità nonché i termini di conservazione dei dati, proporzionati (e non eccedenti) rispetto agli scopi perseguiti.

In più punti, quindi, la disciplina del Rdc, così come inizialmente formulata nel d.l. n. 4/2019, non soddisfava i requisiti richiesti dal diritto dell'Unione; il decreto-legge conteneva infatti previsioni di portata generale, inidonee a definire con

4

sufficiente chiarezza le modalità di svolgimento delle procedure di consultazione e verifica delle varie banche dati da parte di numerose categorie di soggetti, senza specificarne il ruolo assunto in relazione alla protezione dei dati personali; alcune criticità caratterizzavano altresì la disciplina del "monitoraggio" sull'utilizzo della carta Rdc da parte dei beneficiari. Forti perplessità destavano pure alcune disposizioni sulla disciplina di rilascio delle attestazioni Isee e dell'Isee precompilato grazie al patrimonio informativo dell'Agenzia delle entrate (cfr. art. 10, d.lgs. n. 147/2017), suscettibili di pregiudicare la sicurezza dei dati contenuti nell'Anagrafe tributaria e, soprattutto, nell'Archivio dei rapporti finanziari dell'Agenzia delle entrate, in ragione degli elevati rischi connessi al relativo trattamento. Un ultimo rilievo riguardava l'architettura del sito web del Governo dedicato al Rdc, in relazione ad alcune carenze nell'informativa sul trattamento dei dati e nelle modalità tecniche della sua implementazione.

Rispetto alle criticità che tale sistema presentava nella sua architettura originaria, il testo normativo è stato migliorato in sede emendativa, recependo i rilievi del Garante. In tal senso, nella seconda memoria sopra citata, è stata rilevata con favore l'istituzione di un unico Sistema informativo per il Rdc, al fine di evitare duplicazioni di banche dati, presso il quale opereranno le due piattaforme digitali finalizzate a consentire l'attivazione e la gestione dei Patti per il lavoro e dei Patti per l'inclusione sociale, connessi al Rdc, quali strumenti per rendere disponibili le informazioni alle amministrazioni centrali e ai servizi territoriali coinvolti, nel rispetto dei principi di minimizzazione, integrità e riservatezza dei dati. Il Sistema informativo dovrà essere attuato secondo modalità e termini rimessi a un ulteriore decreto ministeriale, unitamente al quale verrà predisposto un piano tecnico di attivazione e interoperabilità delle due piattaforme dedicate al Rdc, prevedendo misure a tutela degli interessati, modalità di accesso selettivo alle informazioni necessarie per il perseguimento delle specifiche finalità perseguite nonché adeguati tempi di conservazione dei dati. È stata prevista la consultazione dell'Autorità in ordine alla predisposizione, da parte dell'Inps, del modulo di domanda per ottenere il beneficio e alla definizione delle comunicazioni dovute allo stesso Istituto in caso di variazione dei requisiti posseduti dai beneficiari. Sono state inoltre superate le criticità riscontrate in ordine al monitoraggio centralizzato e sistematico dei singoli acquisti effettuati dai beneficiari tramite la carta del Rdc che, così come inizialmente prospettato, era suscettibile di comportare anche l'acquisizione di informazioni sensibili. Al tal fine è stato previsto che tutte le movimentazioni sulla carta siano controllate mediante la verifica dei soli importi complessivamente spesi e prelevati e secondo modalità che saranno definite con decreto, previo parere del Garante.

In linea con le perplessità evidenziate dall'Autorità, è stata espunta anche la previsione relativa all'attribuzione, agli operatori dei centri per l'impiego e dei servizi comunali, di funzioni di controllo puntuale sulle scelte di consumo individuali e sui comportamenti dei beneficiari, nonché di valutazione di eventuali anomalie suscettibili di rivelare l'insussistenza dei requisiti dichiarati, con la conseguente segnalazione alle piattaforme per il Rdc, in assenza di procedure a tutela degli interessati e di criteri normativamente individuati. L'attività di controllo sui beneficiari del Rdc, così come sugli enti di formazione accreditati, potrà essere oggetto di una specifica convenzione tra Ministero del lavoro, Mef e Guardia di finanza. Sono state altresì recepite le obiezioni sollevate dall'Autorità in ordine alle modifiche apportate dal decreto-legge alla disciplina di rilascio delle attestazioni Isee, che – anche prescindendo dal funzionamento del Rdc – erano suscettibili di esporre a rischi di accessi abusivi anche soggetti inconsapevoli, non interessati da tale beneficio, rischiando di pregiudicare la sicurezza dei dati contenuti nell'Anagrafe tributaria e,

soprattutto, nell'Archivio dei rapporti finanziari dell'Agenzia delle entrate, soggetti a strettissimi vincoli d'accesso persino nell'ambito delle ordinarie attività di controllo tributario. In conformità ai rilievi del Garante, sono state riformulate le disposizioni che subordinavano la precompilazione della Dichiarazione sostitutiva unica (Dsu) a un complesso meccanismo di consenso/inibizione al trattamento da parte di ogni componente maggiorenne del nucleo familiare, che avrebbe potuto comportare un'ingiustificata comunicazione al dichiarante dei dati dei componenti del nucleo familiare di appartenenza presenti negli archivi dell'Inps e dell'Agenzia delle entrate, anche in contrasto con la volontà degli interessati. In particolare, ferma restando la possibilità di presentazione della Dsu in modalità non precompilata, è stata demandata a un decreto ministeriale – da adottarsi previo parere del Garante – l'individuazione delle modalità tecniche necessarie a consentire l'accesso alla dichiarazione precompilata resa disponibile in via telematica dall'Inps, assicurando misure tecniche e organizzative (ivi incluse opportune modalità di comunicazione al dichiarante di eventuali difformità riscontrate) per scongiurare rischi di violazioni della sicurezza dei dati e dei sistemi. Riguardo infine all'architettura del sito web del Governo dedicato al Rdc, il Garante ha rilevato ulteriori criticità relative alle modalità tecniche della sua implementazione (come la trasmissione a terzi dei dati di navigazione dei visitatori del medesimo sito, quali indirizzi IP e orario di connessione, non necessaria in termini funzionali) ed ha ribadito che, in caso di ricorso a *font* tipografici (stili di carattere) esterni che comportano il conferimento a fornitori di dati riferibili ai visitatori del sito web, appare preferibile configurare lo stesso – pur mantenendone invariate le caratteristiche grafiche e funzionali – in modo che tali *font* vengano resi disponibili direttamente dal titolare del trattamento, evitando l'ulteriore circolazione di dati personali degli utenti del sito.

I pareri sulla disciplina di attuazione

Con un primo parere reso all'Inps, il Garante si è espresso favorevolmente sullo schema di provvedimento attuativo dell'art. 5, d.l. n. 4/2019, concernente il modulo di domanda di Rdc e Pdc, in cui sono state tenute in considerazione le osservazioni fornite dall'Ufficio in termini di rispetto dei principi di liceità, correttezza, trasparenza e minimizzazione, con riferimento, in particolare, all'individuazione delle informazioni da raccogliere presso il richiedente, relative a tutti i componenti del nucleo familiare; alla puntuale indicazione delle amministrazioni pubbliche presso le quali l'Inps è chiamato a verificare il possesso dei requisiti per l'erogazione del beneficio; all'ambito di comunicazione a soggetti terzi delle informazioni; alla necessità e alle modalità di comunicazione delle variazioni dei requisiti patrimoniali previsti e alle relative conseguenze; al trattamento dei dati relativi alle condanne penali e ai reati; all'esaustività delle informazioni fornite a tutti i componenti del nucleo familiare; all'indicazione del periodo di conservazione dei dati (provv. 29 marzo 2019, n. 82, doc. web n. 9106306).

Successivamente, nell'ambito della predisposizione del citato decreto del Ministro del lavoro e delle politiche sociali, da adottare ai sensi dell'art. 6, comma 1, d.l. n. 4/2019, istitutivo del Sistema informativo del reddito di cittadinanza (Sistema Rdc) presso il medesimo Ministero, l'Ufficio ha collaborato con il Ministero del lavoro e delle politiche sociali per assicurare che il nuovo sistema, comprensivo delle due apposite piattaforme digitali dedicate al Rdc, fosse realizzato nel pieno rispetto del RGPD e del Codice.

In esito a tale attività il Garante ha reso un parere favorevole, preceduto dalle indicazioni fornite dall'Ufficio nel corso di numerosi incontri preparatori, sullo schema di decreto volto a disciplinare il funzionamento del Sistema Rdc e delle relative piattaforme, corredato dei piani tecnici di attivazione e di interoperabilità tra le stesse, e a individuare misure appropriate e specifiche a tutela degli interessati,

nonché modalità di accesso selettivo alle informazioni necessarie per il perseguimento delle specifiche finalità e adeguati tempi di conservazione dei dati. Tra le misure introdotte si segnalano: l'esatta individuazione delle finalità di volta in volta perseguite nell'ambito dei trattamenti effettuati nel Sistema informativo del Rdc; la minimizzazione dei dati personali, assicurando, in relazione ad ogni flusso informativo, il rispetto del principio di proporzionalità, soprattutto con riferimento alle categorie di dati di cui agli artt. 9 e 10 del RGPD; l'adozione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi; l'individuazione di tempi di conservazione dei dati proporzionati rispetto alle finalità perseguite; l'utilizzo di dati anonimi o aggregati da parte del Ministero, per fini di analisi, controllo e monitoraggio, e da parte delle regioni, per fini di programmazione, statistica e ricerca e in relazione agli ambiti territoriali di competenza. Il Garante si è espresso altresì ai sensi degli artt. 36, par. 5, del RGPD e 2-*quinquiesdecies* del Codice, autorizzando l'avvio del trattamento a rischio elevato effettuato, tramite le suddette piattaforme, per l'esecuzione di un compito di interesse pubblico in considerazione delle misure introdotte nel predetto schema di decreto e quelle illustrate nella valutazione di impatto predisposta dal Ministero del lavoro e dall'Anpal (provv. 20 giugno 2019, n. 138, doc. web n. 9122428).

4.2.2. L'Isee precompilato

Il Garante si è occupato anche della tematica inerente all'attuazione del cd. Isee precompilato, la cui disciplina è stata modificata con il decreto-legge in materia di Rdc. In particolare, è previsto che la Dichiarazione sostitutiva unica a fini Isee (Dsu) possa essere precompilata da parte dell'Inps, in cooperazione con l'Agenzia delle entrate – utilizzando le informazioni disponibili nell'Anagrafe tributaria, nel Catasto e negli archivi dell'Inps, nonché le informazioni su saldi e giacenze medie del patrimonio mobiliare dei componenti il nucleo familiare – mantenendo comunque la facoltà, per il dichiarante, di optare per la presentazione della Dsu in modalità non precompilata (art. 10, d.lgs. 15 settembre 2017, n. 147, come modificato dal d.l. n. 4/2019 e ss.mm.).

A questo proposito, il Garante ha reso parere favorevole sullo schema di decreto del Ministero del lavoro e delle politiche sociali, attuativo dell'art. 10, comma 2, d.lgs. n. 147/2017, con il quale sono state individuate le modalità tecniche per consentire al cittadino di accedere alla dichiarazione precompilata resa disponibile in via telematica dall'Inps, nonché quelle secondo cui, in caso di Dsu non precompilata, in sede di attestazione dell'Isee, vengono riportate le eventuali omissioni o difformità riscontrate nei dati dichiarati. L'Autorità ha ritenuto che lo schema di decreto, che ha tenuto conto delle indicazioni fornite nel corso di tavoli tecnici con l'Ufficio, fosse conforme ai principi di *privacy by design* e *by default*, in ragione delle misure individuate con particolare riferimento ai rischi di accesso non autorizzato ai dati o di trattamento non consentito o non conforme alle finalità della raccolta. Sono state, infatti, disciplinate le modalità attraverso cui è consentito al dichiarante di accedere direttamente alla Dsu precompilata, anche in relazione agli altri componenti il nucleo familiare maggiorenni che lo abbiano a tal fine appositamente delegato, previo conferimento di adeguati elementi di riscontro, prevedendo altresì che i medesimi elementi di riscontro debbano essere conferiti anche in relazione al dichiarante, in caso di presentazione della Dsu tramite un Caf delegato. Sono stati altresì messi a disposizione degli interessati strumenti volti a permettere l'inibizione del trattamento dei dati necessari all'elaborazione della Dsu precompilata e all'attestazione dell'Isee nel caso di Dsu presentata nella modalità non precompilata, in attuazione dell'art. 21 del RGPD. Infine, nello schema sono state individuate, nel

rispetto del principio di minimizzazione, le informazioni, riferite anche agli altri componenti maggiorenni del nucleo familiare, da riportare nell'attestazione Isee, in caso di omissioni ovvero difformità dei valori relativi al patrimonio mobiliare dichiarati (provv. 20 giugno 2019, n. 136, doc. web n. 9124390).

Successivamente, il Garante ha reso parere favorevole anche sulla proposta di Dsu e sulle relative istruzioni, formulate dall'Inps e trasmesse dal Ministero del lavoro e delle politiche sociali ai sensi dell'art. 10, comma 3, d.P.C.M. 5 dicembre 2013, n. 159, volte ad aggiornare i modelli precedentemente in vigore, recependo le novità introdotte con legge. In particolare, le modifiche hanno riguardato – oltre al calcolo dell'Isee corrente per coloro che, a seguito di presentazione di una prima Dsu, abbiano la necessità di comunicare determinate condizioni (variazione della situazione lavorativa o interruzione dei trattamenti previdenziali, assistenziali e indennitari, variazione significativa della situazione reddituale del nucleo familiare) – la definizione di nucleo familiare rilevante, con l'indicazione dei componenti e la specificazione delle corrispondenti informazioni da riportare nella Dsu, e l'aggiornamento dei termini di validità (provv. 19 settembre 2019, n. 176, doc. web n. 9163393).

Infine, il Garante è stato chiamato ad esprimersi sullo schema di provvedimento congiunto del Direttore dell'Inps e del Direttore dell'Agenzia delle entrate, volto a disciplinare le specifiche tecniche, i meccanismi di delega da parte degli interessati e le misure di sicurezza atte a ridurre al minimo i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, ai fini dell'accesso alla Dsu precompilata ai sensi dell'art. 6 dello schema di decreto sopra descritto, adottato dal Ministero del lavoro e delle politiche sociali il 9 agosto 2019. L'Autorità ha ritenuto conforme al RGPD e al Codice lo schema di provvedimento nel quale sono state recepite le indicazioni fornite dall'Ufficio al fine di rispettare i principi di *privacy by design* e *by default.* In primo luogo, nel rispetto del principio di esattezza dei dati, lo schema ha individuato puntualmente le informazioni utilizzate per la pre-compilazione e il pre-caricamento dei dati contenuti nella Dsu, con riferimento al canone di locazione della casa di abitazione del nucleo familiare e agli assegni per il mantenimento dei figli. Considerato che, in tale contesto, i trattamenti effettuati su larga scala da parte dell'Inps e dall'Agenzia delle entrate per l'esecuzione di un compito di interesse pubblico sono caratterizzati da un rischio elevato per i diritti e le libertà degli interessati, nell'ambito dell'istruttoria sono state esaminate, ai sensi dell'art. 2-*quinquiesdecies* del Codice, anche le valutazioni di impatto prodotte dai titolari del trattamento.

Il Garante ha ritenuto che le numerose misure tecniche e organizzative previste nello schema e nelle valutazioni di impatto possano essere ritenute adeguate a rafforzare la sicurezza del trattamento al fine di mitigare il rischio di accessi abusivi e non autorizzati ai dati oggetto di precompilazione da parte dell'Inps, relativi, in particolare, alla consistenza del patrimonio finanziario degli interessati. È stato introdotto uno specifico meccanismo di verifica delle deleghe rilasciate dai componenti del nucleo familiare in caso di accesso *online* da parte del dichiarante e sono state altresì rafforzate le modalità di accesso all'Isee precompilato da parte dei Caf, su delega degli interessati, prevedendo, tra l'altro, la tenuta di un apposito registro delle deleghe e la definizione di un termine di conservazione della documentazione acquisita (delega e documento di riconoscimento) pari a cinque anni. Inoltre i Caf, a valle di una prima fase di sperimentazione di tre mesi, dovranno trasmettere all'Inps i codici *hash* dei *file* contenenti le deleghe e i documenti di riconoscimento e l'Istituto dovrà porre in essere specifici controlli sugli accessi effettuati *online* da parte del dichiarante e da parte dei Caf.

Fermo restando il più generale diritto di opposizione previsto dall'art. 21 del

RGPD esercitabile nei confronti del titolare del trattamento, al fine di fornire agli interessati strumenti di tutela nei confronti di accessi abusivi e non autorizzati ai propri dati personali, sono state previste, sul sito dell'Inps e dell'Agenzia delle entrate, specifiche modalità di inibizione all'utilizzo dei dati per l'elaborazione della dichiarazione Dsu precompilata, ovvero dell'attestazione dell'Isee, nel caso di Dsu presentata nella modalità non precompilata. Gli interessati, in ogni caso, potranno sempre monitorare il rilascio di dichiarazioni Isee che li riguardino accedendo all'area autenticata del sito dell'Inps e dell'Agenzia delle entrate, dove saranno informati del trattamento dei propri dati personali ai fini di una Dsu precompilata, del soggetto che ha richiesto tale Dsu, nonché del Caf che abbia eventualmente acquisito la Dsu.

Con il provvedimento, adottato anche ai sensi dell'art. 2-*quinquiesdecies* del Codice, il Garante ha autorizzato il suddetto trattamento prescrivendo all'Inps di trasmettere, al termine della prevista fase di sperimentazione (e comunque non oltre 6 mesi dall'avvio del trattamento), una nuova valutazione di impatto aggiornata, che tenga conto delle eventuali anomalie riscontrate e che riesamini, in modo esaustivo, i diversi scenari di rischio connessi all'accesso alla Dsu precompilata *online* da parte del dichiarante e da parte dei Caf (provv. 18 dicembre 2019, n. 225, doc. web n. 9220741).

4.3. *Vigilanza su altre grandi banche dati pubbliche*

Anche in relazione ad altre grandi banche dati pubbliche l'attività consultiva del Garante si è resa necessaria per assicurare il rispetto dei principi in materia di protezione dei dati personali fin dalla progettazione e per impostazione predefinita.

Modalità di consultazione della Bdna da parte di Agea

L'Autorità è stata infatti interpellata in relazione a una convenzione tra l'Agenzia per le erogazioni in agricoltura (Agea) e il Ministero dell'interno, predisposta a seguito delle modifiche apportate al d.lgs. 6 settembre 2011, n. 159, recante il codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia. Tale documentazione ora deve essere richiesta in tutte le ipotesi di aiuti europei su terreni agricoli e zootecnici demaniali in concessione, a prescindere dal loro valore, e su tutti i terreni agricoli che usufruiscono di fondi europei per un importo superiore a 5.000 euro (artt. 83 e 91). La convenzione ha previsto procedure di interscambio di dati basate su flussi automatizzati in quanto, in ragione delle nuove norme, la richiesta della documentazione antimafia con le modalità ordinarie rispetto a un numero estremamente elevato di soggetti, soprattutto in prossimità delle scadenze comunitarie, non avrebbe consentito il rispetto dei termini di erogazione degli aiuti comunitari. È stato evidenziato che, in conformità al d.lgs. n. 159/2011, il funzionamento della Banca dati nazionale unica della documentazione antimafia (Bdna) è disciplinato dal d.P.C.M. 30 ottobre 2014, n. 193, regolamento avente ad oggetto le modalità di funzionamento, accesso, consultazione e collegamento con il Ced, di cui all'articolo 8 della legge 1° aprile 1981, n. 121, della Bdna della documentazione antimafia, sul quale il Garante ha reso a suo tempo il parere favorevole (provv. 30 gennaio 2014, n. 39, doc. web n. 2924878).

Al fine di migliorare la conformità della convenzione al quadro normativo di riferimento, è stata rappresentata la necessità di rivedere alcune delle funzionalità introdotte; è stato, altresì, evidenziato che le agevolazioni nelle modalità di interrogazioni della Bdna avrebbero potuto essere attuate con lo strumento della convenzione, solo ove compatibili con i menzionati d.lgs. n. 159/2011 e d.P.C.M. n. 193/2014, previa valutazione dell'impatto sul diritto alla protezione dei dati. Ciò

alla luce del fatto che la convenzione intendeva introdurre modalità di consultazione contestuale della documentazione antimafia per un numero significativamente più elevato di soggetti, avvalendosi anche di flussi automatizzati (artt. 10, 35 e 36 del RGPD; art. 2-*octies* del Codice). Qualora per raggiungere tale obiettivo si fossero rese necessarie modifiche sostanziali alla disciplina relativa alle modalità di accesso e consultazione, come previste dal d.P.C.M. citato, si è rappresentata la necessità di attuarle con apposito regolamento (art. 17, comma 3, l. 23 agosto 1988, n. 400), previo parere dell'Autorità.

Portale consumi energia e gas

Il Garante ha reso parere favorevole sugli schemi della deliberazione recante l'istituzione del Portale dei consumi di energia elettrica e di gas naturale e del relativo regolamento di funzionamento, ai sensi dell'art. 1, comma 8, l. 27 dicembre 2017, n. 2015, predisposti dall'Arera. Tale Portale è realizzato al fine di rendere disponibili ai clienti finali, a partire dal 1° luglio 2019, i propri dati di consumo, estratti dal Sistema informativo integrato (SII), gestito, in qualità di titolare del trattamento, da Acquirente unico s.p.a. Nella predisposizione di tali atti l'Arera ha tenuto conto delle indicazioni fornite dall'Ufficio, volte a dare maggiore trasparenza al trattamento dei dati effettuato da parte del Gestore nell'ambito del Portale e del SII, individuando in modo chiaro le finalità di interesse pubblico perseguite nell'ambito del Portale. È stata garantita, inoltre, la minimizzazione dei dati personali funzionali all'architettura del Portale e alla relativa interfaccia con il SII, nonché rispetto alle funzioni di *web analytics* e reportistica, assicurando adeguate misure di sicurezza, con particolare riguardo all'utilizzo dello Spid, ai controlli sugli accessi ai dati e alle attestazioni periodiche di sicurezza.

Il Garante ha comunque evidenziato che il trattamento effettuato da Acquirente unico s.p.a. attraverso il Portale per l'esecuzione di un compito di interesse pubblico presenta rischi elevati per i diritti e le libertà degli interessati, in quanto ha per oggetto dati dei consumi individuali, per fascia oraria, di energia elettrica e gas naturale alla massima granularità disponibile, relativi alla totalità dei clienti su scala nazionale, con una profondità storica, a regime, di 36 mesi. Pertanto Acquirente Unico s.p.a., titolare del trattamento, è stata autorizzata, ai sensi dell'art. 58, par. 3, lett. *c*), del RGPD e dell'art. 2-*quinquiesdecies* del Codice, a trattare i dati personali nell'ambito del Portale, a condizione di trasmettere al Garante, prima dell'avvio del trattamento, la valutazione di impatto sulla protezione dei dati, al fine di rappresentare, in particolare, le misure tecniche e organizzative nonché le garanzie per gli interessati adottate in concreto (provv. 20 giugno 2019, n. 131, doc. web n. 9123551).

Sinfi

Il Mise ha chiesto un parere sullo schema di decreto ministeriale sulle procedure di consultazione e accesso al Sistema informativo nazionale federato delle infrastrutture (Sinfi), volto a modificare e integrare il previgente decreto dell'11 maggio 2016 (a sua volta, adottato ai sensi dell'art. 4, comma 1, d.lgs. 15 febbraio 2016, n. 33) al fine di stabilire regole di accesso e consultazione dei dati raccolti in tale sistema, sì da mettere a disposizione di un'ampia platea di soggetti i risultati delle attività svolte in tale ambito dal Ministero. Nell'analizzare lo schema, il Garante ha rilevato che le richieste di accesso al Sinfi da parte di soggetti privati (operatori di rete e altri soggetti interessati) sono assoggettate alle ordinarie regole poste dalla legge 7 agosto 1990, n. 241, mentre quelle provenienti dalle p.a., di norma in relazione al territorio di rispettiva competenza, sono consentite, mediante l'uso del Sistema pubblico di connettività, nel rispetto del principio di leale cooperazione istituzionale di cui all'art. 22, comma 5, della medesima l. n. 241/1990. Rilevata, pertanto, l'assenza di specifiche criticità per i diritti e le libertà degli interessati, è stato reso parere favorevole, fermo restando, più in generale, il rispetto della normativa in materia di protezione dei dati personali nell'ambito del Sinfi, con particolare riferimento alla

corretta definizione del ruolo assunto dai soggetti coinvolti nel trattamento dei dati personali e agli obblighi di sicurezza (provv. 20 giugno 2019, n. 132, doc. web n. 9123563).

4

Sistemi di gioco VLT

Il Garante ha espresso parere favorevole su uno schema di decreto del Direttore dell'Agenzia delle dogane e dei monopoli che ha modificato le regole tecniche per la produzione dei sistemi di gioco VLT, in attuazione dell'art. 9-*quater*, d.l. 12 luglio 2018, n. 87. In base a tale disposizione, al fine di impedire l'accesso ai giochi d'azzardo da parte dei minori, è sempre necessario verificare l'età dei giocatori utilizzando la tessera sanitaria. Nell'ambito delle interlocuzioni intercorse con l'Ufficio, l'Agenzia ha individuato nello schema misure volte ad assicurare il rispetto dei principi di minimizzazione e di *privacy by design* e *by default*, prevedendo che le modalità di accertamento della maggiore età abbiano luogo mediante l'estrazione delle informazioni registrate nella tessera sanitaria (codice fiscale ed identificativo della tessera) senza che le stesse siano memorizzate nelle banche dati del sistema di gioco VLT. Infatti, la verifica della maggiore età del giocatore deve essere effettuata confrontando la data corrente con quella estratta dal codice fiscale della tessera sanitaria ed assicurando meccanismi idonei ad impedire l'avvio di una sessione di gioco in tutti i casi in cui non sia accertata la maggiore età del giocatore tramite lettura della tessera sanitaria e introducendo soluzioni tecniche in grado di visualizzare a video la presenza/assenza della tessera sanitaria nell'apposito dispositivo di lettura (provv. 24 luglio 2019, n. 151, doc. web n. 9126407).

Fir

L'art. 1, commi da 493 a 507, l. 30 dicembre 2018, n. 145, ha istituito il Fondo indennizzo risparmiatori (Fir), che eroga indennizzi a favore dei risparmiatori che hanno subìto un ingiusto pregiudizio da parte di banche e loro controllate aventi sede legale in Italia, poste in liquidazione coatta amministrativa tra il 16 novembre 2015 e il 1° gennaio 2018, in ragione delle violazioni massive degli obblighi di informazione, diligenza, correttezza, buona fede oggettiva e trasparenza. In particolare, il comma 501 ha previsto l'istituzione di un'apposita Commissione tecnica (supportata nelle sue funzioni dal Mef) per l'esame delle domande di indennizzo e devoluto ad un decreto del Ministro dell'economia e delle finanze la definizione delle modalità di presentazione della domanda di indennizzo nonché i piani di riparto delle risorse disponibili. A questo proposito, il Ministero ha sottoposto al parere del Garante uno schema di decreto di modifica del precedente d.m. 10 maggio 2019 (attuativo delle succitate disposizioni e adottato in essenza del parere dell'Autorità) al fine di effettuare gli opportuni adeguamenti a quanto nel frattempo stabilito dall'art. 36, d.l. 30 aprile 2019, n. 34 (a seguito delle modifiche apportate, in sede di conversione, dalla l. 28 giugno 2019, n. 59) e alla disciplina in materia di trattamento dei dati personali. Il Garante ha reso parere favorevole su tale schema di decreto – nel quale sono state recepite le indicazioni fornite dall'Ufficio circa la corretta indicazione della base giuridica del trattamento dei dati effettuato dalla Commissione tecnica e i presupposti normativi per la raccolta, da parte della stessa, dei dati finalizzati a riscontrare le dichiarazioni presentate dai richiedenti –, precisando che i riscontri presso l'Agenzia delle entrate non potranno avvenire, in via generale, consultando i dati contenuti nell'Archivio dei rapporti finanziari, visti i rischi elevati per i diritti e le libertà degli interessati. Sono state altresì correttamente disciplinate le modalità di presentazione delle domande e sono state previste misure per la sicurezza dei trattamenti effettuati nell'ambito della piattaforma informatica (provv. 30 luglio 2019, n. 155, doc. web n. 9126476).

Servizio *IT-alert*

L'art. 28, d.l. 18 aprile 2019, n. 32 (convertito, con modificazioni, dalla l. 14 giugno 2019, n. 55), ha modificato il Cad, istituendo il Sistema di allarme pubblico, denominato "Servizio di IT-*alert*", la cui attuazione è rimessa ad un

apposito decreto del Presidente del Consiglio dei Ministri, sul cui schema è stato consultato il Garante. Nel suo parere, l'Autorità ha sottolineato che il Sistema di allerta pubblico è volto a trasmettere, ai terminali presenti in una determinata area geografica, messaggi IT-*alert* riguardanti gli scenari di rischio, l'organizzazione dei servizi di protezione civile del proprio territorio e le misure di autoprotezione, escludendo l'utilizzo per finalità diverse da quelle ivi previste dei dati eventualmente raccolti. Tale trasmissione non comporta la conoscenza dei numeri di telefono dei terminali mobili contattati e, conseguentemente, nemmeno dell'identità dei contraenti o utenti delle reti di comunicazione mobile cellulare; pertanto, gli apparati di trasmissione di ciascun operatore potranno inviare il messaggio ai propri clienti, ma anche ai clienti di altri operatori di telefonia mobile, in modo del tutto indifferenziato, imprevedibile a priori e, comunque, non tracciabile. Il Sistema di allerta è basato, infatti, sul servizio di *cell broadcast*, disponibile sulle reti pubbliche di telefonia mobile perché previsto dall'architettura di rete GSM, come mezzo di distribuzione e consegna dei messaggi di allarme al dispositivo telefonico del destinatario, con l'invio di brevi messaggi di testo da parte di ciascuna "stazione base" (*Base Transceiver Station*-BTS) della rete pubblica. L'invio del messaggio di allerta avviene rispetto a tutti i dispositivi utente compresi in una determinata area geografica coperta dal segnale radio (cd. cella) in modalità *broadcast* e può essere ripetuto a intervalli di tempo prestabiliti per massimizzare la copertura dei dispositivi destinatari. Al fine di evitare fraintendimenti da parte degli utenti, la normativa tecnica stabilisce che i dispositivi riceventi devono essere in grado di cancellare i messaggi di allerta duplicati, ricevuti in un determinato intervallo di tempo.

Il Garante ha accolto con favore la misura prevista volta a consentire la disattivazione autonoma, da parte dell'interessato, della ricezione dei messaggi di allerta classificati di minore gravità, fermo restando che tale opzione di non visualizzazione di talune tipologie di messaggi *broadcast* debba essere garantita da impostazioni standard di trasmissione e settaggi dei dispositivi riceventi. È stato altresì rilevato che le misure tecniche e organizzative predisposte risultano idonee a garantire un livello di sicurezza adeguato ai rischi, con particolare riferimento alla necessaria certificazione dei messaggi che ne assevera la provenienza da fonti autorizzate.

Il Garante ha tuttavia ritenuto che, al fine di meglio garantire la correttezza e la trasparenza nei confronti dei destinatari dei messaggi, debba essere assicurata la più ampia conoscibilità delle informazioni relative alle modalità e alle finalità di invio dei messaggi attraverso il Sistema pubblico di allerta tramite specifiche campagne informative, chiarendo che la trasmissione *broadcast* dei messaggi non comporta la conoscenza dei numeri di telefono e dell'identità degli interessati, nonché evidenziando agli utenti le modalità di disattivazione dei messaggi di minore gravità (provv. 17 ottobre 2019, n. 193, doc. web n. 9207188).

4.4. *L'istruzione*

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

In tale ambito, particolare rilievo ha assunto il provvedimento 14 febbraio 2019, n. 44 (doc. web n. 9102421) con il quale il Garante ha espresso, ai sensi dell'art. 36, par. 4, del RGPD, parere favorevole su uno schema di regolamento predisposto

Invalsi

4

dall'Istituto nazionale per la valutazione del sistema educativo di istruzione e di formazione, concernente le modalità di svolgimento delle prove Invalsi dell'ultimo anno della scuola secondaria di secondo grado (cd. grado 13). Lo schema di regolamento presentato ha riprodotto i meccanismi previsti nel regolamento della prova Invalsi del terzo anno della scuola secondaria di primo grado (cd. grado 8) del 16 febbraio 2018, in merito al quale il Garante si era espresso con parere favorevole 15 febbraio 2018, n. 76 (doc. web n. 8081291), differenziandosi da quest'ultimo solo in relazione alla classe in cui le prove vengono somministrate (quinto anno della scuola secondaria di secondo grado). Sono così dettate le regole relative allo svolgimento delle prove Invalsi della "quinta superiore" e si disciplinano, in particolare: le modalità di identificazione dello studente ai fini del corretto espletamento e della restituzione delle prove che, nel caso di alunni con disabilità e di alunni con disturbi specifici di apprendimento (Dsa), possono essere personalizzate; lo svolgimento delle prove, prevedendo che l'Invalsi predisponga un documento contenente informazioni che consentono la sicura identificazione di ciascuno studente; le modalità e i tempi di conservazione dei dati da parte di Invalsi, prevedendo la cancellazione del nome e del cognome degli studenti una volta terminato lo svolgimento delle prove; il trattamento di categorie particolari di dati personali, specificando che il trattamento dei dati relativi alla salute è effettuato in attuazione dello schema di regolamento da parte dell'Invalsi e delle scuole, in qualità di autonomi titolari del trattamento per gli aspetti di competenza, per i motivi di interesse pubblico rilevante di cui all'art. 2-*sexies* del Codice.

Diffusione di dati personali

L'Ufficio ha ricevuto, inoltre, numerosi reclami e segnalazioni aventi a oggetto la diffusione, sul sito web istituzionale di taluni istituti scolastici, di graduatorie d'istituto relative al personale docente o al personale amministrativo, tecnico e ausiliario (Ata), contenenti anche informazioni relative all'indirizzo di residenza, al numero di telefono fisso o di cellulare, all'indirizzo *e-mail* del personale nonché (a seguito degli approfondimenti effettuati) all'indicazione dei titoli di preferenza del personale scolastico e ai dati relativi alla salute dei docenti, contrariamente a quanto previsto dal Codice che ne vieta esplicitamente la diffusione. In seguito all'intervento dell'Autorità, gli istituti scolastici hanno prontamente rimosso tali dati dal sito istituzionale. Graduatorie di docenti e dati personali relativi a docenti sono stati diffusi anche da taluni uffici scolastici regionali.

In tutte le ipotesi richiamate, facendo seguito agli approfondimenti effettuati, l'Ufficio ha proceduto alla notifica di violazione ai sensi dell'art. 166 del Codice con conseguente avvio del procedimento per l'adozione di provvedimenti correttivi/sanzionatori. La diffusione di dati personali è stata inoltre oggetto di verifiche, effettuate dal Garante e culminate con la notifica della violazione ai sensi del richiamato art. 166 del Codice, in relazione a reclami riguardanti ipotesi di diffusione di dati personali, anche relativi alla salute, riguardanti studenti, nonché la diffusione di informazioni concernenti le valutazioni intermedie di candidati a una procedura selettiva bandita da un'università.

Esercizio dei diritti

Numerose le richieste di intervento in relazione al mancato riscontro, da parte del titolare del trattamento, a richieste di esercizio dei diritti in materia di protezione dei dati personali, ai sensi degli artt. 15-22 del RGPD. A seguito delle verifiche istruttorie, gli interessati sono stati invitati a esercitare i diritti con istanza rivolta al titolare e, in altri casi, è stato rivolto al titolare del trattamento l'invito ad aderire spontaneamente alla richiesta formulata dall'interessato. Quando la mancata risposta o il ritardo nel riscontro all'interessato è apparso non giustificato, si è proceduto all'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del RGPD.

Uno dei casi di esercizio dei diritti ha riguardato l'istanza di accesso all'elaborato scritto dell'istante relativo alla prova di italiano sostenuta durante l'esame di maturità. Nella trattazione del caso l'Ufficio ha tenuto conto dell'orientamento della Corte di Giustizia dell'Unione europea (cfr. CGUE 20 dicembre 2017, C-434/16) che, chiamata in via pregiudiziale ad esprimersi in merito alla natura di "dati personali" ai sensi della direttiva 95/46 delle informazioni contenute nelle risposte fornite da un candidato durante un esame, si è espressa affermativamente attribuendo alla locuzione un'accezione estesa, tale da comprendere "potenzialmente ogni tipo di informazioni, tanto oggettive che soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano concernenti la persona interessata" e che "le risposte scritte fornite da un candidato nel corso di un esame professionale e le eventuali annotazioni dell'esaminatore relative a tali risposte costituiscono dati personali. Secondo la Corte, il contenuto di tali risposte riflette, infatti, "il livello di conoscenza e di competenza del candidato in un dato settore nonché, se del caso, i suoi processi di riflessione, il suo giudizio e il suo spirito critico. In caso di esame redatto a mano le risposte contengono, inoltre informazioni morfologiche". La Corte ha inoltre affermato che: "va constatato, poi, che i diritti di accesso e di rettifica […] possono anch'essi trovare giustificazione per quanto riguarda le risposte scritte fornite da un candidato durante un esame professionale […]". In precedenza anche l'Autorità si era espressa sul punto con il parere 26 ottobre 2017, n. 433 (doc. web n. 7156158) affermando che per gli specifici profili inerenti l'accesso civico alla copia degli elaborati scritti del concorso pubblico, si deve tenere altresì presente che in generale l'elaborato scritto presentato a un concorso pubblico è, in linea di massima, indicativo anche di molteplici aspetti di carattere personale circa le caratteristiche individuali, relativi ad esempio alla preparazione professionale, alla cultura, alle capacità di espressione, o al carattere del candidato, che costituiscono aspetti valutabili nella selezione dei partecipanti. Inoltre, in alcuni casi, e a seconda della traccia sottoposta, il contenuto degli elaborati può essere potenzialmente capace di rivelare anche informazioni e convinzioni che possono rientrare nella categoria dei dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice (si pensi alle tracce su temi storici o di cultura generale che potrebbero rivelare "opinioni politiche" o "convinzioni filosofiche o di altro genere").

4.5. *La trasparenza amministrativa e la pubblicità dell'azione amministrativa*

Numerose continuano ad essere le questioni esaminate riguardanti il tema della protezione dei dati personali con riferimento alle esigenze di trasparenza e di pubblicità dell'azione amministrativa che, per esigenze di chiarezza espositiva, si esamineranno distinguendo, da un lato, la materia della pubblicazione di dati personali *online* e, dall'altro, l'accesso a informazioni e documenti detenuti dalla p.a. tramite gli strumenti dell'accesso civico (art. 5, d.lgs. 14 marzo 2013, n. 33) nonché dell'accesso ai documenti amministrativi (artt. 22 ss., l. 7 agosto 1990, n. 241), dandosi qui conto solo dei casi più rilevanti conclusi con provvedimento del Collegio.

4.5.1. La pubblicazione di dati personali online

Tra i casi rispetto ai quali l'Autorità è stata chiamata a pronunciarsi, si è nuovamente presentata la questione della diffusione *online* di dati personali da parte di soggetti pubblici in assenza di un idoneo presupposto normativo (norma di legge o di regolamento). Il Garante ha in proposito censurato il comportamento di un comune che aveva pubblicato sull'albo pretorio *online* una deliberazione

della giunta comunale, contenente dati personali non necessari, quali l'esistenza di un procedimento penale (peraltro archiviato) a carico del segnalante dipendente comunale la cui pubblicazione si è protratta per un periodo di tempo superiore ai quindici giorni previsti dalla normativa di settore (art. 124, d.lgs. 18 agosto 2000, n. 267). È stato rilevato che tale condotta configurava una violazione dei principi di liceità e minimizzazione del trattamento (art. 5, par. 1, lett. *a*) e *c*), del RGPD) nonché dell'art. 6, par. 1, lett. *c*) ed *e*); par. 2 e par. 3, lett. *b*), del RGPD, considerando che erano stati diffusi dati personali in assenza di un idoneo presupposto normativo (per il periodo eccedente i tempi di pubblicazione previsti dall'art. 124, comma 1, d.lgs. n. 267/2000) in violazione dell'art. 19, comma 3, del Codice (vigente all'epoca dei fatti, ma il cui contenuto è confluito con analoghe disposizioni nell'art. 2-*ter*, commi 1 e 3, del Codice). In relazione ai predetti elementi, ai sensi dell'art. 83, del RGPD, è stata comminata all'ente locale la sanzione amministrativa di 6.000,00 euro (con possibilità di definire la controversia mediante il pagamento di un importo pari alla metà della sanzione irrogata ai sensi dell'art. 166, comma 8, del Codice): ciò in quanto la gravità del comportamento tenuto non poteva essere bilanciata dalle giustificazioni fornite dall'amministrazione titolare del trattamento (secondo cui la violazione sarebbe stata causata da un errore di valutazione da parte del responsabile del procedimento e da un errore informatico commesso dalla società incaricata della pubblicazione); per la determinazione dell'importo della sanzione, alla luce di quanto previsto dall'art. 83, par. 2, del RGPD, sono state tenute in considerazione ulteriori circostanze, fra cui il carattere non doloso dell'illecita diffusione che, pur protraendosi per oltre un anno, aveva tuttavia riguardato un solo interessato. Inoltre sono state valutate positivamente l'immediata rimozione dei dati dal sito web, la collaborazione offerta dal titolare del trattamento nel corso dell'istruttoria, l'adozione di diverse misure tecniche e organizzative messe in atto ai sensi degli artt. 25-32, del RGPD nonché l'assenza di precedenti violazioni (provv. 7 novembre 2019, n. 209, doc. web n. 9269824).

4.5.2. L'accesso civico

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

Come in passato, il Garante ha invitato l'amministrazione a rivalutare dinieghi a richieste di accesso civico che, pur basati sulla protezione dei dati personali, non erano però adeguatamente motivati (cfr., fra i tanti, parere 13 agosto 2019, n. 160, doc. web n. 9157176).

Persone giuridiche

L'Autorità ha poi ribadito che il limite all'accesso civico derivante dalla protezione dei dati personali non trova applicazione a soggetti diversi dalle persone fisiche. Su tale assunto un'amministrazione è stata invitata a rivalutare il proprio provvedimento di diniego parziale su un'istanza di accesso civico generalizzato volta a ottenere un verbale di violazione amministrativa elevato nei confronti di un circo per l'affissione di cartelli pubblicitari (parere 29 maggio 2019, n. 122, doc. web n. 9128783; sulle persone giuridiche cfr. anche parere 21 febbraio 2019, n. 47, doc. web n. 9103063).

Politici

Fra i casi in cui è stata ritenuta non provata l'esistenza di un pregiudizio concreto alla protezione dei dati personali va annoverato il parere reso su una richiesta di accesso civico avente a oggetto la copia dei provvedimenti adottati nei confronti di alcuni amministratori locali per ottenere il recupero delle somme da restituire in virtù della rideterminazione di indennità di carica nonché dei pagamenti effettuati

ai fini della restituzione delle somme dovute. In questo caso la p.a. è stata invitata a rivalutare il diniego opposto, previo coinvolgimento dei soggetti controinteressati, fornendo una motivazione congrua e completa rispetto all'esistenza o meno del limite di cui all'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013. Ciò tenendo conto, quali elementi favorevoli all'ostensione, della circostanza che alcune informazioni erano già oggetto di pubblicazione obbligatoria; del ruolo, della funzione pubblica e dell'attività di pubblico interesse esercitata dagli amministratori locali cui si riferivano i dati personali oggetto di accesso; del regime di pubblicità e trasparenza rafforzato richiesto per coloro che rivestono incarichi di indirizzo politico in relazione ai compensi percepiti. È stato inoltre evidenziato che, per effettuare la valutazione, è necessario in ogni caso rispettare il principio di minimizzazione, alla luce del quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità di trasparenza propria dell'istituto dell'accesso civico, in modo che non si realizzi un'interferenza ingiustificata e sproporzionata nei diritti e nelle libertà delle persone, tenendo altresì conto dell'eventuale esistenza di contenziosi ancora in corso attivati dai controinteressati in merito alla richiesta di restituzione di parte delle indennità percepite e dell'interferenza che la conoscibilità di questi dati poteva determinare sul diritto di difesa (parere 26 giugno 2019, n. 145, doc. web n. 9126414).

Commissioni di concorso

Analogamente, anche se in relazione a una fattispecie diversa, a fronte del diniego di una richiesta di accesso civico avente a oggetto diversi documenti di un'agenzia regionale, inerenti alla determinazione di indizione e al bando di concorso per le progressioni economiche orizzontali del personale nonché all'atto di nomina della commissione esaminatrice delle candidature, non si è ravvisato con riferimento all'atto di nomina della commissione, il rischio del pregiudizio concreto alla tutela dei dati personali; mentre nel caso del bando, trattandosi di documento non contenente dati personali, non poteva in alcun caso essere richiamato il limite all'accesso civico di cui all'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 28 febbraio 2019, n. 48, doc. web n. 9103079).

Contratti di docenza

In relazione, inoltre, a una istanza di riesame proposta a seguito di un diniego su una istanza di accesso civico generalizzato volta conoscere gli anni accademici in cui un soggetto aveva tenuto alcune docenze presso un'università, è stato rappresentato che dalla motivazione fornita dall'amministrazione non si desumeva il motivo per cui l'ostensione dell'informazione richiesta potesse recare un pregiudizio concreto alla protezione dei dati personali del controinteressato. Ciò considerando che l'informazione relativa alla docenza (compresa la materia oggetto di insegnamento) era già liberamente accessibile nelle note bibliografiche riferite al soggetto controinteressato presenti su diversi siti di informazione *online* (parere 14 novembre 2019, n. 205, doc. web n. 9207868).

Numerosi i casi in cui è stato confermato il diniego totale o parziale di richieste di accesso civico alla luce dei limiti derivanti dalla normativa in materia di protezione dei dati personali; anche rispetto ad essi si darà di seguito conto solo dei casi più significativi, dividendoli per aree tematiche.

Persone adottate o in affidamento educativo

Per l'estrema delicatezza della questione, merita ricordare il parere reso in relazione a una istanza di accesso civico volta a ottenere dati e informazioni personali di bambini di nazionalità estera giunti in Italia con un convoglio umanitario e dati in affido educativo in specifici centri per essere successivamente adottati. Al riguardo, è stato evidenziato che la normativa di settore prevede un divieto di comunicazione di informazioni relative ai bambini adottati, laddove sancisce che l'ufficiale di stato civile e l'ufficiale di anagrafe nonché "qualsiasi altro ente pubblico o privato, autorità o pubblico ufficio" devono "rifiutarsi di fornire notizie, informazioni, cer-

4

tificazioni, estratti o copie dai quali possa comunque risultare il rapporto di adozione, salvo autorizzazione espressa dell'Autorità giudiziaria" (art. 28, comma 3, l. n. 184/1983). Pertanto, tale fattispecie rientrava in una delle ipotesi di cui all'art. 5-*bis*, comma 3, d.lgs. n. 33/2013, che prevede l'esclusione dell'accesso nei "casi di divieti di accesso o divulgazione previsti dalla legge". In relazione invece alle altre informazioni riguardanti bambini interessati dalla vicenda ma non afferenti all'adozione, è stato osservato che in ogni caso si trattava di dati personali delicati, riferiti a soggetti vulnerabili, la cui ostensione, anche parziale, poteva arrecare agli stessi – seppure oggi maggiorenni – ripercussioni negative sul piano sociale, relazionale e professionale, in considerazione del particolare regime di pubblicità dei dati oggetto di accesso civico nonché delle ragionevoli aspettative di confidenzialità dei soggetti interessati (parere 7 febbraio 2019, n. 26, doc. web n. 9100178).

Atti di una commissione etica di un ateneo

Analogamente, per la particolarità della fattispecie, si segnala l'intervento del Garante su due richieste di accesso civico riguardanti la documentazione della commissione etica di un ateneo, relativa a una procedura volta a verificare il rispetto del codice etico da parte di un soggetto. Richiamando i precedenti pareri in materia di sanzioni disciplinari (v. provv.ti 21 novembre 2018, n. 483; 7 dicembre 2017, n. 515; 31 maggio 2017, n. 254), è stato affermato che la generale conoscenza delle informazioni richieste violava il dovere di riservatezza della commissione e determinava un'interferenza sproporzionata nei diritti e nelle libertà dei controinteressati. Ciò tenendo in considerazione le ragionevoli aspettative di confidenzialità dell'interessato (che si era peraltro rivolto spontaneamente alla commissione) e degli altri soggetti coinvolti nella vicenda, i quali potevano fare ragionevolmente affidamento sul carattere riservato del procedimento. Nel caso di specie, il principio di trasparenza è apparso soddisfatto dalla conoscenza dell'esito del procedimento, avviato e concluso, che l'università aveva provveduto ad assicurare. L'ulteriore documentazione di cui si richiedeva l'ostensione, invece, contenendo dati e informazioni personali delicate, poteva effettivamente arrecare un pregiudizio concreto alla tutela della protezione dei dati personali, anche in ragione del particolare regime di pubblicità dei dati oggetto di accesso civico. La probabilità di tale pregiudizio, inoltre, era amplificata dalla notorietà a livello locale che la vicenda aveva assunto su una testata giornalistica *online* e dalla circostanza di poter causare danni legati alla sfera morale, relazionale, professionale e sociale dell'interessato e delle altre persone coinvolte sia all'interno che all'esterno della comunità scientifica di appartenenza. Tali considerazioni impedivano altresì di accordare un accesso civico parziale, oscurando i nominativi dei controinteressati, in quanto questi ultimi risultavano comunque indirettamente identificabili, anche all'interno del luogo di lavoro, attraverso gli ulteriori dati di contesto o le informazioni di dettaglio contenute nei documenti richiesti (pareri 10 ottobre 2019, n. 184, doc. web n. 9195259 e 31 ottobre 2019, n. 196, doc. web n. 9195266).

Denunce all'Autorità giudiziaria

Altra fattispecie di interesse riguarda l'accesso civico alle denunce presentate da un comune, nel caso di specie anche contro ignoti, all'Autorità giudiziaria (o ad un'altra autorità competente), negli anni 2017-2019, per reati ambientali avvenuti nel territorio dell'ente. L'amministrazione aveva negato l'ostensione, rappresentando che gli atti richiesti erano stati trasmessi al Comando dei Carabinieri per la tutela dell'ambiente con riferimento a un'indagine della Procura della Repubblica. Pertanto le informazioni richieste potevano essere coperte da segreto istruttorio. Il soggetto istante è stato quindi invitato a rivolgere al tribunale eventuali richieste di accesso nei termini e modi previsti dalla legge. Il Garante, pur non entrando nel merito del diniego opposto, ha evidenziato che, in ogni caso, i documenti di cui si chiedeva l'accesso civico potevano contenere dati e informazioni personali di tutti

coloro che erano stati destinatari delle predette denunce (tranne per le denunce contro ignoti). Si poteva trattare quindi di documenti – contenenti dati e informazioni delicate – riferiti a soggetti nei cui confronti poteva essere aperto un procedimento penale e la cui generale conoscenza poteva, di conseguenza, causare un pregiudizio alla tutela dai dati personali, quali danni legati alla sfera morale, relazionale, professionale e sociale, gettando discredito sui controinteressati anche nel caso di denunce poi archiviate. Il Garante ha invece ritenuto non sussistere alcuna ragione attinente alla protezione dei dati personali in relazione all'eventuale ostensione di dati aggregati (privi di dati identificativi e di ogni ulteriore informazione idonea a identificare i controinteressati anche indirettamente), quali ad esempio il numero delle denunce effettuare negli ultimi tre anni e la relativa data (parere 10 ottobre 2019, n. 187, doc. web n. 9198109).

Soggetti deceduti

Tra i pareri più significativi c'è, inoltre, quello in materia di accesso civico presentato a un'azienda sanitaria avente ad oggetto dati relativi alla salute (quadro clinico, dettagli su ricovero, degenza, sintomi, anamnesi, diagnosi, esami effettuati, terapia, farmaci somministrati, consulenze mediche effettuate, ecc.) di un paziente, poi deceduto. In particolare, è stato affermato che il riconoscimento della possibilità di esercitare i diritti in materia di protezione dei dati personali (artt. 15-22, del RGPD) da parte dei soggetti elencati nell'art. 2-*terdecies*, comma 1, del Codice, comporta – quale naturale conseguenza e necessario presupposto logico-giuridico – che ai dati personali concernenti le persone decedute continuino ad applicarsi le tutele previste dalla disciplina in materia di protezione dei dati personali. Per tale motivo, considerando che l'art. 2-*septies*, comma 8, del Codice prevede un divieto di diffusione di dati idonei a rivelare lo stato di salute, è stato confermato il diniego dell'azienda all'accesso civico generalizzato ai predetti dati personali ancorché riferiti a un paziente poi deceduto, in forza del richiamo operato dall'art. 5-*bis*, comma 3, d.lgs. n. 33/2013, secondo il quale l'accesso va escluso, fra l'altro, nei casi di divieto di divulgazione espressamente previsti da normative di settore (parere 10 gennaio 2019, n. 2, doc. web n. 9084520; in materia di dati sulla salute, cfr. anche parere 7 febbraio 2019, n. 27, doc. web n. 9090308, in cui è evidenziata la diversa tipologia di valutazione che l'amministrazione deve invece effettuare quando l'accesso è richiesto ai sensi della diversa legge n. 241/1990).

Rapporto di lavoro

Cambiando materia, molto frequenti sono state le richieste di parere in ordine all'accesso civico a dati e informazioni personali riferite a dipendenti, lavoratori e soggetti che hanno avuto contratti o rapporti con la p.a. Al riguardo, è stata più volte affermata la sussistenza di un pregiudizio concreto alla protezione dei dati personali, in considerazione della tipologia e della natura dei dati e delle informazioni personali oggetto dell'istanza, del particolare regime di pubblicità che connota l'accesso civico nonché delle ragionevoli aspettative di confidenzialità dei soggetti controinteressati sui quali si potevano realizzare ripercussioni negative sul piano sociale, relazionale o professionale. È stata altresì evidenziata la necessità di rispettare il principio di minimizzazione dei dati, in base al quale i dati devono essere, fra l'altro, "limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. *c*), del RGPD) e l'impossibilità di accordare un accesso parziale, oscurando i nominativi dei controinteressati, in quanto questi sarebbero risultati indirettamente identificabili, anche all'interno del luogo di lavoro, attraverso gli ulteriori dati di contesto o informazioni di dettaglio contenute nei documenti richiesti. In molti casi, l'amministrazione è stata invitata a fornire, comunque, dati aggregati (privi di dati e informazioni tali da identificare i soggetti interessati anche indirettamente), al fine di dare soddisfazione all'interesse conoscitivo del soggetto istante. In generale, è stato più volte rappresentato che in presenza di un interesse specifico del

4

soggetto istante, laddove i documenti non possano essere forniti mediante l'istituto dell'accesso civico generalizzato, resta in ogni caso salva la possibilità di accedere alla documentazione richiesta ai sensi della disciplina in materia di accesso agli atti amministrativi contenuta negli artt. 22 ss., l. n. 241/1990 dimostrando l'esistenza di "un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso".

Dati di dipendenti e altre ipotesi

Il Garante ha condiviso il diniego opposto da un comune all'accesso civico avente a oggetto una comunicazione fornita all'ente da un proprio dipendente contenente dati personali allo stesso riferiti nonché ulteriori informazioni relative anche alla capacità professionale, alle prospettive di carriera e a iniziative svolte all'esterno dell'amministrazione di appartenenza (parere 7 febbraio 2019, n. 29, doc. web n. 9086520). Analogamente è stato ritenuto sussistente un pregiudizio alla protezione dei dati personali dei controinteressati, in ragione del quale l'amministrazione ha correttamente rifiutato l'accesso civico generalizzato, in relazione a istanze aventi ad oggetto, fra l'altro:

- il nulla osta e il parere tecnico relativo alla mobilità di un dipendente (parere 19 marzo 2019, n. 63, doc. web n. 9114118);
- i fogli presenza dei dipendenti, i giorni e le ore di lavoro oppure le mansioni svolte (pareri 14 marzo 2019, n. 60, doc. web n. 9102014; 10 ottobre 2019, n. 185, doc. web n. 9198091);
- le date di assunzione e cessazione dell'incarico di un dipendente ministeriale (parere 10 ottobre 2019, n. 186, doc. web n. 9198098);
- l'ostensione di tutte le contestazioni disciplinari e dei provvedimenti a esse conseguenti emesse, nei cinque anni anteriori alla richiesta, da un'azienda partecipata da un comune (parere 16 agosto 2019, n. 161, doc. web n. 9161714);
- l'elenco nominativo (o il numero di matricola con ruolo professionale) dei dirigenti di un'azienda presi a riferimento per la costituzione di quattro fondi di risultato delle distinte aree, il numero di ore di plus orario assegnate individualmente nonché il valore economico di ciascuna ora (parere 12 settembre 2019, n. 164, doc. web n. 9157101);
- i documenti di carattere prodromico e funzionale all'approvazione di graduatoria per la progressione economica orizzontale del personale amministrativo dipendente di un'agenzia regionale (parere 28 febbraio 2019, n. 48, doc. web n. 9103079);
- i documenti inerenti alla liquidazione della produttività strategica di un ex dipendente e alla liquidazione di incarichi a professionisti risalenti nel tempo, come indicato nei pareri 7 marzo 2019, n. 54 (doc. web n. 9102429) e 7 febbraio 2019, n. 28 (doc. web n. 9086500); nel secondo caso il pregiudizio era aggravato dall'esistenza di vicende giudiziarie intercorrenti fra il soggetto istante e il soggetto controinteressato;
- i dati "relativi alla spendita delle procure e alla partecipazione alle udienze nei tre gradi di giudizio, per il 2017 e 2018" di tutti gli avvocati che hanno ricevuto la procura alle liti dell'Inps, anche considerando che le informazioni richieste potevano far conoscere la distribuzione dei carichi di lavoro fra i singoli legali, con conseguente possibilità di individuare il trattamento economico dagli stessi percepito nonché, in alcuni casi, anche le situazioni personali rappresentate, ad esempio, da periodi di assenza dal servizio per malattia (parere 19 marzo 2019, n. 62, doc. web n. 9115506);
- i documenti inerenti alla partecipazione a una procedura di gara per l'affidamento di un contratto pubblico contenente dati, informazioni e documenti di diversa specie, riferiti a più di 1.700 persone, riguardanti, in particolare, la

lista del personale utilizzato nei vari servizi, il *curriculum vitae* del personale, la documentazione comprovante il possesso dei titoli, competenze ed esperienze previste per le varie figure professionali, la documentazione richiesta per il personale addetto a specifici servizi (parere 23 maggio 2019, n. 115, doc. web n. 9124946);

- gli atti relativi a un concorso di dottorato di ricerca, quali copia degli elaborati delle prove scritte, dei verbali di correzione degli elaborati e dei *curricula vitae* dei candidati (parere 7 novembre 2019, n. 200, doc. web n. 9196072).

Si menzionano, infine, i numerosi pareri resi su istanze di accesso civico aventi ad oggetto interventi urbanistici, titoli e abusi edilizi, nonché concessioni demaniali. Nel corso del 2019 il Garante è in più occasioni tornato a occuparsi del tema dell'accesso civico generalizzato alla documentazione inerente a Segnalazioni certificate di inizio attività (Scia) e a Certificazioni di inizio attività asseverata (Cila), evidenziando che i casi in cui è necessario presentare l'una o l'altra interessano un insieme molto variegato di interventi edilizi, spaziando dalla semplice apertura o chiusura di un vano finestra, alla costruzione di una recinzione, al frazionamento o accorpamento di unità abitative, fino a operazioni più importanti come il rifacimento di tetti o solai, oppure la ristrutturazione generale di un intero fabbricato. Pertanto, le informazioni e i dati, anche di carattere personale, da presentare all'ente competente, e contenuti nei predetti titoli abilitativi edilizi (Cila e Scia), sono molteplici e di diverso genere e natura, quali, ad esempio, nominativi, data e luogo di nascita, codici fiscali, residenza, *e-mail*, Pec, numeri di telefono fisso e cellulare riferiti al/i titolare/i dell'intervento in qualità di proprietario, comproprietario, usufruttuario, amministratore di condominio o dei loro rappresentanti; informazioni sulla tipologia di intervento; data di inizio e fine dello stesso; ubicazione, dati catastali e destinazione d'uso dell'immobile oggetto dell'intervento edilizio; carattere oneroso o gratuito dell'intervento, eventuale ricevuta dei versamenti effettuati; entità presunta del cantiere; dati dei tecnici incaricati (direttori dei lavori e altri tecnici) e dell'impresa esecutrice dei lavori; prospetto di calcolo preventivo del contributo di costruzione e elaborati grafici dello stato di fatto e progetto.

Scia e Cila

In merito, è stato ribadito che non esiste un obbligo di pubblicazione da parte delle pp.aa. delle Scia o delle Cila presentate all'ente (né in forma integrale, né in forma riassuntiva) e che per i dati personali ivi contenuti il legislatore non ha previsto alcun regime di pubblicità. Ciò in quanto la disposizione contenuta nell'art. 20, comma 6, d.P.R. n. 380/2001 (Testo unico in materia edilizia) è una norma di settore attinente al solo "procedimento per il rilascio del permesso di costruire", che costituisce un titolo edilizio diverso dalla Cila e dalla Scia. Inoltre, la predetta disposizione, che non è ripetuta (né richiamata) per i procedimenti relativi agli altri titoli edilizi (Cila o Scia), non prevede neanche la pubblicazione del provvedimento sull'albo pretorio nella sua integrità, ma della mera "notizia" dell'"avvenuto rilascio del permesso di costruire" (i cui estremi sono peraltro "indicati nel cartello esposto presso il cantiere, secondo le modalità stabilite dal regolamento edilizio"). Alla Cila e alla Scia – disciplinate nel medesimo d.P.R. n. 380/2001 – non è di conseguenza in nessun modo applicabile il limitato regime di pubblicità previsto per la "notizia" dell'avvenuto rilascio del permesso di costruire.

Con riferimento ai casi esaminati, è stato nuovamente affermato che non è possibile accordare una generale prevalenza della trasparenza o del diritto di accesso civico generalizzato a scapito di altri diritti ugualmente riconosciuti dall'ordinamento, in quanto si vanificherebbe il necessario bilanciamento degli interessi che richiede un approccio equilibrato nella ponderazione dei diversi diritti coinvolti. In tale quadro, rispetto all'esistenza del limite dalla tutela dei dati personali a fronte del

4

quale dover rifiutare un accesso civico generalizzato, è stato ricordato che devono essere tenuti in considerazione: la circostanza che i dati e le informazioni fornite all'esito dell'accesso civico generalizzato sono pubblici e tendenzialmente riutilizzabili; il rispetto del principio di minimizzazione dei dati personali; le ragionevoli aspettative di confidenzialità dei controinteressati in relazione al trattamento dei propri dati personali al momento in cui questi sono stati raccolti; la non prevedibilità delle conseguenze derivanti dall'eventuale conoscibilità da parte di chiunque dei dati richiesti. Ciò anche in ragione del fatto che, nel caso esaminato, il richiedente era un'impresa che svolgeva attività di gestione di *database* e di *marketing* e che risultava aver effettuato, con carattere sistematico, analoghe richieste a tutte le Scia e alle Cila di diversi enti locali. Tale circostanza poteva causare un pericolo di duplicazione di banche dati di soggetti pubblici da parte di soggetti privati in assenza del consenso degli interessati o degli altri presupposti di liceità del trattamento previsti dall'art. 6, par. 1, del RGPD, nonché il possibile rischio di "usi impropri" e/o di "riutilizzo" e trattamento ulteriore dei dati personali per finalità non compatibili con quelle per le quali i dati personali erano stati inizialmente raccolti e in contrasto con quanto previsto dall'art. 6, par. 4, del RGPD. Il Garante ha quindi condiviso la scelta dell'amministrazione di respingere l'istanza di accesso civico in quanto l'ostensione dei dati richiesti poteva effettivamente arrecare ai controinteressati quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013. Come già osservato in passato, è stato ribadito che le informazioni di dettaglio contenute nelle Scia e nelle Cila impediscono di poter accordare un eventuale accesso civico ai sensi dell'art. 5-*bis*, comma 4, d.lgs. n. 33/2013, anche oscurando, ad esempio, i dati identificativi (nome e cognome) del committente o del tecnico progettista. Tale accorgimento, infatti, non elimina la possibilità che i soggetti interessati siano identificati indirettamente tramite gli ulteriori dati di contesto contenuti nella documentazione richiesta. È apparso invece conforme alla normativa in materia di protezione dei dati personali la soluzione adottata dall'amministrazione comunale che – allo scopo di soddisfare comunque le esigenze informative alla base dell'accesso civico e di "favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico" (art. 5, comma 2, d.lgs. n. 33/2013) – ha fornito i dati relativi alle Scia e Cila, senza comunicare dati personali, e precisamente: la tipologia di titolo edilizio (Scia o Cila), una descrizione dell'intervento (es: manutenzione straordinaria, installazione insegna; intervento miglioramento sismico, nuovo accesso carraio, variante in corso d'opera per ristrutturazione edilizia; opere interne; variante in corso d'opera, ecc.), le informazioni relative all'effettuazione dell'intervento nel comune o in una sua frazione (parere 3 gennaio 2019, n. 1, doc. web n. 9080951; cfr. anche parere 12 settembre 2019, n. 162, doc. web n. 9157164; parere 24 gennaio 2019, n. 12, doc. web n. 9084347).

Abusi edilizi

Sempre in tema di edilizia, il Garante è stato chiamato a intervenire in relazione a una richiesta di accesso civico generalizzato ai verbali di abusi edilizi e ai relativi provvedimenti adottati negli anni 2018 e 2019; anche in tale fattispecie è stato condiviso il diniego opposto da un comune, in quanto l'ostensione dei dati personali contenuti nella documentazione, unita al particolare regime di pubblicità dei dati oggetto della richiesta, poteva causare, a seconda delle ipotesi e del contesto in cui i dati e le informazioni possono essere utilizzate, un pregiudizio concreto alla tutela della protezione dei dati personali. Non sussistevano invece ragioni attinenti alla protezione dei dati personali in relazione all'ostensione di dati aggregati, quali ad esempio il numero degli abusi edilizi rilevati negli ultimi due anni e le aree/zone

comunali interessate prive di indirizzi e numeri civici (parere 18 dicembre 2019, n. 220, doc. web n. 9232553).

Merita segnalare infine il parere in materia di concessioni demaniali nel quale il Garante ha ritenuto corretto il diniego di un'istanza di accesso civico generalizzato tesa a ottenere copia degli atti delle concessioni demaniali marittime di stabilimenti e chioschi, comprese le relative planimetrie dagli anni 2000, nonché tutte le concessioni per atto formale complete di allegati, rilasciate da un comune. Ciò in quanto l'accesso civico generalizzato ai dati personali contenuti nella documentazione richiesta, unito alla generale conoscenza e al particolare regime di pubblicità dei dati oggetto di accesso civico, poteva costituire un'interferenza sproporzionata nei diritti e libertà dei controinteressati, arrecando a questi ultimi, a seconda delle ipotesi e del contesto di utilizzazione delle informazioni fornite da parte di terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 2 ottobre 2019, n. 179, doc. web n. 9162546).

4.5.3. L'accesso ai documenti amministrativi

Quanto al diverso accesso ai documenti amministrativi ai sensi degli artt. 22 ss., l. n. 241/1990, continuano a pervenire al Garante richieste di parere da parte di amministrazioni o di singoli cittadini rispetto alle quali, come in passato, è stato evidenziato che le norme in materia di accesso ai documenti amministrativi non sono state modificate dal nuovo quadro normativo in materia di protezione dei dati personali (artt. 22 ss., l. n. 241/1990; d.P.R. 12 aprile 2006, n. 184; artt. 6, 9, 10 e 86 del RGPD; artt. 59 e 60 del Codice). In particolare, l'art. 86 del RGPD prevede che "i dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico […] per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità […] conformemente al diritto dell'Unione o degli Stati membri [...] al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione di dati personali". Inoltre, l'art. 59, comma 1, del Codice precisa che "fatto salvo quanto previsto dall'art. 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241 […] anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del Regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso".

È stato pertanto ribadito che spetta all'amministrazione, e non al Garante, nel caso di richieste di accesso ai documenti presentate ai sensi della legge n. 241/1990, accertare l'esistenza nel caso concreto dell'interesse qualificato, alla luce dei motivi sottesi alla richiesta, nonché verificare la sussistenza di una delle ragioni per le quali il documento richiesto può essere sottratto alla conoscibilità del richiedente, anche in base alle tipologie di documenti non accessibili individuati nell'apposito regolamento della singola amministrazione. È stato inoltre precisato che le valutazioni in ordine alle determinazioni adottate dalle amministrazioni sulle specifiche richieste di accesso esulano dall'ambito di competenza del Garante e rimangono sindacabili di fronte alle autorità competenti (art. 25, l. n. 241/1990).

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

Interpellato da numerosi comuni, società a partecipazione pubblica e aziende municipalizzate, il Garante è intervenuto dando chiarimenti in relazione ai trat-

tamenti di dati necessari allo svolgimento delle attività istituzionali, inclusa la comunicazione di dati personali ai sensi dell'art. 2-*ter*, comma 2, del Codice. In proposito, è stato ribadito che l'ipotesi individuata nel citato art. 2-*ter* prevede la comunicazione di dati personali tra autonomi titolari, anche in mancanza di una norma, quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e per lo svolgimento di funzioni istituzionali dell'ente richiedente. L'ipotesi contemplata dalla disposizione, tuttavia, è residuale e ha carattere eccezionale, e non può essere invocata per legittimare una comunicazione regolare e sistematica di dati personali o per superare specifici limiti o presupposti individuati dalle norme.

App

Nell'ambito di verifiche compiute in relazione all'uso delle *app* nel settore pubblico, il Garante ha adottato nei confronti di Roma Capitale il provvedimento 7 marzo 2019, n. 81 (doc. web n. 9121890) in relazione ai trattamenti di dati personali dei dipendenti e degli utenti posti in essere mediante il sistema denominato "TuPassi" per la gestione delle prenotazioni dei servizi erogati al pubblico e delle code allo sportello (cfr. par. 13.8). Il sistema utilizzato dall'Ente costituisce uno strumento per perseguire il miglioramento dell'efficienza ed economicità dell'attività amministrativa attraverso la gestione delle prenotazioni degli appuntamenti dei servizi erogati allo sportello e delle attese; di conseguenza, i trattamenti di dati personali effettuati possono essere considerati necessari per l'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. *e*), del RGPD) contemplato dall'ordinamento (art. 97 Cost.; art. 1, l. n. 241/1990; artt. 1, 10 e 11, d.lgs. n. 165/2001). Tuttavia, dalle risultanze istruttorie è emerso che il titolare del trattamento effettuava, mediante detto sistema, operazioni di trattamento di dati personali degli utenti e dei dipendenti non conformi alla disciplina in materia di protezione dei dati personali, con particolare riferimento all'obbligo di conferire adeguata informativa agli utenti e dipendenti ai sensi degli artt. 13 e 14 del RGPD, alla mancata designazione della società fornitrice del sistema quale responsabile del trattamento e all'adozione di misure tecniche e organizzative adeguate agli specifici rischi connessi al trattamento. Per tali ragioni, è stato ingiunto al titolare di conformare il trattamento alle disposizioni menzionate del RGPD e del Codice e di adottare adeguate azioni correttive volte ad eliminare le criticità tecniche e organizzative; inoltre è stato avviato un procedimento per l'adozione di provvedimenti correttivi/sanzionatori.

4.7. *La materia anagrafica ed elettorale*

Propaganda elettorale

In vista delle numerose consultazioni elettorali, anche europee (svoltesi nel 2019), alla luce del quadro normativo introdotto dal RGPD e dal Codice, il Garante ha adottato un nuovo provvedimento in materia di propaganda elettorale e comunicazione politica (provv. 18 aprile 2019, n. 96, doc. web n. 9105201, in relazione al quale v. anche, per profili ulteriori, parr. 11.3 e 14.5.3). Al riguardo occorre premettere che il legislatore europeo, in considerazione dei potenziali rischi che l'uso illecito dei dati personali può comportare per i processi elettorali e la democrazia, ha previsto "sanzioni pecuniarie nei casi in cui i partiti politici europei o le fondazioni politiche europee sfruttino le violazioni delle norme in materia di protezione dei dati al fine di influenzare l'esito delle elezioni del Parlamento europeo" (modifiche al Regolamento UE, Euratom n. 1141/2014, relativo allo statuto e al finanziamento dei partiti politici europei e delle fondazioni politiche europee, modificato dal regolamento UE, Euratom 2019/493; Dichiarazione 2/2019 del Cepd sull'uso di dati personali nel corso di campagne politiche, adottata il 13 marzo 2019).

In tale contesto, per quanto riguarda l'utilizzo per finalità di propaganda eletto-

rale di dati personali provenienti da fonti pubbliche, il provvedimento in parola ha confermato l'utilizzabilità, per finalità di propaganda elettorale, dei dati personali estratti dalle liste elettorali detenute presso i comuni nonché di altre liste ed elenchi previste dalle norme che disciplinano le diverse consultazioni elettorali e il voto degli italiani all'estero. È stato ribadito che non possono essere trattati, per tali finalità, i dati raccolti o utilizzati dai soggetti pubblici per lo svolgimento delle proprie attività istituzionali, gli elenchi di iscritti ad albi e collegi professionali, i dati resi pubblici alla luce della disciplina in materia di trasparenza o pubblicità dell'azione amministrativa (d.lgs. 14 marzo 2013, n. 33; l. 18 giugno 2009, n. 69). Ulteriori precisazioni hanno riguardato, inoltre, l'inutilizzabilità dei dati raccolti da titolari di cariche elettive e di altre funzioni pubbliche in base a specifiche disposizioni che prevedono il diritto di ottenere dagli uffici di riferimento informazioni utili all'esercizio del mandato ed alla loro partecipazione alla vita politico-amministrativa dell'ente (es. consiglieri comunali e provinciali).

Liste elettorali

Alla luce dell'abrogazione dell'art. 177 del Codice da parte del d.lgs. n. 101/2018, sono pervenuti numerosi quesiti da parte di comuni in merito ai presupposti previsti per il rilascio delle liste elettorali a diversi soggetti di natura privata (associazioni, società, ecc.), considerato che l'art. 177 del Codice, a suo tempo, aveva modificato l'art. 51, d.P.R. n. 223/1967.

L'Ufficio, dopo aver ribadito che il trattamento dei dati personali da parte dei soggetti pubblici è ammesso se la base giuridica "è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento" (art. 6, par. 1, lett. *e*), par. 2 e 3, lett. *b*), del RGPD e art. 2-*ter*, del Codice), ha confermato che, in base alla normativa di settore, le liste elettorali possono essere rilasciate in copia "per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso" (cfr. art. 51, comma 5, d.P.R. n. 223/1967, come modificato, a suo tempo, dall'art. 177 del Codice). Tali finalità, in base all'orientamento del Ministero dell'interno, devono risultare, oltre che motivate ai sensi dell'art. 51, proprie del richiedente e, "ove si tratti di un ente o di un'associazione, devono essere coerenti con l'oggetto dell'attività di tale organismo". A seguito delle modifiche apportate al Codice dal d.lgs. n. 101/2018, è stato precisato inoltre che queste non hanno inciso sull'applicazione dell'art. 51, comma 5, d.P.R. n. 223/1967, ai sensi del quale – anche a seguito dell'abrogazione dell'art. 177 del Codice – le liste elettorali possono essere rilasciate solo per le finalità sopra richiamate; al riguardo anche il Ministero dell'interno si è espresso nei medesimi termini.

Cie

In relazione al decreto del Ministero dell'interno 31 gennaio 2019 che ha apportato modifiche alle modalità tecniche di emissione della carta di identità elettronica (Cie) in favore di soggetti minorenni, sono state segnalate al Garante le criticità derivanti agli interessati dall'attuazione delle predette modifiche. Come è noto, il decreto ha introdotto nel formato della Cie e nella modulistica e procedura per il rilascio del documento, la specificazione di genere "padre" e "madre", in luogo del più generico riferimento ai "genitori". Il Garante aveva espresso forti perplessità sull'impatto di tali modifiche in termini di protezione dei dati personali degli interessati nel proprio parere sullo schema di decreto (provv. 31 ottobre 2018, n. 476, doc. web n. 9058965).

Le segnalazioni hanno lamentato criticità – già evidenziate dal Garante – nei casi nei quali i soggetti esercitanti la responsabilità genitoriale non siano esattamente riconducibili alla figura materna e/o paterna, perché, ad es., dello stesso sesso. In questi casi il minore non potrebbe ottenere la Cie, a meno che i soggetti esercitanti

4

la responsabilità genitoriale non rendano una dichiarazione non coincidente con la propria identità di genere. L'esclusiva indicazione delle figure genitoriali come "padre" e "madre", anche nell'ipotesi in cui essi abbiano – come consentito dall'ordinamento – identità di genere diverse da quelle indicate nel documento e nei moduli di richiesta, urta con i principi in materia di protezione dei dati personali e, in particolare, con il principio di esattezza dei dati trattatati (art. 5 del RGPD).

In relazione a tali segnalazioni, nel ribadire le perplessità a suo tempo manifestate sul testo del decreto, il Presidente dell'Autorità ha inviato una lettera al Ministro dell'interno invitandolo a valutare la possibilità di superare le criticità sopra evidenziate (nota 19 settembre 2019).

4.8. *I trasferimenti di dati personali verso autorità pubbliche o organizzazioni internazionali*

Consob

L'Autorità è stata investita della richiesta di autorizzare un trasferimento di dati personali all'estero sulla base di un accordo amministrativo tra autorità pubbliche, ai sensi degli artt. 46, par. 3, lett. *b*), e 58, par. 3, lett. *i*), del RGPD, in applicazione del meccanismo di coerenza di cui all'art. 63. In mancanza di una decisione di adeguatezza della Commissione europea, infatti, il RGPD prevede che anche gli accordi amministrativi tra autorità o organismi pubblici possano costituire garanzie adeguate al trasferimento dei dati, purché comprendano diritti effettivi e tutelabili e ricevano l'autorizzazione dell'autorità garante nazionale.

Nel caso di specie, la richiesta è pervenuta dalla Commissione nazionale per le società e la borsa (Consob), con riferimento a un progetto di accordo amministrativo per il trasferimento di dati personali tra le autorità di vigilanza finanziaria dello Spazio economico europeo (See) e le autorità di vigilanza finanziaria al di fuori del See, a fini di vigilanza e di *enforcement* ai sensi dell'art. 4, d.lgs. 24 febbraio 1998, n. 58. Tale progetto di accordo è stato definito dall'Autorità europea degli strumenti finanziari e dei mercati (Esma) e dall'Organizzazione internazionale delle commissioni sui valori mobiliari (Iosco), su cui, a sua volta, il Cepd ha reso il parere 4/2019, del 12 febbraio 2019, ai sensi dell'art. 64, par. 2, del RGPD (v. parr. 17 e 21.1). Obiettivo dell'accordo è il trasferimento di informazioni nell'ambito dell'attività di cooperazione internazionale, finalizzata ad assicurare l'assistenza reciproca per la repressione di comportamenti illeciti sui mercati e per il rispetto da parte degli operatori degli obblighi di trasparenza nei confronti del mercato e degli investitori.

Il Garante ha valutato favorevolmente le clausole di garanzia contenute nell'accordo, tra cui rilevano, in particolare, il rispetto dei principi di trasparenza, proporzionalità, qualità dei dati, meccanismi di tutela per gli interessati e adeguate misure di sicurezza, stabilendo altresì l'obbligo, per l'autorità ricevente, di informare senza ritardo l'autorità trasferente della presenza di una violazione di dati personali (*data breach*). È inoltre previsto che i trasferimenti riguardino dati personali esatti e aggiornati, nonché adeguati, pertinenti e limitati a quanto necessario per le finalità per le quali sono trasferiti e successivamente trattati, e avvengano solo nel quadro di responsabilità e mandati normativi specifici, per l'esecuzione dei compiti istituzionali delle autorità, evitando il successivo trattamento dei dati in modo incompatibile con tali finalità. Specifiche cautele riguardano i trasferimenti successivi di dati verso un soggetto che non sia un'autorità partecipante all'accordo o un Paese privo della decisione di adeguatezza della Commissione UE. È stata altresì prevista la presenza di un meccanismo di vigilanza esterno.

Su tali basi il Garante, in linea con il parere espresso dal Cepd, ha autorizzato la

Consob a sottoscrivere il predetto progetto di accordo amministrativo, a condizione che venga svolta un'adeguata attività di vigilanza sulla conformità all'accordo e che la Consob informi il Garante in relazione a qualsiasi sospensione dei trasferimenti di dati personali, nonché revisione o sospensione della partecipazione all'accordo. La Consob, inoltre, dovrà conservare la documentazione relativa all'applicazione dell'accordo (ad es., numero delle richieste e lamentate violazioni presentate dagli interessati a livello europeo) e, per i primi due anni di applicazione, dovrà trasmettere al Garante una relazione annuale elaborata sulla base della predetta documentazione; per gli anni successivi la medesima documentazione dovrà essere messa a disposizione dell'Autorità su richiesta. Il Garante sorveglierà sull'applicazione dell'accordo, verificando il rispetto delle garanzie, la cui violazione comporterebbe la sospensione dei flussi di dati effettuati dalla Consob (provv. 23 maggio 2019, n. 119, doc. web n. 9119857).

Unicef

Il Ministero dell'interno ha interpellato il Garante in relazione a un progetto avviato con l'Unicef in relazione al rafforzamento del sistema d'accoglienza e protezione per minori stranieri non accompagnati (Msna) che prevede la promozione di percorsi di affidamento, come misura alternativa di accoglienza e di inclusione sociale, e il coordinamento delle istituzioni responsabili della presa in carico dei minori stranieri non accompagnati. Lo schema di convenzione predisposto dal Ministero per la gestione del progetto contiene puntuali richiami al rispetto del RGPD e del Codice. Considerato che l'Unicef non può essere destinataria di obblighi derivanti da normative emanate da Stati sovrani o dall'Unione europea – come il RGPD e il Codice – in considerazione delle immunità e privilegi riconosciuti alle organizzazioni internazionali, il Ministero dell'interno ha chiesto al Garante se la normativa in materia di protezione dei dati personali trovi applicazione alla stessa.

L'Ufficio ha evidenziato che il Ministero deve verificare che il trattamento sia effettuato nel rispetto dei principi applicabili (artt. 5, 6, 9 e 10 del RGPD e 2-*ter*, 2-*sexies*, 2-*septies*, 2-*octies* del Codice) e individuare in base a quali presupposti, previsti dagli artt. 44-50 del RGPD, viene effettuato il flusso dei dati personali verso l'organizzazione internazionale. In tale ambito, è stato ricordato che in base all'orientamento espresso dal Cepd (linee guida 2/2018 sulle deroghe di cui all'articolo 49 del RGPD, adottate il 25 maggio 2018), i titolari che intendono effettuare un trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali, devono esplorare preventivamente la possibilità di utilizzare per il trasferimento uno dei meccanismi di garanzia cui agli artt. 45 e 46 del RGPD (decisioni di adeguatezza o garanzie adeguate) e, soltanto qualora ciò non risulti possibile, ricorrere alle ipotesi di deroga indicate dall'art. 49, par. 1, del RGPD. Tali deroghe, infatti, "devono essere interpretate in maniera restrittiva affinché l'eccezione non diventi la regola" (art. 49; cfr. linee guida 2/2018 cit.; cfr. anche WP114 Documento di lavoro su un'interpretazione comune dell'art. 26, par. 1 della direttiva 95/46/CE", adottato dal Gruppo Art. 29 il 25 novembre 2005).

Nel caso specifico, al fine di verificare se possa 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"), l'interesse pubblico perseguito deve essere riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro (art. 49, par. 4). In questo quadro, si è ricordato che l'esistenza di un accordo o di una convenzione internazionale che stabilisca un determinato obiettivo, da favorire con la cooperazione internazionale, "deve essere considerato come un indicatore ai fini della valutazione dell'esistenza di un interesse pubblico ai sensi dell'art. 49, par. 1, lett. *d*), purché l'Unione europea o gli Stati membri abbiano sottoscritto tale accordo o convenzione". È stato anche suggerito al Ministero di valutare l'esi-

stenza presso l'Unicef di *policy* interne o l'adesione ad accordi standard o principi internazionalmente riconosciuti che, nelle more dell'adozione di decisioni di adeguatezza, offrano comunque agli interessati garanzie in ordine al rispetto dei diritti fondamentali e delle garanzie in materia di protezione dei dati personali (nota 15 luglio 2019).

4.9. *L'attività svolta in relazione ai Responsabili della protezione dei dati in ambito pubblico*

In occasione di diverse istruttorie l'Ufficio è venuto a conoscenza di numerose situazioni in cui un unico soggetto (per lo più persone giuridiche, spesso già fornitrici di supporto tecnologico/informatico) risultava designato quale Rpd da parte di diverse centinaia di enti pubblici (prevalentemente, amministrazioni comunali di piccole e medie dimensioni ed istituzioni scolastiche). Conseguentemente, in ragione della numerosità degli incarichi accumulati da singole società e di possibili conflitti di interesse dovuti alla sovrapposizione dei ruoli di Rpd e di fornitore di servizi IT, l'Autorità ha effettuato una serie di accertamenti sui profili connessi alla designazione di soggetti esterni quali Rpd da parte di enti pubblici. Altri aspetti oggetto di indagine hanno riguardato l'instaurazione del rapporto contrattuale con la società scelta quale Rpd nonché l'individuazione della persona fisica quale referente presso l'ente per conto della persona giuridica. L'attività di raccolta di informazioni ha altresì comportato lo svolgimento di una procedura di consultazione delle altre autorità europee, ai sensi dell'art. 61 del RGPD, al fine di comprendere se nei vari ordinamenti si fossero registrate problematiche analoghe nonché per conoscere le eventuali iniziative intraprese. Tutte le informazioni raccolte nel corso di questa intensa attività di controllo e consultazione verranno debitamente analizzate e costituiranno la base per programmare le future iniziative del Garante al fine di rafforzare il ruolo del Rpd, quale elemento centrale di supporto ai titolari nell'assicurare che i trattamenti effettuati in ambito pubblico siano in linea con il quadro giuridico in materia di protezione dei dati personali.

L'Autorità ha inoltre proseguito le attività volte a sostenere i Rpd nello svolgimento del loro delicato compito, anche attraverso incontri e iniziative formative. Attraverso due progetti europei (T4DATA e SMEDATA, illustrati nel dettaglio al par. 21.5), il Garante ha svolto una rilevante attività di supporto alla formazione dei Rpd di amministrazioni pubbliche e del settore privato tramite seminari e convegni, svolti su tutto il territorio nazionale, e autoproducendo n. 32 *webinar* che illustrano i principali aspetti del nuovo quadro normativo, resi disponibili gratuitamente a tutti i Rpd pubblici tramite un'apposita piattaforma. Tra le varie iniziative messe in campo con l'obiettivo di sensibilizzare i titolari e i responsabili del trattamento a riconoscere l'importanza del ruolo del Rpd, il Garante ha promosso, sin dal primo incontro di Bologna del 2018, la creazione di "reti di Rpd" per settori omogenei.

In diversi ambiti questa sollecitazione è stata raccolta e si sono create, principalmente in ambito pubblico, le prime reti con le quali si sono aperti tavoli di lavoro: ci si riferisce, in particolare, alla rete dei Rpd del settore della ricerca pubblica, del settore della fiscalità, dei Ministeri, delle autorità indipendenti e del settore sanitario, su base regionale. Attraverso questa attività è stata incoraggiata l'analisi delle problematiche comuni ai vari settori e l'individuazione di soluzioni condivise, con l'obiettivo di accelerare il processo di adeguamento.

A seguito di un'attività di analisi del contenuto delle comunicazioni concernenti le designazioni dei Rpd inviate al Garante, è stata altresì avviata una massiccia cam-

pagna di sollecitazione nei confronti di quegli enti pubblici che, pur essendo tenuti a designare il Rpd, non hanno effettuato correttamente la comunicazione dei dati di contatto. Quest'azione, che proseguirà anche nel 2020, consentirà di poter interagire con i Rpd con la tempestività necessaria, ogni qual volta se ne determineranno i presupposti (ad es. in caso di *data breach*), e di disporre di una mappatura più accurata dell'adempimento per le successive eventuali azioni correttive.

L'Autorità ha altresì formulato diversi pareri ai Rpd volti a chiarire gli aspetti organizzativi e le modalità idonee a garantire il corretto svolgimento dei compiti assegnati. Tra questi si segnala il parere rilasciato al Rpd di un ente comunale sulla compatibilità tra tale funzione e lo svolgimento di un altro incarico dirigenziale. Sul punto, nel rammentare quanto dichiarato nelle linee guida sui responsabili della protezione dei dati, adottate il 13 dicembre 2016 dal Gruppo Art. 29, circa l'inopportunità, per un Rpd, di rivestire, all'interno dell'organizzazione del titolare del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali, si è ribadito l'obbligo, posto in capo ai titolari, di garantire che il Rpd possa svolgere il suo incarico con indipendenza e imparzialità, anche fornendogli le risorse umane e temporali necessarie allo svolgimento del suo ruolo strategico (note 21 marzo e 17 aprile 2019).

5 La sanità e la ricerca

5.1. *I trattamenti di dati per fini di cura*

Violazione dei dati

Numerose istruttorie hanno riguardato comunicazioni di violazioni di dati personali effettuate da aziende e strutture sanitarie; nel 70% dei casi la violazione nasce da un'erronea comunicazione della documentazione clinica (es. referti, schede di dimissione ospedaliera, cartelle cliniche) a un soggetto diverso dall'interessato. Nella metà dei casi oggetto di istruttoria, tale erronea comunicazione di dati sulla salute è avvenuta attraverso lo strumento del Fascicolo sanitario elettronico (Fse) e del *dossier* sanitario; in alcuni dei *data breach* notificati al Garante la violazione ha avuto ad oggetto il sistema di refertazione *online*; altri casi hanno riguardato la mancata adozione di misure di sicurezza, soprattutto di tipo organizzativo, da parte delle aziende sanitarie, con conseguente accesso non autorizzato ai dati sulla salute o perdita di informazioni e di documenti diagnostici. In altri casi, la violazione è stata causata dall'erroneo utilizzo dei dati di contatto dell'interessato, che ha determinato la comunicazione non autorizzata di informazioni cliniche a terzi (familiari o a professionisti sanitari).

Comunicazione a terzi

Un altro gruppo di violazioni di dati personali si sono verificate per un utilizzo improprio dell'*e-mail* nell'invio di comunicazioni contenenti dati sulla salute (per erroneo indirizzamento o per l'invio di comunicazioni relative a più interessati utilizzando il campo "copia conoscenza" (cc), in luogo di quello riservato "copia conoscenza nascosta" (ccn), comunicando così indirettamente, a soggetti che non erano tenuti a conoscerli, dati sulla salute di numerosi interessati).

Si evidenzia il caso relativo a una segnalazione concernente una procedura amministrativa attuata da un'azienda sanitaria per ottenere, da una società fornitrice di presidi ortopedici, la presentazione di offerte economiche per la fornitura di un certo numero di protesi. Unitamente alla richiesta di preventivo l'azienda aveva inviato anche moduli contenenti dati personali e sulla salute dei pazienti destinatari dei dispositivi ordinati. Nell'ambito dell'istruttoria è stato accertato che la citata comunicazione era stata effettuata in violazione dei principi di liceità, correttezza, trasparenza e minimizzazione (art. 5 del RGPD) e al di fuori dei casi previsti dall'art. 9, par. 2, del RGPD, per i quali il trattamento dei dati sulla salute è ammesso. All'esito del procedimento, in relazione alle predette violazioni, tenendo in considerazione tutte le circostanze del caso e in considerazione di quanto previsto dall'art. 22, comma 13, d.lgs. n. 101/2018 in ordine alla "prima applicazione delle disposizioni sanzionatorie", il Garante ha comminato all'azienda sanitaria una sanzione amministrativa pari a 8.000 euro (provv. 14 novembre 2019, n. 210, doc. web n. 9269852).

Cartelle cliniche

Una questione sollevata in maniera ricorrente riguarda la richiesta di cancellazione, da parte degli interessati, di dati personali contenuti nelle cartelle cliniche. In questo peculiare ambito è stato più volte ribadito che tali informazioni non possono essere cancellate, essendo ammessa unicamente una loro rettifica o integrazione. Ciò in considerazione del fatto che tale documento è qualificato dalla giurisprudenza come atto pubblico volto ad attestare fedelmente, fino a querela di falso e nell'interesse di tutte le parti coinvolte, le specifiche scelte cliniche e terapeutiche

effettuate durante un episodio di ricovero e, in quanto tale, idoneo a produrre effetti su plurime situazioni giuridiche soggettive. La cartella clinica documenta, infatti, l'andamento della malattia, i medicamenti somministrati, le terapie e gli interventi praticati, l'esito della cura e la durata della degenza del paziente (v. già Cass. pen., sez. VI, 30 giugno 1975); "l'annotazione postuma (nella cartella clinica) di un fatto clinico rilevante integra il reato di falso materiale in atto pubblico, di cui all'art. 476 del codice penale" (Cass. pen., sez. V, 21 aprile 1983; Cass. pen., sez. V, 8 febbraio 1990).

Occorre infatti tenere presente che il diritto alla cancellazione dei dati personali, riconosciuto dall'art. 17 del RGPD, non può essere esercitato nei casi in cui il trattamento sia necessario:

- per l'adempimento di un obbligo legale, previsto dal diritto dello Stato membro cui è soggetto il titolare del trattamento, o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri (art. 17, par 3, lett. *b*), del RGPD);
- per motivi di interesse pubblico, nel settore della sanità pubblica e per fini di archiviazione nel pubblico interesse (art. 17, par. 3, lett. *c*), del RGPD).

Gli obblighi legali connessi alla tenuta della cartella clinica configurano quindi un caso di esclusione del diritto alla cancellazione. Ciononostante, è stato più volte ribadito che all'interessato è consentito ottenere l'aggiornamento, la rettifica, oppure, per motivi legittimi ed oggettivi, l'integrazione dei dati contenuti nella cartella clinica. Un'eventuale rivalutazione della correttezza delle informazioni presenti nella cartella clinica da parte del personale sanitario a ciò preposto, effettuata sulla base di presupposti tecnico-scientifici, non comporta la cancellazione dell'informazione, ma il diritto alla sua rettifica, al fine di garantire la correttezza dei dati, senza pregiudicare l'inalterabilità del contenuto della cartella clinica (a tutela del paziente e del medico che ha provveduto a redigerla).

App in pronto soccorso

Nel settore della digitalizzazione della sanità, sono state avviate attività istruttorie in merito all'utilizzo di *app* all'interno dei dipartimenti di emergenza e urgenza di aziende sanitarie e ospedali (pronto soccorso) volte ad offrire ai pazienti e ai loro familiari un servizio informativo relativo al percorso di cura. Le recenti linee di indirizzo nazionali sul *triage* intraospedaliero del Ministero della salute (accordo in sede di Conferenza Stato-Regioni 1° agosto 2019) richiamano in più punti la necessità che i dipartimenti di emergenza e urgenza assicurino una comunicazione "efficace ed empatica sia con il paziente, sia con i familiari/accompagnatori". Secondo quanto rappresentato nelle citate linee di indirizzo, "il tempo d'attesa in pronto soccorso può rappresentare un'opportunità per trasmettere al cittadino informazioni utili e coerenti sull'esperienza che sta vivendo come paziente o accompagnatore". In tal senso, il Ministero della salute ritiene necessario promuovere una serie di iniziative di "attesa attiva" finalizzate al miglioramento degli aspetti di *comfort* in sala attesa; tra questi, sono segnalati la presenza di strumenti quali "cartellonistica", "la presenza di *display* che permettono di conoscere in tempo reale il numero di postazioni di emergenza impegnate, il numero di pazienti nelle sale visita o in attesa di ricovero, in modo da tenere aggiornati i pazienti oltre che sul proprio *iter* anche sul carico di lavoro complessivo del pronto soccorso". Alla luce della disciplina vigente, tali iniziative devono però essere accuratamente analizzate da parte del titolare – tenendo in particolare considerazione che, attraverso tali strumenti, potrebbero essere trattate, in relazione agli ampi bacini di utenza degli ospedali pubblici, informazioni sulla salute relative a un numero considerevole di pazienti – commisurando in via preventiva i rischi per i diritti e le libertà degli interessati e individuando misure adeguate al fine di minimizzarli.

5

In relazione ad alcune di queste istruttorie il Garante ha avviato un procedimento sanzionatorio in relazione alla violazione dei principi di *accountability*, di minimizzazione e di sicurezza dei dati (art. 166 del Codice).

5.1.1. Il trattamento dei dati personali riferiti ai pazienti per finalità ulteriori rispetto alla cura

Diverse istruttorie hanno messo in evidenza la circostanza che non sempre sono tenute nella dovuta considerazione le buone pratiche di anonimizzazione dei dati nell'ambito delle relazioni tenute da professionisti sanitari a convegni scientifici; la prassi di riportare, nella presentazione dei *case study*, elementi quali le iniziali del nome e del cognome, il nome di battesimo, i dettagli relativi alla storia personale dei pazienti ai quali ci si riferisce, non consente di ritenere non identificabili gli interessati, con la conseguenza che i dati mantengono la natura "personale" e non possono quindi essere liberamente diffusi. Ciò tenendo conto che la disciplina vigente vieta la diffusione dei dati idonei a rivelare lo stato di salute degli interessati (artt. 2-*septies*, comma 8 e 166, comma 2, del Codice) e che, con specifico riferimento alla pubblicazione di casi clinici, il codice di deontologia medica, approvato dalla Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri nel 2014 (così come modificato nel 2016 e nel 2017), prevede espressamene che "il medico assicura la non identificabilità dei soggetti coinvolti nelle pubblicazioni o divulgazioni scientifiche di dati e studi clinici" (art. 11 - riservatezza dei dati personali).

In relazione a questi casi sono state avviate alcune istruttorie al fine di accertare le responsabilità in ordine all'utilizzo dei dati e alla correttezza del processo di anonimizzazione dei documenti clinici utilizzati nell'ambito delle pubblicazioni o dei convegni scientifici.

Un altro caso di utilizzo improprio di dati idonei a rivelare lo stato di salute degli interessati è emerso nell'ambito di una istruttoria avente ad oggetto la documentazione presentata da alcuni medici per la partecipazione a concorsi pubblici. Al fine di attestare la specifica esperienza maturata, sono state depositate presso la commissione di concorso le copie dei registri di casistica operatoria contenenti gli elenchi degli interventi chirurgici effettuati recanti, in chiaro, i dati identificativi dei pazienti operati, data e tipo di intervento, diagnosi e natura della terapia effettuata. Nell'ambito dell'istruttoria è emerso che tale documentazione era stata acquisita dai medici delle strutture presso le quali avevano operato in modo non conforme alla disciplina vigente. La partecipazione di un medico all'avviso pubblico per una selezione non è infatti finalità riconducibile a quelle di cura o amministrativa che stanno alla base del trattamento dei dati relativi alla salute degli interessati da parte dell'azienda ospedaliera o sanitaria presso la quale il medico ha operato, essendo invece volta al perseguimento di una finalità personale (la partecipazione alla procedura selettiva). Nel caso considerato è stato altresì rilevato che la comunicazione dei dati personali non era neanche prevista dall'avviso pubblico che si limitava alla sola "certificazione del direttore sanitario riguardante la tipologia quantitativa e qualitativa delle prestazioni effettuate dal candidato" (quindi a documentazione priva di dati personali), in linea con il d.m. 30 gennaio 1992, n. 283 (art. 4, comma 5). Analogamente, nell'ambito dell'attribuzione dei punteggi, si faceva riferimento alla tipologia quantitativa e qualitativa delle prestazioni effettuate dal candidato, anche con riguardo all'attività casistica, misurabile in termini di volume e complessità. In relazione alle violazioni accertate nell'ambito del procedimento sono stati avviati procedimenti sanzionatori nei confronti dei medici e, in un caso, anche di un'azienda sanitaria.

L'Autorità è intervenuta con riferimento a comunicazioni di dati relativi alla salute di pazienti sottoposti agli accertamenti diagnostici presso un'azienda sanitaria

pubblica effettuate nei confronti di una società che forniva le apparecchiature di alta diagnostica. Nel caso istruito, riferito ad un periodo antecedente all'applicazione del RGPD, è emerso infatti che l'azienda sanitaria aveva messo a disposizione della società copie di immagini della TAC di alcuni pazienti, dopo aver proceduto alla pseudonimizzazione dei dati, per attestare la qualità delle proprie apparecchiature nell'ambito di una gara d'appalto. Nel caso di specie è stato rilevato un trattamento illecito consistente nella comunicazione (in assenza di un'adeguata base normativa), da parte dell'azienda sanitaria alla società, di informazioni sulla salute di alcuni pazienti identificati; la mera disponibilità dei dati in conseguenza della designazione della società a responsabile del trattamento (per le attività di manutenzione e mantenimento in efficienza dell'apparecchiatura e della qualità delle immagini della TAC) non consente infatti l'utilizzo da parte della stessa dei dati personali per una finalità propria (quale deve essere considerata la partecipazione a una gara pubblica), in assenza di idonea base giuridica (provv. 24 luglio 2019, n. 153, doc. web n. 9136842).

Consip

In merito al trattamento dei dati personali effettuato nelle gare pubbliche del settore sanitario, è stato quindi avviato un confronto con Consip al fine di individuare modalità appropriate per consentire alle società partecipanti alle gare del settore sanità di dimostrare la sussistenza dei requisiti tecnico-funzionali richiesti nei bandi di gara, individuando però opportune misure a protezione dei dati personali dei pazienti. È stato evidenziato che la struttura sanitaria può, previa anonimizzazione e nel rispetto del principio di minimizzazione dei dati (art. 5, par. 1, lett. *c*), del RGPD), fornire le immagini richieste alle società partecipanti alle gare. Più in generale, è stata condivisa con Consip l'opportunità di prevedere, già in sede di predisposizione dei bandi di gara aventi ad oggetto l'acquisto delle apparecchiature e dei dispositivi medici da parte delle strutture sanitarie, come peraltro previsto nel cons. n. 78 del RGPD, specifiche misure a garanzia degli interessati nonché la necessità di inserire, nel contratto standard, la nomina dell'aggiudicatario quale responsabile del trattamento ai sensi dell'art. 28 del RGPD. La prosecuzione dell'interazione con Consip potrà consentire di predisporre i modelli contrattuali utilizzati nelle iniziative di selezione del contraente a evidenza pubblica in modo da prevedere idonee misure a garanzia della riservatezza dei diritti e delle libertà degli interessati ogni qual volta si determina un trattamento di dati personali su larga scala o il trattamento riguarda soggetti vulnerabili.

5.2. *Il Fascicolo sanitario elettronico e il* dossier *sanitario*

L'Ufficio ha continuato a prestare la propria collaborazione al Ministero della salute e del Mef in relazione all'implementazione del Fascicolo sanitario elettronico (Fse) anche attraverso l'attività prestata in seno al tavolo tecnico di monitoraggio e indirizzo per l'attuazione delle disposizioni inerenti al Fse (art. 26, d.P.C.M. n. 178/2015) presso il Ministero della salute. In particolare, sono state fornite specifiche osservazioni in merito alle iniziative legislative volte a ridefinire la disciplina in tema di Fse. Al riguardo, l'Autorità ha ritenuto ammissibile, alla luce del nuovo quadro giuridico in materia di protezione dei dati, un'eventuale modifica normativa che preveda l'abolizione della necessità di acquisire il consenso dell'interessato all'alimentazione del Fascicolo (provv. 7 marzo 2019, n. 55, punto 1, doc. web n. 9091942). Tale possibile modifica comporterebbe, nelle regioni in cui è stata creata l'infrastruttura tecnologica, l'immediata disponibilità a vantaggio di tutti gli interessati del Fse, con tutti i dati e documenti sanitari riguardanti l'assistito relativi alle

5

cure a carico del Servizio sanitario nazionale; tali dati potrebbero essere trattati dal Ministero della salute e dalle regioni per finalità amministrative di programmazione e controllo.

Ove tale modifica fosse apportata, rimarrebbe comunque ferma la necessità di acquisire uno specifico consenso dell'interessato per consentire la consultazione del Fse da parte del personale sanitario coinvolto nel percorso di cura. Occorre sempre considerare che, allo stato, il Fse si configura come uno strumento informativo di ausilio al personale sanitario per inquadrare lo stato di salute e non anche un documento, avente fede pubblica, come la cartella clinica. Una complessiva revisione dell'originario progetto dovrebbe essere accompagnata da una riflessione sulla natura giuridica del Fse e su un rinnovato sistema di alimentazione e consultazione dello stesso da parte dei professionisti sanitari nonché dall'individuazione di un adeguato quadro di garanzie per i diritti e le libertà fondamentali dell'interessato.

La proficua attività di collaborazione istituzionale ha riguardato anche le modalità tecniche e i servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità dei Fse. In particolare, l'Ufficio ha ribadito la necessità di analizzare la tipologia di dati e documenti che legittimamente sono conservati nel Sistema tessera sanitaria (Sistema Ts), al fine di individuare quelli che possono essere resi disponibili al Fse, in linea con la disciplina vigente che impone al Mef di conservare le informazioni solo per il tempo strettamente necessario al completamento delle operazioni tecniche di verifica, con l'irreversibile cancellazione di tali informazioni al termine delle operazioni (cfr. decreto Mef 27 luglio 2005, con riferimento alle ricette, e art. 50, comma 10, d.l. n. 269/2003, in relazione ai dati sulla liquidazione periodica dei rimborsi versati alle strutture di erogazione di servizi sanitari per prescrizioni farmaceutiche e specialistiche).

Sul punto è stata poi più volte espressa la necessità di limitare al solo interessato l'accesso, tramite Fse, ai documenti – concernenti l'aspetto prescrittivo e certificatorio legato alle prestazioni sanitarie, farmaceutiche e alle agevolazioni erogate dal Servizio sanitario nazionale – che non sono stati invece generati per finalità di cura; ciò al fine di evitare che a tali informazioni possano avere accesso soggetti diversi da quelli espressamente indicati dalla legge (Inps e, con certe limitazioni, il datore di lavoro).

In materia di Fse e *dossier* sanitario, l'Ufficio è intervenuto anche con riferimento a segnalazioni, reclami e *data breach* relativi all'erroneo inserimento, all'interno di tali strumenti, di documenti sanitari (quali referti o schede di dimissione ospedaliera) relativi a soggetti diversi dall'intestatario del Fascicolo o del *dossier*. In alcuni casi, l'erroneo inserimento è stato determinato da una non corretta identificazione dell'interessato dettata dalla mancanza di procedure volte a verificare l'esattezza del dato; in altri casi, l'Ufficio ha invece riscontrato una violazione del principio della *privacy by default* nella definizione dei profili di autorizzazione legati all'accesso al *dossier* sanitario.

Al fine di scongiurare il rischio di un accesso alle informazioni trattate mediante il *dossier* sanitario da parte di soggetti non autorizzati, il Garante, già nelle linee guida del 2015 (provv. 4 giugno 2015, n. 331, doc. web n. 4084632), aveva specificamente chiesto ai titolari del trattamento di porre particolare attenzione nell'individuazione dei profili di autorizzazione e nella formazione dei soggetti abilitati, in modo che l'accesso al *dossier* fosse limitato al solo personale sanitario che interviene nel processo di cura del paziente e fossero adottate opportune modalità tecniche di autenticazione. A tal fine, nelle linee guida il Garante aveva anche indicato ai titolari del trattamento la necessità di effettuare un monitoraggio dei casi in cui il personale sanitario può avere necessità di consultare il *dossier* sanitario per finalità di cura

dell'interessato e, in base a tale ricognizione, individuare i diversi profili di autorizzazione all'accesso. La mancanza di un'adeguata analisi da parte di alcune aziende sanitarie ha creato i presupposti per l'accesso ai dati relativi alla salute contenuti nei *dossier* sanitari aziendali da parte del personale medico, non al fine di prestare le cure all'interessato, ma per ragioni personali, riconducibili, in talune ipotesi, alla "mera curiosità". In questi casi l'Ufficio ha avviato un procedimento per l'adozione di provvedimenti correttivi e sanzionatori.

In altri casi è stato segnalato che, a fronte di una specifica richiesta dell'interessato di oscurare alcuni documenti sanitari all'interno del Fse o del *dossier*, in quanto attinenti ad ambiti particolarmente riservati (es. scelta riproduttiva consapevole), tali informazioni non sono state oscurate, con la conseguenza di essere risultate accessibili al medico di base dell'assistito, inficiando così l'essenza stessa della misura dell'oscuramento che ha lo scopo, in analogia a quanto avviene nel rapporto paziente-medico curante, di lasciare libero l'interessato di addivenire alla determinazione consapevole di non informare il secondo di alcuni eventi sanitari che lo riguardano, ovvero di consentire all'interessato di richiedere il parere di un altro professionista, senza che quest'ultimo possa essere influenzato da quanto già espresso da un collega. Anche in questi casi sono stati avviati i procedimenti per l'adozione di provvedimenti correttivi e sanzionatori.

5.3. *I trattamenti di dati relativi alle condizioni di salute per fini amministrativi*

L'Autorità continua a ricevere segnalazioni in merito alla presenza di diciture che riportano in modo esteso la tipologia dei dispositivi medici e delle prestazioni sanitarie in documenti fiscali, anche nei casi in cui tale livello di dettaglio non è richiesto dalla normativa di settore. Al riguardo è stata avviata una collaborazione con l'Agenzia delle entrate al fine di individuare una soluzione idonea a contemperare la protezione dei dati personali con l'attuazione della disciplina fiscale.

Nell'ambito dell'attività di collaborazione istituzionale con il Ministero della salute, l'Autorità ha partecipato ai lavori per l'aggiornamento della disciplina degli obiettivi, delle funzioni e della struttura del Sistema informativo trapianti (Sit) e del Registro nazionale dei donatori di cellule riproduttive a scopi di procreazione medicalmente assistita di tipo eterologo (parere 30 luglio 2019, n. 158, doc. web n. 9131111).

Uno dei principali ambiti di intervento ha riguardato la titolarità del trattamento che ha portato a superare l'originaria previsione della contitolarità tra il Ministero della salute e il Centro nazionale trapianti (Cnt) che non appariva conforme ai compiti e alle responsabilità dettate dal RGPD. Dagli approfondimenti svolti è emerso infatti che, nell'ambito del Sit, il ruolo di titolare è svolto esclusivamente dal Cnt, mentre al Ministero è attribuita la gestione di tutti i dati conservati nel Sit, nell'ambito del Nuovo sistema informativo del servizio sanitario nazionale (Nsis).

Un altro specifico ambito di intervento ha riguardato l'utilizzo di sistemi di codifica, mediante l'adozione di un sistema di identificazione indiretta e univoca a livello nazionale, dei dati anagrafici delle madri che hanno effettuato la fecondazione medicalmente assistita di tipo eterologo idonea, da un lato, ad assicurare la rintracciabilità del percorso delle cellule riproduttive dal donatore al nato e viceversa e, dall'altro, a garantire la riservatezza delle interessate. Al riguardo, sono state individuate le condizioni e i limiti che potevano legittimare la conoscibilità dei dati personali del donatore di gameti da parte della persona nata sulla base di tecniche di fecondazione eterologa, attraverso uno specifico richiamo alle disposizioni nor-

5

mative che consentono il processo di re-identificazione, con particolare riferimento ai cd. eventi avversi.

Ulteriori ambiti di intervento hanno riguardato i tempi di conservazione dei dati, l'assegnazione del codice identificativo nazionale della donazione, del donatore e del ricevente di organi e del codice unico europeo nonché la disciplina circa la destinazione e la conservazione dei dati personali contenuti nella relativa documentazione in caso di cessazione dell'attività dei centri di procreazione medicalmente assistita.

L'Autorità ha anche concluso la collaborazione con il Ministero della salute relativa alla definizione della disciplina per l'organizzazione e il funzionamento, presso il Dicastero, del Sistema di segnalazione delle malattie infettive, denominato Premal (parere 18 aprile 2019, n. 105, doc. web n. 9124009). Le principali osservazioni hanno riguardato la corretta individuazione del titolare e del responsabile del trattamento, anche con riferimento al ruolo dell'Istituto superiore di sanità, e l'esigenza che il titolare del trattamento adotti e verifichi periodicamente le misure adeguate in relazione al rischio al fine di prevenirne l'obsolescenza; sono state oggetto di specifica attenzione anche le informazioni da fornire all'interessato in merito a tale delicato trattamento, le modalità di esercizio dei diritti riconosciuti dal RGPD nonché l'individuazione delle misure per assicurare il rispetto del principio di limitazione della conservazione.

Significativa la collaborazione nell'ambito di un tavolo tecnico istituito presso il Ministero della salute con la partecipazione di vari attori istituzionali coinvolti nel procedimento di regolamentazione delle disposizioni anticipate di trattamento (Dat). All'esito delle valutazioni emerse in tale contesto, è stato adottato, con il parere favorevole dell'Autorità, un decreto volto all'istituzione presso il Ministero della salute di una Banca dati nazionale destinata alla raccolta delle Dat (cd. testamento biologico), che consentono alla persona di stabilire in anticipo i trattamenti sanitari ai quali intende essere sottoposta in caso di sopravvenuta incapacità ad autodeterminarsi (parere 29 maggio 2019, n. 123, doc. web n. 9117770). Obiettivo della Banca dati è quello di costituire un polo unico nazionale di tali dichiarazioni, seppure su base volontaria, costantemente aggiornato e di consentire un accesso tempestivo alle stesse da parte del personale medico in caso di necessità. Nella menzionata Banca dati saranno raccolte, con il consenso della persona che si è avvalsa del testamento biologico, le copie delle dichiarazioni, i successivi aggiornamenti delle stesse nonché la nomina e la revoca dell'eventuale fiduciario, anche di quanti non sono iscritti al Ssn.

I principali interventi del Garante hanno riguardato l'introduzione di disposizioni volte ad assicurare, in linea con quanto indicato sul punto anche dal Consiglio di Stato con il parere del 31 luglio 2018, che l'accesso alle Dat sia consentito solo al medico che ha in cura l'assistito, allorché sussista una situazione di incapacità di autodeterminarsi, e al fiduciario, se nominato. Il Garante è inoltre intervenuto con riferimento al periodo di conservazione dei dati, prevedendo che gli stessi siano cancellati dalla Banca dati nazionale, trascorsi dieci anni dal decesso dell'interessato. Ulteriori ambiti di intervento hanno riguardato l'esercizio dei diritti degli interessati, le informazioni da rendere agli stessi, le modalità di accesso alle Dat da parte del medico che ha in cura l'assistito o del fiduciario come pure la corretta individuazione dei soggetti che, in qualità di titolari del trattamento, sono legittimati a trasmettere le Dat alla Banca dati. L'Autorità ha poi considerato una misura appropriata la previsione della comunicazione di riscontro tempestiva, all'interessato che ne abbia fatto richiesta, in merito all'avvenuta acquisizione della documentazione nella Banca dati nazionale.

Con riferimento al trattamento dei dati personali effettuato nell'ambito della raccolta delle Dat, nelle more della realizzazione della Banca dati nazionale, l'Ufficio è intervenuto anche in relazione ad alcune iniziative regionali volte alla realizzazione di banche dati locali per favorirne un coordinamento con quella nazionale ed evitare così duplicazioni degli archivi, assicurando l'introduzione di misure coerenti a tutela degli interessati sul territorio nazionale.

Medicina d'iniziativa

È proseguita l'attività istruttoria in merito ad alcune iniziative regionali legate alla cd. medicina di iniziativa, locuzione presente in numerosi atti di indirizzo e programmazione del Ministero della salute e regionali ancorché non esista nell'ordinamento nazionale una definizione e una disciplina specifica riservata ad essa. Dall'analisi di tali documenti risulta che per medicina di iniziativa si intende un modello assistenziale orientato alla promozione attiva della salute dell'individuo, specie se affetto da malattie croniche o disabilità, e alla responsabilizzazione delle persone nel percorso di cura. Sul punto, riprendendo riflessioni già espresse con riferimento al Fse e ai regolamenti per il trattamento dei dati sensibili e giudiziari, va rilevato che l'adozione di tali sistemi determina la raccolta e l'elaborazione di dati sanitari al fine di realizzare, con riferimento a specifiche patologie, un profilo sanitario di rischio dell'interessato, configurandosi quindi un trattamento finalizzato al miglioramento dell'offerta di cura, autonomo e ulteriore rispetto a quello principale per il quale il paziente si è rivolto al medico di medicina generale.

Il trattamento in questione, presente in varie iniziative regionali, è da intendersi quindi non strettamente necessario alla cura ed è legato al diritto di conoscere (o meno) il proprio profilo di rischio sanitario. Tale trattamento dovrebbe pertanto assumere il carattere della volontarietà ed essere effettuato sulla base della preventiva acquisizione del consenso informato dell'assistito ovvero di un altro presupposto di liceità di cui all'art. 9, par. 2, lett. *a*), del RGPD (cfr. provv. 7 marzo 2019, n. 55, doc. web n. 9091942). Al riguardo, il Ministero della salute è stato più volte invitato a disciplinare con un atto normativo questa complessa e delicata attività che presenta rischi elevati per i diritti e le libertà delle persone e presenta altresì significativi risvolti etici (quale il diritto di non sapere).

Cup

Continuano le attività istruttorie nei confronti dei sistemi regionali di prenotazione delle prestazioni sanitarie (Cup) che spesso prevedono la fornitura del servizio di *call center* in *outsourcing*. Al riguardo, è stato evidenziato che prevedere la preposizione al trattamento dei dati di società che prestano tali servizi comporta la necessità di disciplinare il trattamento, nell'ambito di un idoneo atto giuridico, ai sensi dell'art. 28 del RGPD. In particolare, sono state riscontrate criticità nella scelta, seguita in alcune realtà territoriali, di autorizzare al trattamento persone fisiche che non operano presso il titolare o il responsabile, bensì presso una società terza non designata responsabile del trattamento. In tal caso gli operatori Cup autorizzati al trattamento devono effettivamente operare sotto la "diretta autorità" del titolare o del responsabile del trattamento.

5.4. *I chiarimenti rispetto alle innovazioni normative in ambito sanitario*

In ambito sanitario il nuovo assetto normativo previsto dal RGPD ha avuto un impatto significativo sulla disciplina relativa al trattamento dei dati sulla salute, sì che il Garante ha ritenuto opportuno fornire chiarimenti a supporto dei soggetti operanti nel settore (provv. 7 marzo 2019, n. 55, doc. web n. 9091942). Nel provvedimento si è illustrato come debba essere applicata l'eccezione indicata nell'art. 9, par. 2, lett. *h*), del RGPD, ricollegabile ai trattamenti necessari per "finalità di

5

cura", precisando che detti trattamenti sono quelli effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa tenuta all'obbligo di segretezza. Ciò comporta che tali figure professionali non hanno più l'obbligo di richiedere, come per il passato, il consenso per i trattamenti di dati necessari alla prestazione sanitaria richiesta, sia che operino come liberi professionisti presso uno studio medico sia all'interno di una struttura sanitaria pubblica o privata. Di contro, è stato precisato che è richiesto il consenso, o una distinta base giuridica, quando tali trattamenti non sono strettamente necessari per le finalità di cura, cioè essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute, anche quando effettuati da professionisti della sanità. Ne sono un esempio i trattamenti di dati sulla salute connessi all'uso di *app* mediche (ad eccezione di quelle per la telemedicina), quelli effettuati per la fidelizzazione della clientela (come quelli praticati da alcune farmacie o parafarmacie), oppure per finalità promozionali, commerciali o anche elettorali.

In ogni caso, sulla base della normativa di settore vigente e precedente all'applicazione del RGPD, permane invece la necessità di acquisire il consenso per la consultazione dei referti *online* (d.P.C.M. 8 agosto 2013, art. 5) e, come detto, per il trattamento dei dati relativo al Fse (art. 12, comma 5, d.l. 18 ottobre 2012, n. 179).

Per quanto riguarda i trattamenti effettuati attraverso il *dossier* sanitario, oggetto delle linee guida in materia di *dossier* sanitario del 4 giugno 2015, n. 331 (doc. web n. 4084632), il Garante ha colto l'occasione per anticipare che verranno individuati, nell'ambito dell'adozione del provvedimento contenente le misure di garanzia ai sensi dell'art. 2-*septies*, del Codice, i trattamenti che potranno essere effettuati senza il consenso degli interessati. Nel medesimo provvedimento sono stati forniti chiarimenti anche in merito alle informazioni che devono essere rese agli interessati in attuazione del principio di trasparenza (artt. 5, par. 1, lett. *a*), e 13 del RGPD). In questo ambito il RGPD prevede nuovi elementi informativi, quali quelli relativi al tempo di conservazione dei dati che, se non specificati dalla normativa di settore, dovranno comunque essere individuati dal titolare alla luce del principio di responsabilizzazione. Inoltre i titolari del trattamento sono stati invitati ad adottare informative in forma concisa, trasparente, intelligibile e facilmente accessibile per gli interessati, utilizzando un linguaggio semplice e chiaro ed è stato suggerito, per i titolari del trattamento che effettuano più operazioni caratterizzate da particolare complessità (come ad es. le aziende sanitarie) di fornire le informazioni in modo progressivo, rendendo gli elementi informativi relativi a particolari attività di trattamento, in fasi successive, solo ai pazienti effettivamente interessati.

Rpd in ambito sanitario

In relazione agli altri adempimenti previsti dal RGPD, l'Autorità ha anche colto l'occasione per fornire alcuni chiarimenti in merito alla designazione del Rpd, evidenziando che sono tenuti alla nomina di tale figura tutti gli organismi pubblici, nonché gli operatori privati che effettuano trattamenti sanitari su "larga scala", quali le case di cura, gli ospedali privati e le residenze sanitarie assistenziali (Rsa) (cfr. anche linee guida sui Responsabili della protezione dei dati, WP243, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, punto 2.1.3, doc. web n. 612048, fatte proprie dal Cepd il 25 maggio 2018: cfr. *Endorsement* 1/2018). Non sono invece tenuti alla nomina del Rpd i singoli professionisti che operino in regime di libera professione a titolo individuale o altri soggetti che non effettuano trattamenti su "larga scala", come le farmacie, le parafarmacie, le aziende ortopediche (cons. 91 e linee guida sui Rpd cit., punto 2.1.3).

Registro dei trattamenti

Quanto, infine, al registro delle attività di trattamento, previsto dall'art. 30 del RGPD, il Garante ha chiarito che tutti gli operatori sanitari sono tenuti a questo

obbligo. Ciò in quanto, essendo le fattispecie di esenzione di cui all'art. 30, par. 5, del RGPD tra loro alternative (cfr. Gruppo Art. 29, *Position paper related to article 30(5)* fatte proprie dal Cepd con l'*Endorsement* 1/2018), la deroga relativa alla tenuta del Registro non opera in presenza anche di uno solo degli elementi indicati da tale disposizione. È stato infine evidenziato che la redazione del Registro dei trattamenti rappresenta un elemento essenziale per il governo dei trattamenti e per l'efficace individuazione di quelli a maggior rischio, nonché per dimostrare il rispetto del principio di *accountability* previsto dal RGPD.

5.4.1. L'esercizio dei diritti in ambito sanitario

L'Ufficio ha fornito chiarimenti in ordine alle procedure da seguire in caso di esercizio dei diritti (artt. da 15 a 22 del RGPD) aventi ad oggetto dati relativi alla salute e in questo ambito sono stati trattati diversi reclami.

In particolare, tra quelli pervenuti e in relazione ai quali l'Autorità ha invitato il titolare del trattamento ad aderire alle richieste del reclamante (nelle ipotesi di mancato o inidoneo riscontro) o l'interessato a esercitare i diritti nei confronti del titolare (nei casi in cui il reclamante non avesse ancora proposto al titolare alcuna istanza), quelli concernenti la richiesta di accesso ai dati di cui all'art. 15 del RGPD sono risultati prevalenti rispetto a quelli relativi all'esercizio degli altri diritti. Ciò, nella maggioranza dei casi, per ottenere l'accesso ai dati contenuti nella propria cartella clinica o in quella di congiunti deceduti, secondo quanto disposto dall'art. 2-*terdecies* del Codice.

La prevalenza dei reclami attraverso i quali sono stati lamentati riscontri incompleti o poco chiari, più che veri e propri atteggiamenti omissivi da parte dei titolari del trattamento, ha messo a nudo le difficoltà che incontrano questi ultimi nel soddisfare adeguatamente le istanze conoscitive degli interessati.

5.4.2. La valutazione d'impatto in ambito sanitario

In più di un'occasione l'Autorità ha avuto modo di fornire indicazioni in merito alle valutazioni di impatto effettuate con riferimento a iniziative in ambito sanitario che prevedevano il trattamento dei dati sulla salute dei pazienti, in relazione alle quali alcune aziende sanitarie avevano avanzato al Garante una richiesta di consultazione preventiva (art. 36, par. 3, del RGPD). In alcuni casi si è evidenziato che la mancanza degli elementi essenziali della valutazione di impatto non consentiva di poter esprimere il parere sulla richiesta; è stato così osservato che la richiesta di consultazione preventiva all'Autorità deve essere effettuata solo qualora dalla valutazione d'impatto sulla protezione dei dati emerga un rischio elevato per i diritti e le libertà delle persone se non venissero adottate dal titolare le garanzie, le misure di sicurezza e i meccanismi per attenuare i rischi individuati nella valutazione (cfr. cons. 94). Nella richiesta di consultazione preventiva il titolare è quindi chiamato a indicare le misure che sono state individuate per affrontare e, di conseguenza, ridurre i rischi che un determinato trattamento può comportare per i diritti e le libertà delle persone, affinché il Garante possa valutare se individuare misure aggiuntive, al fine di attenuare ulteriormente tale rischio.

Sul punto è stato in più occasioni rilevato che non spetta all'Autorità, nell'ambito del procedimento di consultazione preventiva, individuare la base giuridica di liceità del trattamento; in base ai principi in materia di protezione dei dati personali e, in particolare, al principio di responsabilizzazione, è rimesso infatti a ciascun titolare individuare i presupposti e le condizioni di liceità del trattamento dei dati nonché essere in grado di dimostrare che il trattamento venga effettuato conformemente al RGPD (cfr. artt. 5 e 24).

5

Tra i casi esaminati merita evidenziare anche la richiesta di consultazione preventiva, avanzata da una società operante in ambito sanitario, in relazione alla possibilità di procedere alla consegna dei referti ai pazienti attraverso l'applicativo Telegram. Il Garante ha rappresentato di non poter rendere il previsto parere essendo la richiesta priva di alcuni degli elementi indicati dall'art. 36, par. 3, del RGPD e, in particolare, delle ragioni per le quali si intendeva introdurre, nel rispetto dei principi di minimizzazione e di proporzionalità dei dati, una modalità differente di consegna dei referti all'interessato rispetto a quelle indicate nel d.P.C.M. 8 agosto 2013 relativo alle modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali (artt. 5 e 6, par. 3, lett. *b*), del RGPD). La richiesta è risultata altresì priva dell'indicazione dei rispettivi ruoli e delle responsabilità dei titolari e dei responsabili del trattamento, con particolare riferimento alla società Telegram LLC; né sono state indicate le ragioni dell'inidoneità delle misure e delle garanzie previste per proteggere i diritti e le libertà degli interessati tali da dover richiedere la consultazione preventiva del Garante. La valutazione d'impatto si era limitata, infatti, a descrivere le menzionate modalità di consegna dei referti e a indicare sommariamente i rischi, senza procedere a determinare le specifiche misure per ridurli.

Le ragioni addotte dal titolare relative alla circostanza che il sistema Telegram arginerebbe il rischio di "mancato invio della *e-mail*, invio del referto errato, invio ad un destinatario errato, mancato inserimento dell'allegato" e assicurerebbe una maggiore "immediatezza" della disponibilità del referto non sono state suffragate da valutazioni di carattere tecnico e giuridico in merito al rispetto dei principi di minimizzazione e di proporzionalità di cui agli artt. 5 e 6, par. 3, lett. *b*), del RGPD. Il sistema esaminato avrebbe comunque determinato una sistematica comunicazione di categorie particolari di dati alla società Telegram LLC, con riferimento alla quale non sono state indicate le misure e le garanzie con le quali il titolare del trattamento avrebbe inteso proteggere i diritti e le libertà degli interessati nell'ambito del suddetto flusso di dati sulla salute, tenuto conto che il servizio di messaggistica istantanea e *broadcasting* Telegram è realizzato per finalità di comunicazione di carattere personale; l'uso di tale servizio privo di configurazioni *ad hoc* per le finalità diverse e ulteriori, e, quindi, senza la possibilità di prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi del paziente, né tantomeno di verificare periodicamente tali misure (ad es. svolgere *audit, vulnerability assessment, penetration test*), non consente quindi di realizzare un sistema di refertazione aderente al principio di *accountability* alla base della protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (artt. 5 e 25 del RGPD).

5.4.3. I chiarimenti in relazione ai Responsabili della protezione dei dati e le attività con le reti dei Rpd del settore della sanità e della ricerca

L'attività prestata dall'Autorità nell'ambito del progetto volto alla formazione dei Rpd denominato T4DATA (cfr. par. 21.5) ha riguardato anche il trattamento dei dati personali in ambito sanitario e di ricerca. In particolare, per tali settori è stato realizzato un seminario *ad hoc* sul trattamento dei dati personali per finalità di cura e ricerca cui hanno partecipato circa 300 Rpd del settore sanitario pubblico e privato (Ancona, 7 giugno 2019). In tale ambito sono state affrontate varie tematiche quali quelle della sanità e della gestione dei rischi connessi ai trattamenti di dati personali, dell'esame dei presupposti di liceità del trattamento in ambito sanitario, dell'implementazione del quadro normativo di riferimento attraverso regole deontologiche, codici di condotta e misure di garanzia, dell'analisi della disciplina applicabile per il trattamento dei dati a scopi di ricerca scientifica in campo medico, biomedico e

epidemiologico. L'evento si è concluso con l'esame dei primi casi pratici sottoposti all'attenzione dell'Autorità a seguito dell'entrata in vigore del RGPD e con un dibattito nel corso del quale è stato fornito riscontro ai principali quesiti inerenti alle questioni maggiormente controverse. In ambito sanitario e di ricerca sono stati anche registrati 5 *webinar* relativi alle seguenti aree tematiche: "Presupposti di liceità del trattamento dei dati sulla salute in ambito sanitario"; "Banche dati sanitarie pubbliche e trattamenti per fini amministrativi correlati alla cura"; "Sanità digitale"; "I registri delle attività di trattamento e la cooperazione con l'autorità di controllo"; "Il trattamento dei dati personali per finalità di ricerca scientifica e a fini statistici"; "Archiviazione nel pubblico interesse e ricerca storica e libertà di espressione e di informazione". Tali *webinar* sono stati resi disponibili ai Rpd operanti nel settore pubblico attraverso la piattaforma appositamente creata e accessibile tramite il sito dell'Autorità.

A completamento dell'attività di supporto, l'Ufficio ha svolto anche numerosi incontri con i Rpd delle aziende sanitarie, tra i quali si segnala quello svolto presso la Conferenza Stato-Regioni con i Rpd delle regioni con specifico rifermento ai trattamenti dei dati da parte di queste ultime nel settore sanitario.

Una significativa attività di collaborazione è stata svolta con numerose associazioni e federazioni di categoria in ordine all'avvio di iniziative volte alla realizzazione dei codici di condotta previsti dall'art. 40 del RGPD in specifici settori caratterizzati dal trattamento dei dati sulla salute e per finalità di ricerca scientifica.

Parimenti è stato fornito un significativo supporto all'attività dei Rpd che operano nel settore della ricerca e della statistica. Tale attività ha portato all'insediamento, il 4 luglio 2019, alla presenza dei rappresentanti dell'Ufficio, del Tavolo di lavoro permanente dei Rpd degli Enti Sistan e dei direttori degli uffici di statistica.

5.5. *La ricerca*

5.5.1. Prescrizioni relative al trattamento dei dati genetici e al trattamento dei dati personali effettuato per scopi di ricerca scientifica

Conclusa la consultazione pubblica sullo schema di provvedimento adottato il 13 dicembre 2018, con il quale sono state individuate le prescrizioni contenute nelle autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 ritenute compatibili con la nuova cornice normativa (cfr. Relazione 2018, pp. 85 ss.), il Garante ha adottato le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, d.lgs. 10 agosto 2018, n. 101 (provv. 5 giugno 2019, n. 101, doc. web n. 9124510).

Con specifico riferimento alle prescrizioni relative al trattamento dei dati genetici e al trattamento dei dati personali effettuato per scopi di ricerca scientifica – confluite, rispettivamente, negli all. nn. 4 e 5 del citato provvedimento –, va evidenziata la partecipazione alla consultazione pubblica di una platea alquanto eterogena di operatori dei settori della ricerca e della sanità (che spazia dai comitati etici, alle industrie farmaceutiche, agli enti di ricerca, ai coordinamenti di responsabili della protezione dei dati). In linea generale, i contributi pervenuti hanno evidenziato una certa difficoltà degli operatori di settore a orientarsi nel rinnovato quadro normativo di riferimento, soprattutto in relazione al rapporto tra il RGPD e la disciplina sulla sperimentazione clinica dei medicinali per uso umano contenuta nel regolamento (UE) 536/2014; ciò nonostante l'adozione da parte del Cepd di un primo provvedimento relativo alle domande e risposte sull'interazione tra i due testi normativi (cfr. parere 3/2019 del 23 gennaio 2019).

5

I principali dubbi interpretativi hanno riguardato l'uso ed il valore giuridico del consenso per il trattamento di dati genetici e dei dati relativi alla salute per scopi di ricerca medica, biomedica ed epidemiologica quale idoneo presupposto di liceità dei suddetti trattamenti.

L'Autorità ha preso atto e tenuto in considerazione tutti i contributi ricevuti, procedendo con una modifica e un aggiornamento del menzionato provvedimento prescrittivo del 5 giugno 2019 che, come è noto, ha natura transitoria, in attesa del provvedimento contenente le misure di garanzia di cui all'art. 2-*septies* del Codice (art. 21, comma 4, d.lgs. n. 101/2018).

Su tali basi, in primo luogo, nel preambolo del provvedimento, si precisa che l'art. 9, parr. 2 e 4, del RGPD individua i presupposti per il trattamento dei dati personali relativi, tra l'altro, alla salute degli interessati e ai dati genetici, consentendo agli Stati membri di introdurre, in riferimento a tali dati, ulteriori condizioni, comprese limitazioni; facoltà, questa, esercitata anche attraverso le richiamate prescrizioni. Più in dettaglio, nell'all. n. 4 al richiamato provvedimento del 5 giugno 2019, recante le prescrizioni per il trattamento dei dati genetici, è stata confermata la definizione di "dato genetico" secondo quanto previsto nel RGPD (art. 4, par. 1, n. 13).

Il provvedimento riporta, inoltre, le prescrizioni relative alla consulenza genetica e all'attività di informazione, attesa l'indispensabilità di assicurare l'effettiva autodeterminazione informativa degli interessati e tutelarne la dignità, anche alla luce dei principi di diritto internazionale e etici che informano l'uso dei dati genetici. Inoltre è stato prescritto ai medici di medicina generale e ai pediatri di libera scelta di indicare, nelle informative da rendere agli interessati ai sensi degli artt. 13 e 14 del RGPD e ai sensi degli artt. 77 e 78 del Codice: a) i risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici; b) la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale utilizzo di tali dati per ulteriori scopi. Dopo il raggiungimento della maggiore età, le informazioni sul trattamento di dati personali devono essere fornite all'interessato anche ai fini dell'acquisizione di una nuova manifestazione del consenso (cons. 38, 58, e artt. 5 e 8 del RGPD nonché art. 82, comma 4, del Codice; cfr. punti 4.3. e 4.4).

Nel provvedimento, quale ulteriore misura a tutela dei diritti degli interessati per il trattamento dei dati genetici, è prescritta la manifestazione del consenso da parte dell'interessato per: a) finalità di tutela della salute di un soggetto terzo (cfr. punto 4.7); b) lo svolgimento di test genetici nell'ambito delle investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria, salvo che un'espressa disposizione di legge, o un provvedimento dell'Autorità giudiziaria in conformità alla legge, disponga altrimenti (cfr. punto 4.9); c) i trattamenti effettuati mediante test genetici, compreso lo *screening*, a fini di ricerca o di ricongiungimento familiare. In questi casi, all'interessato è richiesto di dichiarare se vuole conoscere o meno i risultati dell'esame o della ricerca, comprese eventuali notizie inattese che lo riguardano, qualora queste ultime rappresentino per lo stesso un beneficio concreto e diretto in termini di terapia o di prevenzione o di consapevolezza delle scelte riproduttive (cfr. punto 4.10); d) finalità di ricerca scientifica e statistica non previste dalla legge o da altro requisito di cui all'art. 9 del RGPD (cfr. punto 4.11).

Tenuto conto che anche in queste ipotesi il consenso non perde la sua caratteristica di revocabilità, nel provvedimento si è precisato che, salva diversa disposizione di legge, in caso di revoca del consenso da parte dell'interessato, i trattamenti debbano cessare e i dati debbano essere resi anonimi, anche attraverso la distruzione del

campione biologico prelevato (cfr. punto 5.4.1; artt. 7, comma 3 e 89 del RGPD).

Il provvedimento indica inoltre specifiche prescrizioni concernenti il trattamento di dati genetici per finalità di ricerca scientifica e statistica nel caso di impossibilità ad acquisire il consenso per la conservazione e l'ulteriore utilizzo di campioni biologici e di dati genetici raccolti per la realizzazione di progetti di ricerca e indagini statistiche non direttamente collegati a quelli originari (cfr. punto 4.11.3).

In ogni caso, è previsto che i progetti di ricerca debbano essere conservati in forma riservata (essendo la consultazione del progetto possibile ai soli fini dell'applicazione della normativa in materia di dati personali) per cinque anni dalla conclusione programmata della ricerca, ciò anche in conformità a quanto previsto all'art. 3, comma 3 delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, d.lgs. 10 agosto 2018, n. 101 (provv. 19 dicembre 2018, n. 515, doc. web n. 9069637). Fermo restando, alla luce dei principi di responsabilizzazione nonché di *privacy by design* e di *privacy by default*, l'obbligo per i titolari di mettere in atto, sin dalla progettazione, misure tecniche e organizzative adeguate a garantire l'effettività dei principi applicabili al trattamento, anche in ragione delle diverse variabili che caratterizzano il contesto del trattamento.

Il provvedimento conferma, infine, la vigenza di specifiche prescrizioni in ordine alla custodia e alla sicurezza dei dati genetici e dei campioni biologici (cfr. punto 4.2; artt. 5, 24, 25 e 23 del RGPD).

L'allegato n. 5 al richiamato provvedimento 5 giugno 2019 individua, invece, le prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica in campo medico, biomedico ed epidemiologico di cui all'art. 110 del Codice. Le prescrizioni specificano quali sono le ipotesi in cui si ritiene che un titolare del trattamento non sia nelle condizioni di informare adeguatamente e acquisire il consenso degli interessati (cfr. punto 5.3). Tali circostanze devono essere esplicitate nell'eventuale richiesta di consultazione preventiva all'Autorità, anche nell'ambito della valutazione d'impatto (artt. 5, par. 2, 24 e 35 del RGPD). Sono state poi formulate specifiche prescrizioni in ordine alle modalità di trattamento dei dati ai quali, in omaggio al principio di minimizzazione, dovranno essere applicate tecniche di cifratura o di pseudonimizzazione ritenute adeguate in relazione al contesto di trattamento, anche nella fase di conservazione dei dati. A tale riguardo, in coerenza con il principio di responsabilizzazione, deve essere motivata per iscritto l'associazione al materiale di ricerca dei dati identificativi dell'interessato, sempre che sia temporanea ed essenziale per il risultato della ricerca (cfr. punti 5.4 e 5.6).

Nel provvedimento è precisato, inoltre, che il trattamento di dati personali per scopi di ricerca scientifica in campo medico, biomedico o epidemiologico può riguardare i dati relativi alla salute degli interessati e, solo ove indispensabili per il raggiungimento delle finalità della ricerca, anche i dati relativi alla vita sessuale o all'orientamento sessuale, nonché all'origine razziale ed etnica (art. 5, par. 1, lett. *c*), del RGPD).

Il provvedimento si conclude prescrivendo specifici accorgimenti tecnici volti a garantire un elevato livello di sicurezza e qualità dei dati in ciascuna fase del trattamento, fino alla loro anonimizzazione, alla quale dovrà procedersi allo scadere del tempo di conservazione dei dati previsto nel progetto di ricerca (cfr. punti 5.6 e 5.7). In tale ambito è stata suggerita, a titolo esemplificativo, l'applicazione parziale o integrale di tecnologie crittografiche a *file system* o *database*, oppure l'adozione di altre misure che rendano inintelligibili i dati ai soggetti non legittimati; è stato prescritto l'uso di canali di trasmissione protetti nella comunicazione dei dati e, laddove detta trasmissione sia effettuata mediante supporto ottico (cd-rom), l'obbligo

5

di designare uno specifico incaricato della ricezione presso il promotore come pure l'obbligo di utilizzare, per la condivisione della chiave di cifratura dei dati, un canale di trasmissione differente da quello utilizzato per la trasmissione del contenuto (cfr. punto 5.7).

5.5.2. Parere in ordine al trattamento dei dati personali, anche inerenti a particolari categorie di dati, per finalità di ricerca medica, biomedica e epidemiologica

Il Garante, con provvedimento 20 giugno 2019, n. 140 (doc. web n. 9123447), adottato ai sensi degli artt. 110 del Codice e 36 del RGPD, ha espresso parere favorevole in ordine al trattamento dei dati personali, anche inerenti a particolari categorie di dati, per finalità di ricerca medica, biomedica ed epidemiologica, riferiti alla coorte di pazienti arruolati nello studio denominato MATTERHORN (studio retrospettivo volto ad approfondire la conoscenza medico-scientifica relativa al microcitoma polmonare attraverso l'analisi di campioni di tessuto prelevati in passato e archiviati presso i sei centri partecipanti al progetto di ricerca). Il parere fa seguito a una istanza di consultazione preventiva presentata, ai sensi dell'art. 110, comma 1, ultimo capoverso, del Codice, da una società biofarmaceutica, titolare del trattamento, in qualità di *sponsor* e promotore del richiamato studio, in ragione del fatto che esso ha ad oggetto il trattamento anche di particolari categorie di dati riferiti, oltre che a soggetti in vita, a defunti.

Il quadro normativo di riferimento in materia di trattamento di dati personali per la ricerca medica, biomedica e epidemiologica, dispone che "il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento".

Su tali basi, il titolare nel trattamento ha trasmesso al Garante, unitamente all'istanza di consultazione preventiva, i pareri favorevoli dei competenti comitati etici a livello territoriale – che integrano le condizioni di liceità del trattamento quando non è possibile acquisire il consenso degli interessati – e la valutazione di impatto redatta ai sensi dell'art. 35 del RGPD, nella quale la società istante ha dato evidenza delle misure appropriate per tutelare i diritti e le libertà degli interessati coinvolti nel progetto di ricerca, della designazione, quale responsabile del trattamento dei dati, di altra società con sede a Dublino, incaricata di supportare il titolare del trattamento ai fini dello studio in qualità di CRO (*Clinical Reasearch Organization*) e del fatto che i dati pseudonimizzati verranno comunicati dalla CRO al proprio dipartimento medico, con sede a Chicago, sulla base di uno specifico *data transfer agreement* che consente detto trasferimento, ai sensi dell'art. 46, par. 2, lett. *c*), del RGPD.

6 La statistica

Nel corso dell'anno sono proseguite le interlocuzioni, anche informali, con l'Istituto nazionale di statistica finalizzate alla formulazione dei pareri di competenza relativi, ai lavori statistici necessari per la realizzazione del censimento permanente e sullo schema di Programma statistico nazionale 2017-2019, aggiornamento 2019 (Psn).

I principali temi oggetto di confronto hanno riguardato l'adeguamento dell'attività statistica sia al rinnovato quadro normativo, sia alla specifica disciplina di settore di cui all'art. 6-*bis*, comma 1-*bis*, d.lgs. n. 322/1989, inserito dall'art. 9, comma 6-*bis*, lett. *c*), d.l. 28 gennaio 2019, n. 4, convertito, con modificazioni, dalla l. 28 marzo 2019, n. 26; disposizione secondo la quale "per i trattamenti di dati personali, compresi quelli di cui all'articolo 9 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, effettuati per fini statistici di interesse pubblico rilevante ai sensi dell'art. 2-*sexies*, comma 2, lett. *cc*), del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, in conformità all'articolo 108 del medesimo codice, nel programma statistico nazionale sono specificati i tipi di dati, le operazioni eseguibili e le misure adottate per tutelare i diritti fondamentali e le libertà degli interessati, qualora non siano individuati da una disposizione di legge o di regolamento. Il programma statistico nazionale, adottato sentito il Garante per la protezione dei dati personali, indica le misure tecniche e organizzative idonee a garantire la liceità e la correttezza del trattamento, con particolare riguardo al principio di minimizzazione dei dati, e, per ciascun trattamento, le modalità, le categorie dei soggetti interessati, le finalità perseguite, le fonti utilizzate, le principali variabili acquisite, i tempi di conservazione e le categorie dei soggetti destinatari dei dati. Per i trattamenti dei dati personali di cui all'articolo 10 del citato regolamento (UE) 2016/679 effettuati per fini statistici di interesse pubblico rilevante ai sensi del citato articolo 2-*sexies*, comma 2, lettera *cc*), del codice di cui al decreto legislativo n. 196 del 2003 trova applicazione l'articolo 2-*octies* del medesimo codice".

Con specifico riferimento all'adeguamento al RGPD, si segnala che, nell'ambito delle interlocuzioni informali con l'Istituto, sono state fornite talune indicazioni per assicurare che, nello svolgimento dell'attività di rilevante interesse pubblico perseguita dall'Istat, sia assicurata un'effettiva applicazione dei principi di protezione dei dati, con particolare riferimento, in questa preliminare fase, al principio di minimizzazione dei dati al fine di garantire un elevato livello di tutela ai diritti e alle libertà fondamentali degli interessati.

6.1. *Parere sull'indagine europea sulla salute (European Health Interview Survey – EHIS IST-02565)*

Il Garante, con provvedimento 11 aprile 2019, n. 94 (doc. web n. 9113830), nel fornire il parere di competenza previsto dall'art. 36, par. 4, del RGPD e

6

dall'art. 6-*bis*, comma 1-*bis*, del richiamato d.lgs. n. 322/1989, concernente il prospetto identificativo del lavoro statistico IST-02565-Indagine europea sulla salute (*European Health Interview Survey* - EHIS), ha autorizzato l'Istat, ai sensi dell'art. 58, par. 3, lett. *c*), del RGPD e dell'art. 2-*quinquiesdecies* del Codice, ad avviare i trattamenti di dati personali connessi al predetto lavoro statistico, nel rispetto di specifiche misure e condizioni.

L'indagine in esame e i connessi trattamenti erano stati sospesi con parere 9 maggio 2018, n. 271, (doc. web n. 9001732) relativo allo schema di Programma statistico nazionale 2017-2019, aggiornamento 2018-2019, in quanto erano state rilevate specifiche criticità riguardanti, principalmente, il trattamento di dati personali sulla salute riferiti a interessati minori, anche giovanissimi (di età compresa tra i 2 e 15 anni), chiamati a rispondere, talvolta anche obbligatoriamente, a numerosi quesiti volti a raccogliere dati relativi ad aspetti molto delicati della vita quotidiana, idonei a creare situazioni di forte disagio e imbarazzo (ad es. in relazione alle difficoltà nelle attività quotidiane, quali la cura della persona, le attività domestiche, la contraccezione e la vita sessuale; i determinanti della salute, quali l'abitudine al fumo, i problemi di peso, l'attività fisica, il consumo di alcol, il consumo di frutta e verdura e la storia migratoria).

L'Istat ha così sottoposto all'Autorità, per il parere di competenza, il lavoro statistico in esame, rivisto alla luce dei rilievi formulati nel parere sul Psn (relativi in particolare a: condizioni di liceità del trattamento; obbligo di risposta; integrazione dei dati raccolti con altre fonti informative; tempi e modalità di conservazione; informazioni agli interessati; quesiti di natura sensibile) unitamente alla documentazione recante l'illustrazione delle garanzie messe in atto per attuare i principi della protezione dei dati sanciti dal RGPD e la valutazione d'impatto sulla protezione dei dati.

Il Garante, esaminata la documentazione trasmessa dall'Istituto, ha, in primo luogo, evidenziato la necessità di integrare il prospetto identificativo del lavoro statistico con tutti gli elementi previsti dal rinnovato quadro normativo. In secondo luogo, ha verificato la sussistenza delle condizioni di liceità dei trattamenti, evidenziando come essi siano svolti dall'Istat sia in adempimento di un obbligo legale, sia per l'esecuzione di un compito di interesse pubblico sulla base del diritto dell'Unione e della normativa nazionale (artt. 6, par. 1, lett. *c*) ed *e*) e art. 9, par. 2, lett. *g*), del RGPD; artt. 2-*sexies* e 106 del Codice e 4-*bis* delle regole deontologiche; d.lgs. 6 settembre 1989, n. 322), essendo la citata indagine prevista, a livello nazionale, anche dal regolamento (UE) 2018/255 della Commissione, del 19 febbraio 2018, che ha attuato il regolamento (CE) n. 1338/2008. Si è inoltre preso atto che l'Istituto aveva eliminato l'obbligo di risposta, dandone evidenza anche nei singoli questionari da sottoporre ai rispondenti, ed escluso ogni forma di integrazione dei dati raccolti nell'ambito dell'indagine EHIS con ulteriori fonti informative.

L'Autorità ha quindi prescritto all'Istat di ridurre il periodo di conservazione degli identificativi diretti dei rispondenti, da 36 a 24 mesi, in quanto dalla documentazione trasmessa non era emersa alcuna indicazione circa la necessità e la proporzionalità del tempo di conservazione indicato rispetto alla finalità perseguita. In relazione, invece, all'ulteriore periodo di conservazione, l'Autorità, tenuto conto che l'Istituto non ha fornito sufficienti indicazioni in ordine alla proporzionalità del termine (10 anni di conservazione) e della sussistenza di un, seppur basso, rischio di reidentificazione degli interessati, ha prescritto all'Istituto di adottare tecniche di cifratura delle particolari categorie di dati raccolti affinché

6

essi possano risultare intellegibili solo a soggetti autorizzati. Ciò anche in ossequio alle specifiche garanzie relative al trattamento dei dati a fini statistici previste dall'art. 89 del RGPD, che impone ai titolari del trattamento di attuare misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato.

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

7.1. *I trattamenti in ambito giudiziario*

Notifiche di atti giudiziari

Con riferimento ad alcune segnalazioni e reclami con cui si lamentava la notifica di atti giudiziari con l'indicazione di dati ritenuti eccedenti e non pertinenti, si è rappresentato che, trattandosi di atti inerenti al giudizio, la loro valutazione spetta al giudice adito ai sensi dell'art. 160-*bis* del Codice.

In un caso, in particolare, era stata lamentata la possibile illegittimità nella notifica, avvenuta per pubblici proclami ed effettuata anche tramite il sito web di un tribunale, del decreto di fissazione di udienza preliminare, della richiesta di rinvio a giudizio e dell'elenco delle persone offese relativamente ad un procedimento penale, soprattutto rispetto alle persone offese che non avevano sporto querela. L'Ufficio ha rilevato che, trattandosi di dati inerenti al giudizio, l'Autorità non è competente a valutare l'eventuale illiceità del trattamento oggetto di segnalazione; il legislatore stesso, infatti, assicurando un equo bilanciamento tra contrapposte esigenze di pari rango costituzionale, ha previsto i requisiti in presenza dei quali il giudice può procedere attraverso le notificazioni per pubblici annunzi alle persone offese (art. 155 c.p.p.) (nota 18 marzo 2019).

In un altro caso, concernente l'invio di una notifica tramite Pec contenente dati personali e giudiziari presso il luogo di lavoro, non si sono ravvisati elementi tali da configurare una violazione della normativa sui dati personali, dal momento che la comunicazione via Pec era stata inviata unicamente al fine di garantire l'esercizio e la difesa in sede giudiziaria delle ragioni del proprio assistito e conteneva solo i dati necessari per individuare la procedura esecutiva, dati adeguati e pertinenti nel rispetto dell'art. 5 del RGPD (nota 4 dicembre 2019).

Produzione di dati in giudizio

Diversi reclami hanno riguardato la legittimità della produzione di dati personali in giudizio. Secondo un consolidato orientamento, l'Ufficio ha precisato che spetta al Giudice, ove ritualmente richiesto, 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 conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali" (si vedano i conformi 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:* provv. 23 settembre 2010, doc. web n. 1756065; provv. 4 novembre 2010, doc. web n. 1770943; provv. 17 novembre 2010, doc. web n. 1779765).

In un reclamo si è lamentata la produzione in giudizio da parte dell'avvocato di controparte di dati relativi alla salute dell'interessata non corrispondenti al vero. In conformità all'art. 160-*bis* del Codice, si è innanzitutto ribadita l'incompetenza del Garante a valutare l'eventuale illiceità del trattamento consistito nella produzione in giudizio di dati riferibili all'interessata. In ordine, invece, alla supposta acquisizione illecita di dati riferiti alla salute dell'interessata, si è rappresentato che l'art. 9, par. 2, lett. *f*), del RGPD, sancisce che il divieto del trattamento di dati personali relativi alla salute della persona, di cui al par. 1 del medesimo articolo, non si applica se "il

trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria". Il procedimento è stato quindi archiviato, anche in considerazione del fatto che dalla documentazione acquisita è risultato che l'avvocato aveva esclusivamente dedotto un determinato stato di salute dell'interessata, non sussistendo gli elementi per ritenere che il professionista avesse acquisito dati relativi alla salute della reclamante né che terzi glieli avessero illegittimamente trasmessi (nota 14 marzo 2019).

In un altro caso una delle parti in un giudizio pendente ha lamentato la produzione nel corso dello stesso, da parte del legale dell'ex coniuge, anch'egli parte del predetto giudizio, di documenti inerenti alla separazione giudiziale e contenenti dati personali relativi al reclamante. Tali documenti, sarebbero stati ininfluenti ai fini del giudizio *de quo*, concernente la restituzione di somme di denaro alle parti attrici, genitori della parte reclamante. Anche questo reclamo, per le indicate ragioni, è stato archiviato.

Mancata ostensione di atti di un giudizio dinanzi alla Corte EDU

Mediante un reclamo un'interessata ha lamentato la mancata ostensione da parte dell'avvocato delle sorelle e della madre defunta di atti relativi ad un procedimento dinanzi alla Corte EDU; l'interessata ha altresì evidenziato il legittimo interesse a conoscere tali atti, nella parte riferibile alla madre, anche al fine di una richiesta di intervento nella procedura dinanzi la Corte EDU in qualità di erede. Secondo il professionista, la richiesta della reclamante si porrebbe invece in frontale contrasto col dovere, oltre che diritto primario e fondamentale dell'avvocato, di mantenere il segreto e il massimo riserbo sull'attività prestata stabilito dall'art. 28 del vigente Codice deontologico forense. A giudizio dell'Autorità, gli atti oggetto della menzionata richiesta avevano natura giudiziaria, considerato che l'interessata aveva chiesto di conoscere "copia del ricorso e o dei ricorsi" presentati innanzi alla Corte EDU e di avere informazioni relative allo stato attuale di tale procedura, anche in relazione alla copia della "raccomandazione" attraverso la quale la Corte sarebbe intervenuta presso lo Stato italiano per sollecitare una definizione di tale contenzioso. Come è noto, nell'ordinamento nazionale la conoscenza di un atto giudiziario è sottoposta a precise regole contenute nelle pertinenti disposizioni processuali, anche alla luce delle più generali esigenze inerenti al diritto alla difesa e alla libera determinazione della condotta processuale (art. 24 Cost.), esigenze che sono peraltro riconosciute anche dall'ordinamento sovranazionale (art. 6 della Convenzione EDU del 4 novembre 1950 e art. 47 della CDFUE del 7 dicembre 2000). Ne discende il diritto-dovere al segreto professionale da parte del legale che detiene atti giudiziari nell'ambito della sua attività professionale (art. 622 c.p., art. 200 c.p.p., art. 28 del Codice deontologico forense). Alla luce di tali considerazioni, si è rappresentato che l'interessata potrà rivolgersi direttamente all'Autorità giudiziaria competente, nella fattispecie la Corte EDU, deputata a valutare la sussistenza o meno di un interesse qualificato a conoscere gli atti giudiziari richiesti (nota 4 marzo 2019).

Procedura di sovraindebitamento presso un tribunale

L'Autorità si è occupata della protezione dei dati riferiti alle persone coinvolte nelle procedure di composizione delle crisi da sovraindebitamento presso i tribunali, disciplinata dalla legge 27 gennaio 2012, n. 3, secondo la quale, tra l'altro, il giudice stabilisce "idonea forma di pubblicità" relativamente ad alcuni atti della procedura, tra i quali la proposta di accordo o di piano del consumatore ed il provvedimento di omologazione dell'accordo e del piano del consumatore (cfr. artt. 10, comma 2, 12, comma 2 e 12-*bis*, comma 3, l. n. 3/2012).

Al riguardo il Garante ha segnalato al Csm e al Ministero della giustizia che in un reclamo era stata lamentata la pubblicazione in forma integrale sul sito web di un tribunale della relazione del professionista incaricato, che per legge viene allegata alla proposta di piano del consumatore (cfr. art. 9, comma 3-*bis*, l. n. 3/2012), riguardante la famiglia del reclamante e contenente dati quali il reddito della

7

stessa, la situazione economica, lo stato di difficoltà nonché i dati sensibili relativi allo stato di salute del fratello invalido. Più in dettaglio, ancorché il Garante non sia competente per il controllo dei trattamenti effettuati dall'Autorità giudiziaria nell'esercizio delle proprie funzioni (cfr. art. 154, comma 7, del Codice), purtuttavia, il RGPD trova applicazione anche ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado o presso il Ministero della giustizia, anche se per tali finalità sono previste alcune limitazioni in relazione ai diritti degli interessati ex art. 23, par. 1, lett. *f*), del RGPD, e art. 2-*duodecies* del Codice. Ai trattamenti effettuati per fini di giustizia sono comunque applicabili i principi generali in materia di trattamento dati, tra i quali, per quanto qui interessa, quello di minimizzazione dei dati, secondo il quale "i dati personali sono […] adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (cfr. art. 5, comma 1, lett. *c*), del RGPD). Orbene, nella fattispecie considerata, la segnalazione al Ministero ed al Csm è stata ritenuta necessaria in quanto la pubblicazione in forma integrale della relazione allegata alla proposta del consumatore ex art. 9, comma 3-*bis*, l. n. 3/2012 (facilmente raggiungibile da chiunque, digitando il cognome del reclamante su internet all'interno del motore di ricerca di Google) è apparsa in contrasto con l'art. 2-*septies*, comma 8, del Codice, in base al quale i dati relativi alla salute non possono essere diffusi, oltre che in violazione dei principi di proporzionalità e non eccedenza e minimizzazione dei dati, di cui all'art. 5 del RGPD, riconducibile agli artt. 8 CEDU e 8 CDFUE (nota 18 febbraio 2019).

In un reclamo è stato lamentato il mancato riscontro, da parte di un tribunale militare, all'istanza di cancellazione (a mezzo distruzione) di una serie di dati giudiziari contenuti in atti amministrativi, detenuti dal tribunale e relativi a trattamenti che il Garante, con provvedimenti del 2015, 2016 e 2017, aveva già dichiarato non conformi alla disciplina in materia di protezione dei dati personali. Tali provvedimenti avevano ritenuto esauriti gli effetti della condotta lamentata dall'interessato e, pertanto, non erano state adottate misure di cancellazione, di competenza del Collegio. Il reclamante non aveva impugnato tali statuizioni, prestando così acquiescenza anche sulla non adozione di misure di cancellazione. Di conseguenza la richiesta di cancellazione da ultimo presentata – che doveva essere semmai contenuta nell'impugnazione dei provvedimenti medesimi dinanzi l'Autorità giudiziaria – non è stata ritenuta valutabile, con conseguente archiviazione del procedimento (nota 18 dicembre 2019).

Improcedibilità ex art. 19, d.lgs. n. 101/2018

È stata esaminata una richiesta, non motivata, di informazioni in merito ad un'istruttoria su un reclamo presentato all'Autorità prima del 24 maggio 2018. Tenuto conto che, ai sensi dell'art. 19, comma 1, d.lgs. 10 agosto 2018, n. 101, i soggetti che hanno presentato reclami e/o segnalazioni prima del 24 maggio 2018 possono dichiarare il loro attuale interesse alla trattazione degli stessi mediante "motivata richiesta" al Garante entro il termine di sessanta giorni dalla data di pubblicazione in G.U. dell'avviso di cui all'art. 19, comma 3, d.lgs. n. 101/2018 (avviso che è stato pubblicato il 4 ottobre 2018, in G.U. n. 231/2018) e che, ai sensi dell'art. 19, comma 4, in caso di mancata presentazione di una richiesta di trattazione ai sensi del comma 1 "i relativi procedimenti di cui al comma 1 sono improcedibili", tale epilogo è stato rappresentato anche in relazione al procedimento in parola (nota 28 febbraio 2019).

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

Un'amministrazione provinciale ha posto un quesito in ordine alle richieste avanzate da parte di alcune Forze di polizia operanti sul territorio provinciale di accedere, per motivi di sicurezza, alla banca dati afferente al sistema di controllo del traffico veicolare per l'accertamento da remoto (in automatico) delle violazioni ai limiti di velocità e della mancanza di copertura assicurativa Rc-auto.

L'Ufficio ha ricordato che i trattamenti effettuati dalle Forze di polizia per le finalità istituzionali sono oggetto della direttiva (UE) 2016/680, recepita nell'ordinamento italiano con il decreto legislativo 18 maggio 2018, n. 51, in base al quale (artt. 3, comma 2, e art. 47, comma 1) la comunicazione di documentazione acquisita da un soggetto per finalità diverse da quelle cd. di polizia (come i dati personali raccolti ed elaborati per finalità amministrative concernenti l'accertamento delle violazioni dei limiti di velocità e della mancanza di copertura assicurativa Rc-auto) può avvenire legittimamente solo ove tale comunicazione sia conforme alle vigenti disposizioni legislative e regolamentari. Pertanto, l'accesso da parte delle Forze di polizia a dati personali acquisiti da altro titolare per il perseguimento delle finalità consentanee alle competenze istituzionali di quest'ultimo non può fondarsi sulla base di una generica ed indeterminata affermazione dell'esistenza di "motivi di sicurezza", in quanto occorre indicare la specifica finalità perseguita e la relativa base normativa (ovviamente nel rispetto delle esigenze connesse al segreto investigativo ed istruttorio). Ciò in quanto l'utilizzo per finalità di polizia di un dato acquisito ad altro fine da parte di una p.a. costituisce una forte interferenza con il diritto alla vita privata ed alla protezione dei dati personali degli interessati ed è ammissibile per quanto strettamente necessario in uno stato democratico sulla base di idonei presupposti normativi (cfr. artt. 8 CEDU e 7 e 8 CDFUE), sicché anche la normativa in parola deve rispettare i principi di necessità e proporzionalità.

Attività istruttorie sono in corso con riguardo alla diffusione, da parte di Forze di polizia, di dati e immagini di vittime di reati e di persone sottoposte a poteri coercitivi. Altre importanti istruttorie tuttora in corso riguardano i presupposti e le cautele da porre in essere per i collegamenti da parte di Forze di polizia a banche dati di pubbliche amministrazioni.

Della cooperazione con le autorità europee di protezione dati nel settore libertà, giustizia e affari interni si riferisce al par. 21.2.

7.3. *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.

È tuttora in corso l'attuazione delle raccomandazioni ricevute in esito alla valutazione sui trattamenti di dati personali effettuati in applicazione dell'*acquis* di Schengen svoltasi nel 2016.

Come noto, il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nel SIS II, in virtù dei quali l'interessato può rivol-

7

gersi 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, condividendo la raccomandazione formulata all'esito della precedente valutazione sull'applicazione dell'*acquis* di Schengen, il Ministero invia trimestralmente *report* statistici, privi di dati di natura personale, contenenti però 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. 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 nel regolamento (CE) n. 1987/2006 da parte degli interessati.

Nel corso del 2019, si è assistito ad un minimo incremento del numero delle richieste degli interessati indirizzate direttamente al Garante rispetto all'anno precedente; tra queste poi sono in lieve aumento 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 si continua ad assistere ad un moderato ma costante aumento delle richieste di accesso da autorità nazionali di controllo di altri Stati, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane. Le relative informazioni vengono comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni di cui all'art. 62 della decisione 2007/533/GAI del Consiglio e all'art. 46 del regolamento (CE) n. 1987/2006.

8 L'attività giornalistica

8.1. *Premessa*

L'attività dell'Autorità, con riguardo ai profili attinenti alla tematica della libertà di manifestazione del pensiero, è stata particolarmente intensa sia in termini di produzione di provvedimenti che di riflessioni avviate in ordine al delicato tema del bilanciamento di detta libertà con i diritti degli interessati. Tale ultimo aspetto ha costituito un momento preponderante dell'attività del Garante in questo settore nel quale la trattazione dei numerosi reclami pervenuti ha rappresentato l'occasione per enunciare importanti principi, anche alla luce dei nuovi criteri derivanti dall'applicazione delle disposizioni contenute nel RGPD. Ciò, in particolare, è avvenuto con riguardo agli artt. 17 e 21 che, in parte, hanno rideterminato i parametri di bilanciamento ponendo, in alcuni casi, una sorta di vantaggio preventivo a favore dell'interessato (cfr. par. 8.5).

Delle peculiarità insite nell'ambito del trattamento di dati per fini giornalistici è apparso consapevole anche il legislatore europeo che ha, infatti, rimesso agli Stati membri l'introduzione nei rispettivi ordinamenti nazionali di eventuali correttivi alle disposizioni del RGPD al fine di contemperare la regolazione ivi contenuta, valida nei confronti della generalità dei trattamenti, con le peculiarità riconosciute a questo ambito (cfr. art. 85).

Il legislatore italiano ha ritenuto di attuare questa prerogativa mantenendo nella disciplina nazionale, seppur con alcune integrazioni, le deroghe già previste dalla disciplina previgente (cfr. artt. 136-139 del Codice). Si segnala la facoltà di trattare dati riconducibili alle categorie particolari previste dagli artt. 9 e 10 del RGPD, quali i dati riguardanti la sfera sanitaria, sessuale e giudiziaria, a condizione del rispetto delle regole deontologiche, oltreché l'esplicita introduzione del regime sanzionatorio anche con riguardo a questa tipologia di trattamenti. Quest'ultimo profilo ha richiesto tuttavia, in virtù della copertura costituzionale garantita ai diritti coinvolti, un'attenta valutazione dei presupposti al ricorrere dei quali ritenere applicabili dette misure.

8.2. *Dati statistici ed aspetti procedurali*

Il reclamo, come detto, ha rappresentato nel corso del 2019 lo strumento di elezione utilizzato dagli interessati per rivolgersi all'Autorità esercitando uno dei diritti disciplinati dagli artt. 15-22 del RGPD, in particolare quelli di opposizione all'ulteriore trattamento e di cancellazione. Una parte considerevole delle richieste pervenute sono state definite mediante note istruttorie con le quali è stata comunicata alle parti la conclusione del procedimento a seguito dell'avvenuta adesione del titolare del trattamento ovvero l'insussistenza dei presupposti per procedere. Un quarto dei casi è stato invece concluso con l'adozione di provvedimenti adottati dal Garante tramite i quali sono state per lo più disposte misure correttive nei confronti dei titolari del trattamento.

Le doglianze presentate dagli interessati hanno riguardato, in larga parte: a) l'av-

venuta pubblicazione di dati ritenuti eccedenti da parte degli editori di testate giornalistiche e la successiva diffusione degli stessi quale effetto dell'indicizzazione degli articoli effettuata tramite motori di ricerca esterni ai rispettivi siti; b) la pubblicazione sui *social network* di dati personali in assenza del consenso dell'interessato o di altre basi giuridiche idonee a fondare la liceità del trattamento posto in essere; c) la perdurante reperibilità, tramite motori di ricerca, di risultati associati al nominativo di una determinata persona, la conoscibilità dei quali, in virtù del tempo trascorso, del ruolo ricoperto e di altri parametri utilizzati con riguardo a questa tipologia di trattamenti, è stata ritenuta non più rispondente alla situazione attuale della medesima ed al conseguente interesse del pubblico a disporre delle relative informazioni.

Non di rado l'attività istruttoria ha evidenziato carenze sul piano delle informative da rendere agli utenti dei siti ai sensi degli artt. 13 e ss. del RGPD.

È proseguita, come nel passato, la valutazione delle segnalazioni pervenute, pari a circa la metà dei reclami presentati; alcune di esse hanno fornito spunti interessanti per l'avvio di riflessioni su tematiche coinvolgenti diversi settori di attività del Garante.

Il settore dei trattamenti in ambito giornalistico, benché conservi una sua specificità, è stato ovviamente interessato dalle novità procedimentali introdotte con i nuovi regolamenti interni (cfr. par. 1) e ciò è valso, in particolare, con riguardo all'introduzione della fase costituita dalla comunicazione di avvio formale di procedimento da notificarsi al titolare del trattamento in tutti quei casi in cui, sulla base dell'istruttoria svolta, sia ravvisabile un *fumus* di violazione tale da richiedere un approfondimento in vista dell'eventuale adozione di un provvedimento correttivo e/o, se del caso, di tipo sanzionatorio. Ciò ha richiesto la necessità di avviare una riflessione in ordine alle circostanze alle quali dare maggior peso in questi casi, tenuto conto degli effetti che potrebbero derivare sulla libertà di informazione da un uso non equilibrato di questo nuovo potere, pur non potendosi perdere di vista il ruolo di garanzia dei diritti fondamentali della persona riconosciuto alle autorità di protezione dati.

Le regole deontologiche

In una prospettiva di adeguamento al nuovo quadro normativo europeo, ed in attuazione di quanto espressamente previsto dal decreto legislativo 10 agosto 2018, n. 101, il 4 gennaio 2019 sono state pubblicate in G.U. le "Regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica", tramite le quali si è provveduto ad individuare le disposizioni del preesistente "Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica" ritenute compatibili con il RGPD, aggiornando, nel contempo, i richiami ad atti normativi presenti all'interno di esso. Le disposizioni contenute nel testo indicato costituiscono condizioni essenziali di liceità del trattamento dei dati personali in ambito giornalistico (art. 2-*quater* del Codice) e conserveranno la loro efficacia sino a che non sarà posta in essere la revisione delle stesse in collaborazione con il Consiglio nazionale dell'Ordine dei giornalisti, secondo quanto previsto dagli artt. 2-*quater* e 139 del Codice.

Alla luce del rinnovato quadro normativo, si è tenuto un incontro tra il Garante e il Presidente del Consiglio nazionale dell'Ordine dei giornalisti, all'esito del quale si è rinnovato il richiamo ai mezzi di informazione affinché rispettino le regole alla base della professione giornalistica e i provvedimenti adottati dall'Autorità, anche in ragione del nuovo quadro sanzionatorio. In tale circostanza è stata condivisa l'urgenza di tornare a sensibilizzare i *media* sul rispetto della dignità e delle libertà fondamentali delle persone, anche attraverso l'organizzazione in comune di attività formative su tali tematiche; verrà inoltre avviata una discussione volta ad individuare le modalità più opportune per trasmettere i provvedimenti adottati

dall'Autorità ai Consigli dell'Ordine in vista della valutazione dei fatti da parte degli stessi per i profili deontologici (v. comunicato stampa 6 novembre 2019, doc. web n. 9179762).

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

8.3.1. Dati giudiziari

L'Autorità è stata chiamata ad affrontare nuovamente il tema del trattamento di dati giudiziari da parte di testate giornalistiche e di siti web, oltreché da parte dei motori di ricerca (cfr. par. 8.5), attraverso l'individuazione dei principi di un corretto trattamento di questa particolare categoria di dati. Ciò in quanto, senza voler comprimere le esigenze informative connesse a notizie riguardanti rilevanti fatti di cronaca giudiziaria, si è avvertita con urgenza, in virtù di quanto emerso dall'esame dei casi sottoposti all'attenzione del Garante, l'esigenza di garantire con particolare incisività la tutela dei diritti delle persone coinvolte, sia che si tratti di vittime, sia che si tratti di persone sottoposte ad indagine per fatti di reato descritti all'interno degli articoli diffusi *online.*

Sono stati così ribaditi i limiti che gli editori incontrano con riguardo al trattamento di dati afferenti a vicende giudiziarie, tenendo anche conto del fatto che, pur essendo stata prevista dallo stesso RGPD la possibilità di introdurre, in ambito giornalistico, deroghe al regime generale, il legislatore nazionale ha comunque mantenuto un punto fermo vincolando il trattamento delle categorie particolari di dati di cui agli artt. 9 e 10 del RGPD al rispetto delle regole deontologiche di settore.

Il travalicamento dei criteri dettati da queste ultime è stato riscontrato con riguardo alla pubblicazione di immagini di persone coinvolte in fatti di cronaca giudiziaria riprese in condizioni di costrizione fisica o comunque in circostanze la cui diffusione è stata ritenuta lesiva della dignità delle medesime. Ciò è avvenuto, ad esempio, in occasione della riscontrata diffusione in rete di un video ritraente le reazioni autolesionistiche di un uomo, in evidente stato di alterazione psico-fisica, filmato all'interno dei locali di un commissariato di polizia: il Garante, rinvenendo nel trattamento così effettuato gli estremi di una violazione delle norme di riferimento (cfr. art. 137, comma 3, del Codice e art. 8, comma 1, delle regole deontologiche), ha adottato, in via d'urgenza, una serie di provvedimenti di limitazione provvisoria del trattamento, attraverso i quali è stata inibita ai titolari coinvolti l'ulteriore propagazione delle immagini con modalità tali da rendere identificabile la persona ripresa, tenuto anche conto delle esternazioni rese da quest'ultima all'interno del video in relazione al proprio stato di salute (*ex multis* provv. 25 marzo 2019, n. 73, doc. web n. 9114416). Ad analoga valutazione si è pervenuto a fronte dell'avvenuta diffusione, all'interno di siti web riconducibili a varie testate giornalistiche, di immagini, pubblicate a corredo dei corrispondenti articoli di stampa, ritraenti due persone che, poste in stato di fermo a seguito di un grave fatto di cronaca, sono state riprese in evidente stato di costrizione fisica (provv. 25 ottobre 2019, n. 198, doc. web n. 9199034; provv. 31 ottobre 2019, n. 199, doc. web n. 9199046). Anche in questo caso si è ritenuto, sulla base di una valutazione effettuata nell'immediatezza del fatto, che il trattamento dei dati riferiti agli individui coinvolti fosse avvenuto con modalità tali da risultare in contrasto con il principio di essenzialità dell'informazione e con quello di rispetto della dignità umana, oltreché con specifiche norme poste dall'ordinamento a tutela delle persone arrestate, quale l'art. 114, comma 6-*bis*, c.p.p. che espressamente vieta "la pubblicazione dell'immagine di persona privata della libertà personale ripresa mentre la stessa si trova sottoposta all'uso di

manette ai polsi ovvero ad altro mezzo di coercizione fisica, salvo che la persona vi consenta".

L'Autorità, al fine di richiamare il mondo dei *media* al rispetto delle norme vigenti in materia, ha accompagnato l'adozione dei provvedimenti sopra citati con appositi comunicati stampa (cfr. comunicato stampa 25 ottobre 2019, "Omicidio a Roma: i *media* rispettino il codice di procedura penale", doc. web n. 9170332) finalizzati, da un lato, a favorire un processo di adeguamento spontaneo anche da parte di eventuali ulteriori titolari del trattamento e, dall'altro, a richiamare, in generale, l'attenzione dei mezzi di informazione sull'importanza del rispetto di regole che costituiscono, prima di tutto, un baluardo di civiltà.

L'importanza attribuita al rispetto di determinati principi con riguardo al trattamento di questa categoria di dati è emersa anche nell'ambito di una decisione innovativa adottata dall'Autorità con il provvedimento del 27 novembre 2019, n. 213 (doc. web n. 9236677) che, seppure diretta in via immediata nei confronti del gestore di un motore di ricerca, ha preso le mosse dalla valutazione di una presumibile illiceità nel trattamento di dati giudiziari imputabile agli editori che avevano curato l'originaria pubblicazione di articoli oggetto di indicizzazione. Questi ultimi, infatti, contenevano, oltre alla descrizione della vicenda giudiziaria sottostante, immagini delle persone indagate che, per le modalità con cui erano state realizzate, apparivano riconducibili alla categoria delle foto segnaletiche, la cui diffusione ad opera delle Forze di polizia è sottoposta ad uno specifico vincolo di finalità. Ritenendo dubbia la liceità del trattamento effettuato *ab origine* dagli editori delle testate giornalistiche interessate, ha disposto, nelle more dello svolgimento di un accertamento da condurre nei confronti di questi ultimi, la limitazione provvisoria del trattamento effettuato dal gestore del motore di ricerca al fine di ridurre il pregiudizio subito dall'interessato in virtù della perdurante diffusione, in associazione al suo nominativo, delle immagini sopra descritte.

Su questo tema il Garante ha inoltre adottato un provvedimento a seguito di un reclamo con cui l'interessato ha chiesto la rimozione di articoli di stampa che riportavano la notizia del suo arresto quale presunto "responsabile di tentato furto archeologico e danneggiamento" di un sito archeologico, diffondendo i suoi dati anagrafici e riportando, altresì, la sua foto segnaletica; ritenendo che la pubblicazione di questa specifica immagine fosse illecita, in quanto non supportata da comprovate ragioni di giustizia e di polizia, né altrimenti giustificata in ragione di esigenze informative sulla vicenda, il reclamo è stato accolto (provv. 7 febbraio 2019, n. 38, doc. web n. 9101651).

Sempre in relazione agli effetti della indicizzazione in rete di notizie di cronaca giudiziaria, va menzionato un altro provvedimento del Garante con il quale è stato accolto il reclamo di un professionista che lamentava la reperibilità di un articolo recante il contenuto e la trascrizione di alcuni atti giudiziari relativi a procedimenti penali in tema di associazione mafiosa nei quali egli veniva menzionato, ma rispetto ai quali era estraneo. L'Autorità ha rilevato che, quand'anche la pubblicazione dell'articolo, risalente al 2013, fosse stata a suo tempo motivata da esigenze di cronaca rispetto alle risultanze dei procedimenti allora in corso, la sua persistente reperibilità in internet in associazione al nominativo del reclamante risultava idonea a fornire, alla luce delle attuali risultanze giudiziarie, un'informazione incompleta e non aggiornata a cominciare dallo stesso titolo dell'articolo; ciò alla luce del fatto che i procedimenti penali *de quibus* erano giunti ad una fase avanzata in cui i soggetti imputabili di reato erano stati individuati e tra questi non figurava il reclamante. Nell'ambito dell'istruttoria sono state altresì rilevate e sanzionate carenze del titolare del trattamento anche in ordine all'informativa da fornire agli utenti, con

particolare riferimento ai contatti attraverso i quali esercitare i diritti di cui agli artt. 15-22 del RGPD (provv. 11 dicembre 2019, n. 227, doc. web n. 9269868).

8.3.2. Dati relativi a minori

Il quadro normativo concernente la tutela dei minori fornisce parametri sufficientemente precisi. In particolare, il Codice (art. 50) e le allegate regole deontologiche (art. 7) documentano una scelta precisa dell'ordinamento volta ad accordare una specifica protezione alle informazioni riguardanti i minori e a privilegiare l'interesse di tali soggetti anche rispetto ad altri diritti e libertà fondamentali quali quelli tutelati dall'art. 21 Cost. Alla base di tale scelta c'è la consapevolezza che i minori risultano particolarmente esposti ai rischi legati alla diffusione non controllata dei dati che li riguardano: evento che, in molti casi, rischia di segnare profondamente il loro sviluppo, provocando danni ben più rilevanti di quelli che possono essere prodotti in una persona adulta. La *ratio* della disciplina sta dunque nel tutelare la personalità del minore coinvolto in fatti di vita – già di regola negativi – la cui pubblicizzazione su internet risulta per lo stesso (ulteriormente) pregiudizievole.

A tale riguardo si può richiamare un provvedimento relativo ad un reclamo con il quale due genitori hanno chiesto la rimozione di un articolo di stampa, diffuso anche mediante il sito internet di un quotidiano, che riportava le generalità, la fotografia e i dati sanitari riguardanti la figlia minore deceduta in ospedale a causa di una malattia. Il Garante ha ritenuto di accogliere la richiesta, vietando l'ulteriore diffusione delle generalità e delle immagini della medesima, considerando questi elementi eccedenti rispetto alle finalità informative dell'articolo, ossia quelle di dare conto di un'indagine svolta dalla Procura della Repubblica competente per l'accertamento delle responsabilità connesse alla morte di una bambina. Nel caso di specie, la tutela normalmente garantita alla dignità della persona malata, poi deceduta, è stata rafforzata dalla circostanza della minore età dell'interessata, interpretandosi perciò il parametro dell'interesse pubblico in modo particolarmente rigoroso anche a protezione della memoria della defunta e della serenità del suo nucleo familiare (provv. 4 aprile 2019, n. 90, doc. web n. 9113909).

8.3.3. Registrazioni audio e video

Nuove occasioni di riflessione sul tema dell'uso di strumenti di registrazione audio e video a fini giornalistici sono state fornite da alcuni reclami presentati all'Autorità nel periodo di riferimento. Si segnalano, in particolare, due decisioni con cui sono state dichiarate infondate le doglianze formulate in relazione alla identificabilità dei reclamanti, protagonisti di alcuni servizi televisivi aventi lo scopo di denunciare talune condotte irregolari, suscettibili di assumere anche rilevanza penale, tenute dagli stessi, nel contesto più generale di denuncia del fenomeno del lavoro nero e/o sommerso e delle assunzioni irregolari (provv. 24 ottobre 2019, n. 201, doc. web n. 9207828) nonché delle azioni di discriminazione e di contrasto all'integrazione sociale degli immigrati (provv. 20 giugno 2019, n. 141, doc. web n. 9123578).

8.4. *Diffusione di dati personali sui* social network

Numerosi reclami e segnalazioni hanno avuto ad oggetto la pubblicazione di dati personali (commenti, fotografie, ecc.) sui profili *social* e, in particolare, su Facebook, Instagram e YouTube. Le disposizioni che disciplinano tale materia sono, anche in questo caso, quelle di cui agli artt. 136 ss. del Codice dedicate a "Finalità gior-

nalistiche e altre manifestazioni del pensiero", in quanto tale ampia formulazione 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 in rete. Come nel caso della diffusione dei dati per finalità giornalistiche, non è richiesto pertanto il consenso dell'interessato, sempre che sussistano adeguate finalità di interesse pubblico, inteso come interesse della cerchia dei soggetti che hanno accesso alle informazioni pubblicate sui *social*. Anche in questi casi, perciò, il bilanciamento tra la libertà di manifestazione del pensiero e la tutela dei dati personali va effettuato caso per caso sulla base del tipo di diffusione sui *social media* e della natura dell'informazione di volta in volta immessa dall'interessato o, più frequentemente, da altri soggetti. I reclami e le segnalazioni hanno riguardato, nella maggior parte dei casi, le seguenti condotte:

- diffusione di foto di minori da parte di uno dei genitori separati: riguardo a tali reclami e segnalazioni relativi a *social network* si sono andati consolidando una serie di orientamenti in base ai quali il Garante ha chiesto di provvedere all'eliminazione delle foto di minori "postate" da uno dei due genitori separatati senza il consenso dell'altro;
- diffusione di foto presenti su profili Facebook chiusi e aperti: per i profili chiusi si ritiene che non si applichi la normativa sulla protezione dei dati, reputandosi il trattamento in questione effettuato per finalità personali e domestiche. Quanto ai profili aperti, l'eliminazione tende ad essere disposta per le foto e i video in cui il segnalante risulta essere riconoscibile, ove questi non abbia prestato il consenso;
- diffusione di foto sui *social* finalizzate a denunciare attività illecite (ad es., conferire in modo improprio la spazzatura; rendere noto un veicolo parcheggiato in un luogo non consentito): la relativa diffusione è stata ritenuta ammissibile a condizione che fossero riprese in luogo pubblico e che i soggetti fotografati non fossero riconoscibili;
- diffusione sui *social* di atti giudiziari: si è valutato caso per caso se i dati diffusi fossero tutti di interesse pubblico, chiedendo di eliminare i dati non essenziali (ad es., il numero di telefono degli interessati);
- diffusione sui *social* di profili *fake*: il Garante ha chiesto al titolare della pagina Facebook la rimozione degli stessi.

L'unico provvedimento adottato in materia ha riguardato un reclamo, presentato da un personaggio che riveste un ruolo pubblico, con il quale lo stesso ha lamentato la diffusione su Facebook e su altri *social network* di video che diffondevano l'indirizzo di residenza e le fotocopie degli assegni circolari con i quali aveva proceduto all'acquisto della sua abitazione. Il Garante ha ordinato l'eliminazione di questi video, posto che si trattava di dati privati che, in considerazione delle potenzialità diffusive proprie di internet e dei *social media*, mettevano a rischio l'incolumità dell'interessato e della sua famiglia (provv. 18 aprile 2019, n. 104, doc. web n. 9113894).

8.5. *Trattamento dei dati tramite i motori di ricerca*

Il settore dei reclami proposti nei confronti dei gestori di motori di ricerca è stato interessato da alcune importanti novità riguardanti le modalità di trattazione degli stessi. Avendo per lo più le caratteristiche di trattamenti definibili come transfrontalieri (cfr. art. 4, punto n. 23, del RGPD), le richieste avanzate nei confronti dei relativi titolari risultano tendenzialmente soggette all'applicazione della procedura

di cooperazione di cui agli artt. 56 ss. del RGPD che implica un coinvolgimento dell'autorità capofila (*Lead Supervisory Authority*, coincidente con l'autorità dello stato membro in cui il titolare del trattamento ha individuato il proprio stabilimento principale) e delle altre autorità di protezione dati interessate (*Concerned Supervisory Authority*).

La regola generale presenta, tuttavia, alcune eccezioni.

Google, gestore dell'omonimo motore di ricerca, nei primi mesi del 2019 ha dato, infatti, comunicazione alle autorità europee di aver mantenuto la gestione dei trattamenti effettuati in tale ambito presso la propria sede principale negli Stati Uniti; non essendo stato individuato uno stabilimento principale nel territorio dell'Unione europea, con riferimento ai trattamenti effettuati da tale società attraverso la gestione del motore di ricerca è pertanto venuto meno il presupposto di applicazione del meccanismo dello sportello unico (cd. *One Stop Shop*); di qui, il permanere in capo alle singole autorità di protezione dati della competenza a definire autonomamente i casi nazionali (che, nel caso del Garante, si è tradotto nell'adozione di circa 25 provvedimenti).

Diverso è stato invece l'approccio seguito con riguardo ad altre società, quali Microsoft Corporation e Verizon Media Emea Limited (già Oath Emea Limited) – rispettivamente titolari dei motori di ricerca Bing e Yahoo! – in virtù del fatto che tali società hanno invece ritenuto di avvalersi della facoltà riconosciuta dal RGPD di individuare uno stabilimento principale nel territorio dell'UE; ciò ha determinato l'applicabilità del meccanismo di cooperazione, pur restando salva la possibilità di proporre all'autorità capofila una definizione del reclamo a livello locale al ricorrere dei presupposti indicati dall'art. 56, par. 2, del RGPD.

Nel corso del 2019, tuttavia, si sono verificate le condizioni per l'attivazione di questa procedura in un solo caso, in quanto, in relazione alla maggior parte dei reclami proposti, i titolari del trattamento da ultimo indicati hanno mostrato un approccio particolarmente collaborativo già in sede di riscontro alla richiesta di informazioni preliminari inviata dall'Autorità, circostanza che ha portato a definire le relative vicende senza necessità di attivare una formale procedura di cooperazione. Nell'ambito, invece, delle procedure aperte da altre autorità europee di protezione dati, e inserite all'interno della piattaforma IMI (cfr. par. 21.1), si è provveduto, nella maggior parte dei casi, a manifestare l'interesse del Garante a prendere parte ad un processo di valutazione congiunta ritenendo utile l'esame delle relative questioni anche ai fini della definizione di vicende analoghe.

La specificità dei reclami proposti nel settore dei trattamenti effettuati mediante motori di ricerca – la definizione dei quali passa per l'individuazione di un punto di equilibrio tra l'interesse pubblico a disporre delle informazioni presenti in rete ed il diritto ad essere dimenticati rivendicato dagli interessati – ha registrato, con l'applicazione del RGPD, un elemento di cambiamento connesso alla nuova formulazione dell'art. 21 relativo al diritto di opposizione che, nei casi individuati nella norma, ha spostato a carico del titolare l'onere di provare la sussistenza di ragioni idonee a giustificare la prosecuzione del trattamento, agevolando l'accoglimento delle istanze di rimozione formulate dagli interessati.

Nell'ambito dei procedimenti trattati, l'Autorità ha avuto modo, da un lato, di confermare alcuni principi già affermati nella lunga esperienza anteriore all'ingresso del RGPD e, dall'altro, di intraprendere strade nuove anche attraverso l'ampliamento di riflessioni già avviate in precedenza. Ciò è quanto avvenuto, ad esempio, con riguardo alla definizione dei criteri cui ricorrere per chiedere al gestore di un motore di ricerca la rimozione di URL reperibili in rete in associazione ai dati identificativi degli interessati. Allo stato attuale tale criterio, secondo l'orientamento

8

emerso nella sentenza *Google Spain* (causa C-131/12) e confermato anche da successive pronunce della CGUE (Causa C-507/17 e C-136/17), coincide essenzialmente con il nome della persona interessata, ma, in taluni casi, la valenza identificativa insita in ulteriori termini utilizzabili in associazione al nome o finanche a prescindere da esso è stata ritenuta tale da determinare, in una valutazione complessiva della richiesta, un'estensione dei criteri presi a riferimento. È quanto avvenuto nel caso di un senatore della Repubblica italiana coinvolto, negli anni novanta, in una vicenda giudiziaria per la quale era stato condannato in primo grado, ma che si era successivamente conclusa con sentenza di assoluzione; il medesimo, ritenendosi pregiudicato dalla perdurante reperibilità in rete di informazioni non aggiornate, ha chiesto la rimozione dei corrispondenti risultati di ricerca indicizzati in associazione al proprio nominativo, includendovi altresì la parola "condannato". In questa circostanza l'Autorità (provv. 10 gennaio 2019, n. 10, doc. web n. 9090292) ha reputato opportuno dare seguito alla richiesta, anche mediante l'estensione a criteri di ricerca ulteriori rispetto al nome, in quanto la funzione ricoperta dall'interessato rendeva plausibile il fatto che detto criterio potesse essere impiegato dagli elettori per acquisire informazioni utili ai fini dell'esercizio del diritto di voto. La richiesta dell'interessato è stata poi accolta nel merito ritenendo che la circolazione in rete di informazioni non aggiornate, oltreché in contrasto con i principi di liceità del trattamento indicato nell'art. 5 del RGPD, risultando per lo stesso pregiudizievole, fosse altresì idonea ad incidere sulla corretta formazione delle opinioni dell'elettorato e sulle conseguenti scelte effettuate.

In un altro caso (provv. 20 giugno 2019, n. 144, doc. web n. 9124401) si è ritenuto di dare rilievo alle caratteristiche specifiche della vicenda sottoposta all'attenzione del Garante, riconoscendo il diritto all'oblio invocato dall'interessato con riguardo a risultati di ricerca reperibili tramite termini di ricerca che, pur diversi dal nome e cognome, erano da ritenersi idonei a consentire l'identificabilità, anche se in via indiretta, dell'interessato medesimo. La richiesta proveniva da un professionista che aveva richiesto invano a Google la deindicizzazione di un URL reperibile *online* digitando non il proprio nome, ma il riferimento alla sua qualifica di presidente di una società cooperativa. Quest'ultima informazione consentiva il collegamento ad una pagina contenente una notizia non aggiornata relativa ad un procedimento penale nel quale era stato coinvolto dieci anni prima, ma riguardo al quale era poi intervenuta una sentenza definitiva di assoluzione. La permanenza in rete della notizia rappresentava, ad avviso dell'interessato, un gravissimo e irreparabile pregiudizio alla propria reputazione. L'Autorità ha ritenuto, in tale specifica circostanza, di poter accogliere la richiesta del reclamante muovendo dalla definizione di "dato personale" contenuta nell'art. 4 del RGPD (e riferita a "qualsiasi informazione riguardante una persona fisica identificata o identificabile") e concludendo l'esame della vicenda nel senso che la qualifica menzionata all'interno dell'articolo si riferisse in maniera inequivocabile alla persona del reclamante, che rivestiva quella carica da moltissimi anni, tanto da essere ormai univocamente identificato con essa, specie nell'ambito della realtà di riferimento.

Larga parte delle doglianze presentate all'Autorità ha riguardato poi la perdurante reperibilità in rete di informazioni non aggiornate relative a vicende giudiziarie nelle quali sono stati coinvolti gli interessati proponenti il reclamo, conclusesi in modo per loro favorevole e/o comunque diverso rispetto a quanto rappresentato negli articoli contestati. La posizione assunta dal Garante ha portato, nella maggioranza dei casi, all'accoglimento delle richieste avanzate tenuto conto del fatto che, come affermato in più occasioni anche dalla CGUE, il gestore del motore di ricerca, in quanto titolare autonomo del trattamento consistente nell'indicizzazione di con-

tenuti pubblicati in rete da terzi, è tenuto al rispetto delle disposizioni dettate dalle norme in materia di protezione dei dati personali, tra le quali assume particolare rilievo quella riguardante i principi di liceità del trattamento (art. 5 del RGPD).

La necessità di garantire il rispetto di tali principi è avvertita, in questo settore, in modo particolare tenuto conto del fatto che l'aggregazione di dati provenienti da varie fonti consente agli utenti di disporre di una visione strutturata di informazioni riferite ad una determinata persona che, in assenza del motore di ricerca, non potrebbero essere connesse tra loro con la stessa facilità. Da qui l'importanza che il profilo che ne risulta veicoli informazioni esatte ed aggiornate su tale persona.

Questo aspetto è stato tenuto in considerazione, ad esempio, al fine di valutare positivamente la richiesta di un'interessata, avente un ruolo pubblico di rilievo, diretta ad ottenere la rimozione, dai risultati di ricerca reperibili in associazione al suo nominativo, di URL rinvianti ad articoli relativi ad un procedimento penale attivato a suo carico e conclusosi nei suoi confronti con la pronuncia di un decreto di archiviazione, circostanza della quale non si dava alcun conto all'interno di dette pagine. L'Autorità, ritenendo che la perdurante indicizzazione di tali informazioni fosse in contrasto con i principi di esattezza ed aggiornamento dei dati espressamente previsti dal RGPD (cfr. art. 5, par. 1, lett. *d*), ha accolto l'istanza disponendo la rimozione del collegamento con i contenuti pregiudizievoli (provv. 18 aprile 2019, n. 93, doc. web n. 9123997); la presenza di tali informazioni aveva peraltro determinato, quale ulteriore conseguenza a carico dell'interessata, l'associazione del suo nominativo con parole chiave aventi valenza negativa – quale "indagata" – nell'ambito della funzione di autocompletamento (cd. *autocomplete*), associazione poi corretta nel corso del procedimento dallo stesso titolare del trattamento.

Gli orientamenti dell'Autorità nell'ambito del trattamento di dati giudiziari si sono poi arricchiti di nuovi ed importanti parametri che tengono conto anche delle finalità riconosciute a determinati istituti previsti in ambito penale dall'ordinamento nazionale, come nel caso del beneficio della non menzione della condanna nel casellario giudiziale e dell'istituto della riabilitazione. Riguardo al primo profilo, ci sono stati diversi casi nei quali il Garante, nell'effettuare un bilanciamento tra l'interesse del pubblico a conoscere determinate informazioni ed il diritto di opposizione esercitato da un interessato coinvolto in un procedimento penale, ha dato rilievo alla posizione espressa da quest'ultimo riconoscendo, nel caso specifico, la sussistenza di una delle fattispecie cui la legge collega, quale effetto automatico dipendente dall'esiguità della pena inflitta, il beneficio della non menzione della condanna all'interno del certificato del casellario giudiziale richiesto dell'interessato medesimo (cfr. art. 24, d.P.R. 14 novembre 2002, n. 313, come modificato dal d.lgs. 2 ottobre 2018, n. 122, recante il "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"). Ciò che si è inteso valorizzare in questi casi (provv. 31 ottobre 2019, n. 203, doc. web n. 9207856) è la funzione riconosciuta dall'ordinamento a tale istituto che appare finalizzato a limitare la conoscibilità della condanna subita da un determinato soggetto: tale effetto verrebbe di fatto vanificato ove fosse consentito al gestore di un motore di ricerca l'ulteriore diffusione di dati giudiziari riferiti all'interessato (cfr. anche provv. 28 febbraio 2019, n. 50, doc. web n. 9103108).

Il tema della riabilitazione è stato invece esaminato in un provvedimento del 24 luglio 2019, n. 153 (doc. web n. 9136842) mediante il quale è stata accolta la richiesta di rimozione di alcuni URL reperibili in associazione al nominativo dell'interessato e riconducibili ad informazioni giudiziarie non più rappresentative della sua situazione attuale. Il procedimento nel quale era stato coinvolto l'interessato

8

si era infatti concluso nel 2010 con una sentenza di patteggiamento in relazione alla quale, circa tre anni dopo, lo stesso aveva ottenuto la riabilitazione, circostanza quest'ultima della quale non vi era alcuna traccia nelle pagine web indicate nell'atto di reclamo. La persistenza in rete di informazioni giudiziarie non aggiornate è stata giudicata in contrasto con i principi alla base dell'istituto della riabilitazione che, pur non estinguendo il reato, comporta il venir meno delle pene accessorie e di ogni altro effetto penale della condanna come misura premiale finalizzata al reinserimento sociale della persona (cfr. anche provv. 26 settembre 2019, n. 170, doc. web n. 9165117). Sono state sottoposte all'attenzione del Garante anche fattispecie nelle quali il tema della tutela dei dati personali si è in parte sovrapposta a questioni attinenti la violazione di diritti diversi facenti capo al medesimo individuo, quale quello alla reputazione, ed il cui accertamento spetta tendenzialmente all'Autorità giudiziaria ordinaria. Si sono registrati, tuttavia, casi nei quali non si è ravvisata la possibilità di operare una netta distinzione tra i due aspetti, se non a costo di negare tutela ai profili di protezione dati presenti. Ciò si è, ad esempio, verificato nell'ipotesi di richieste di rimozione di URL collegati a commenti negativi espressi all'interno di *forum* di utenti, per lo più non identificabili, nei quali veniva affermata l'esistenza di procedimenti penali pendenti a carico dell'interessato, informazione rivelatasi inesatta sulla base delle certificazioni prodotte dal medesimo nel corso del procedimento. Benché, in linea generale, l'Autorità non possa spingersi sino al punto di valutare la veridicità o meno di fatti o circostanze rappresentati all'interno di articoli di giornale o di commenti resi da terzi – trattandosi di aspetti non suscettibili di essere verificati in termini oggettivi – tuttavia, nei casi esaminati (provv. 24 gennaio 2019, n. 17, doc. web n. 9090795; provv. 26 settembre 2019, n. 175, doc. web n. 9168753), è emersa una sostanziale inesattezza dei dati ivi contenuti, tenuto conto del fatto che gli addebiti mossi alle persone interessate non risultavano comprovati dall'esistenza di procedimenti penali pendenti nei loro confronti o da condanne dagli stessi subite, come desumibile dalle certificazioni prodotte dai medesimi. L'ulteriore diffusione di tali informazioni non è stata pertanto ritenuta rispondente ad un interesse pubblico prevalente sul diritto all'oblio esercitato dall'interessato, né è stata altrimenti giustificata dal titolare del trattamento sul quale grava, ai sensi dell'art. 21 del RGPD, l'onere di dimostrare la sussistenza di motivi legittimi e cogenti per proseguire il trattamento.

L'Autorità ha invece riscontrato la presenza dei presupposti per la prosecuzione del trattamento, ritenendo quindi legittima la perdurante reperibilità in rete di informazioni relative ad una determinata persona, laddove il decorso di un lasso di tempo non significativo, unitamente alla gravità dei fatti addebitati all'interessato ed alla presenza in rete di informazioni aggiornate riguardo alla vicenda, abbiano portato a ritenere ancora sussistente l'interesse della collettività a disporre delle relative notizie (provv.ti 4 dicembre 2019, nn. 217 e 218, rispettivamente docc. web nn. 9232581 e 9232567); ciò anche nel caso in cui tale aggiornamento sia derivato dalla pubblicazione di informazioni recenti, provenienti anche da fonte diversa da quella segnalata dall'interessato, la disponibilità delle quali consentiva comunque agli utenti della rete di disporre di un quadro complessivo della vicenda corrispondente alla situazione attuale del medesimo (provv. 19 settembre 2019, n. 169, doc. web n. 9165102). Tale approccio è stato peraltro recentemente confermato dalla CGUE con la sentenza del 24 settembre 2019 (causa C-136/17) secondo la quale i limiti relativi al trattamento dei dati particolari di cui agli artt. 9 e 10 del RGPD trovano applicazione anche con riguardo ai gestori dei motori di ricerca. Pertanto questi ultimi devono, in linea di massima, accogliere le richieste di deindicizzazione riguardanti i *link* che rinviano a pagine web nelle quali compaiono dati personali

sensibili, a meno che tali *link* non si rivelino strettamente necessari per proteggere la libertà di informazione degli utenti di internet potenzialmente interessati ad avere accesso alle relative pagine web.

Tuttavia, nel caso in cui la richiesta di deindicizzazione riguardi pagine contenenti informazioni non più attuali (ad es., relative ad una condanna in primo grado di una persona poi assolta in appello) e sussistano circostanze tali da far ritenere prevalente l'interesse pubblico alla conoscenza – quali il ruolo pubblico rivestito dalla persona o la gravità del reato ad essa addebitato –, il gestore del motore di ricerca dovrà comunque ordinare i risultati di ricerca in base all'attualità dell'informazione.

9 Cyberbullismo

L'attività dell'Autorità nel settore del cyberbullismo è stata caratterizzata dalla gestione tempestiva delle segnalazioni che, in virtù dell'ampia collaborazione assicurata dai principali titolari del trattamento coinvolti in questo ambito, ha portato ad una rapida definizione delle richieste degli interessati concernenti, principalmente, la rimozione di contenuti e/o immagini di carattere offensivo e denigratorio nonché di falsi profili creati all'interno di *social network*. Esiguo il numero di casi nei quali non sono stati ravvisati i presupposti per poter procedere in ragione della riscontrata carenza degli elementi che la legge n. 71/2017 indica quali requisiti minimi per qualificare una condotta come atto di cyberbullismo.

È stata consolidata la procedura già implementata dall'Ufficio per la trattazione di questa tipologia di segnalazioni ed è stata altresì avviata una riflessione sulla possibile sovrapposizione, in relazione alle specifiche competenze assegnate al Garante, tra la disciplina dettata dalla legge sul cyberbullismo – che comprende, tra le condotte elencate nell'art. 1, anche il trattamento illecito di dati personali – e la normativa di riferimento in tale settore costituita dal RGPD nonché dal Codice; ciò anche per raccordare l'esigenza di assicurare una rapidità di intervento in questo ambito con quella di attivare, nel caso in cui ne ricorrano i presupposti, la procedura di cooperazione con le altre autorità interessate. Tale concomitanza potrebbe anche consentire di disporre di strumenti aggiuntivi idonei ad agevolare il contatto con titolari del trattamento aventi sede all'estero, tenuto conto del fatto che il RGPD pone l'obbligo di nominare un rappresentante in capo a quei soggetti che, pur non stabiliti nel territorio dell'UE, ricadono nell'ambito di applicazione della normativa europea in materia di protezione dati personali (cfr. art. 3, par. 2, del RGPD).

Nel corso dell'anno vi sono state utili occasioni di confronto con gli altri soggetti istituzionali impegnati nel piano integrato d'azione per l'adozione di misure e strategie dirette alla prevenzione del fenomeno; in particolare, è stato riattivato il dialogo all'interno della sede a ciò deputata dalla legge n. 71/2017, ovvero il Tavolo tecnico per la prevenzione ed il contrasto al cyberbullismo (disciplinato dall'art. 3), che si è riunito nel mese di luglio con lo scopo di condividere le iniziative intraprese in via autonoma da parte di ciascuno dei partecipanti nonché di raccordare le attività dirette a realizzare i compiti attribuiti al consesso comune, quali quello di monitoraggio del fenomeno – tenuto conto del fatto che, allo stato attuale, non risultano dati certi sull'entità di quest'ultimo, scontandosi piuttosto un'estrema variabilità statistica dipendente dalla fonte di provenienza dei dati – e di redazione di un codice di co-regolamentazione al quale dovranno adeguarsi gli operatori del settore.

È stata altresì colta l'occasione per implementare strumenti di collaborazione con organismi legati ad una dimensione territoriale di tipo locale, quali i Co.re.com., con alcuni dei quali sono state siglate apposite convenzioni aventi principalmente lo scopo di agevolare la divulgazione di informazioni relative al fenomeno secondo un criterio di prossimità con l'utenza di riferimento, senza con ciò alterare lo schema di competenze attribuite dalla legge al Garante che, come tali, non appaiono delegabili.

In chiusura d'anno è stato infine ripreso il dialogo con il Miur anche con riguardo al progetto "Generazioni connesse" che ha portato alla partecipazione dell'Autorità al *Safer Internet Day 2020*, manifestazione avente lo scopo di sen-

9

sibilizzare la collettività su tematiche di interesse per questo settore e che, in tale occasione, ha posto il *focus* sulle misure da implementare per rendere più sicuro l'utilizzo della rete da parte dei ragazzi. È emersa, in particolare, la necessità di assicurare una sinergia educativa tra scuola e famiglia e quindi una rete di supporto ai giovani, specie se minori di età, allo scopo di favorire un approccio più consapevole e prudente nell'utilizzo di dispositivi che, se ben impiegati, sono in grado di offrire validi strumenti di conoscenza e di interazione sociale.

10 *Marketing* e trattamento dei dati personali

10.1. *Telemarketing*

Come già indicato in passato (cfr. Relazione 2018, p. 105, e ivi più risalenti richiami), le segnalazioni in materia di *marketing*, alle quali nel 2019 si sono aggiunti anche numerosi reclami formulati ai sensi del RGPD, hanno riguardato, in assoluta prevalenza, il cd. *telemarketing* selvaggio e, in misura minore, comunicazioni commerciali via *e-mail* o sms.

Con particolare riguardo all'ambito del *telemarketing*, migliaia permangono le segnalazioni portate all'attenzione del Garante (per un'analisi di dettaglio v. sez. IV, tab. 10) che, in ragione della loro numerosità e della complessità delle operazioni necessarie per risalire all'effettiva (sovente articolata) "filiera" del trattamento (con la conseguente individuazione delle relative responsabilità), continuano a costituire il "carico" di lavoro assolutamente prevalente dell'Autorità.

Specie con riguardo alle segnalazioni presentate nei confronti di taluni operatori, non si sono registrati purtroppo segnali tangibili di flessione malgrado gli interventi e i conseguenti provvedimenti di varia natura (inibitori, prescrittivi e sanzionatori) già adottati dall'Autorità e menzionati nelle precedenti Relazioni.

Dall'analisi delle segnalazioni pervenute risulta che le telefonate indesiderate continuano ad interessare sia gli abbonati iscritti nel Registro pubblico delle opposizioni – circostanza dalla quale si devono quindi desumere comportamenti poco virtuosi da parte dei soggetti operanti nella filiera del *telemarketing*, che dal committente della campagna promozionale si snoda fino all'ultimo anello della stessa, l'operatore che materialmente effettua la chiamata –, sia i titolari di numerazioni (residenziali e, sempre più spesso, mobili) non pubblicate su elenchi telefonici (cd. numerazioni riservate).

I settori merceologici nei quali operano i committenti oggetto di segnalazione continuano ad essere soprattutto quello telefonico ed energetico, con una differenziata consistenza numerica delle segnalazioni rispetto a ciascuno degli operatori. Modalità particolarmente aggressive (oltre che la mancata identificazione del committente) vengono lamentate rispetto a chiamate promozionali nel settore finanziario e valutario e, meno frequentemente, nel settore telefonico.

Non di rado, come pure segnalato in passato, le telefonate promozionali indesiderate vengono eseguite da parte di *call center* stabiliti al di fuori del territorio nazionale, all'esito di processi di delocalizzazione delle attività economiche per le ragioni più varie, perlopiù di natura fiscale e giuslavoristica.

Si registra una flessione del fenomeno delle telefonate effettuate, in violazione di legge, con numerazione chiamante oscurata.

Sotto un diverso profilo, persistono i casi nei quali viene lamentato il mancato o tardivo riscontro all'esercizio dei diritti degli interessati da parte degli operatori economici nel cui interesse si lamentano essere effettuate le comunicazioni promozionali, fenomeno peraltro già segnalato (cfr. Relazione 2018, p. 106). In particolare, vengono lamentate non solo la violazione del diritto di opposizione all'ulteriore trattamento per finalità di *marketing*, ma anche, in spregio dei diritti di accesso ai propri dati, l'assenza o la carenza di riscontro rispetto alle necessarie indicazioni,

ad esempio, circa l'origine dei medesimi, elemento conoscitivo imprescindibile al fine di consentire all'interessato di risalire alle banche dati che stanno a monte delle comunicazioni telefoniche ricevute.

La dimensione assunta dal fenomeno del cd. *marketing* selvaggio e la sua persistenza in termini sostanzialmente immutati (come risulta dall'analisi delle ultime Relazioni), ha indotto l'Autorità ad inviare il 19 aprile 2019 un corposo ed articolato appunto alla Procura della Repubblica presso il Tribunale di Roma, in ordine al menzionato fenomeno del *marketing* selvaggio, con particolare riferimento alle telefonate promozionali, contenente una puntuale ricostruzione storica della complessa e variegata attività messa in atto dall'Autorità (provvedimenti inibitori e prescrittivi; provvedimenti generali e linee guida; ordinanze di ingiunzione per la contestazione delle correlate sanzioni) e una disamina delle principali criticità riscontrate, peraltro corredata da un prospetto sulle maggiori sanzioni inflitte nell'ultimo periodo.

10

Appunto inviato alla Procura della Repubblica

L'esigenza di informare l'Autorità giudiziaria è nata, da un lato, dall'aver riscontrato i limiti dei poteri di "indagine" del Garante, soprattutto con riferimento a società che nascono anche solo per una campagna promozionale e fanno rapidamente perdere ogni traccia, oppure sono localizzate in Paesi extra-UE e, dall'altro, dall'esigenza di rappresentare il fenomeno anche in vista di possibili esiti di carattere penale collegati alle istruttorie, in corso o future, nei confronti degli operatori telefonici, come sopra evidenziato, sui quali si appuntano in modo ricorrente segnalazioni e reclami.

Il riscontro ai segnalanti

Ovviamente, nonostante tale segnalazione, è proseguita l'attività ordinaria di contrasto al fenomeno e di assistenza all'elevato numero di utenti che si sono rivolti al Garante. Così, riformulate le FAQ presenti sul sito web dell'Autorità (v. doc. web n. 1794339) adeguandole alle modifiche normative intervenute, l'Ufficio ha continuato, pur a fronte di risorse limitate, a dare riscontro individualizzato a larga parte delle (migliaia di) segnalazioni pervenute (sovente da parte di segnalanti che reiteratamente, o anche solo episodicamente, hanno lamentato la persistenza dei contatti indesiderati, nonostante l'esercizio del diritto di opposizione o l'iscrizione della propria numerazione nel Rpo). Ciò al fine di rendere edotti gli interessati della particolare attenzione dedicata dall'Autorità alla problematica del *marketing* indesiderato, oltre che della possibilità di considerare le loro doglianze, in forma comunque aggregata, in vista dell'accertamento della correttezza e legittimità dei trattamenti posti in essere.

Nei medesimi riscontri sono stati indicati i provvedimenti assunti e forniti alcuni suggerimenti pratici sulle possibilità e modalità di blocco delle comunicazioni non gradite. Con analoghi riscontri sono state costantemente fornite informazioni sugli strumenti messi a disposizione dall'ordinamento a vantaggio degli interessati per opporsi alle telefonate indesiderate e/o per ottenere informazioni sull'origine dei propri dati nella disponibilità delle imprese committenti o incaricate dell'attività di *telemarketing* (o per esercitare gli altri diritti di cui agli artt. 15-22 del RGPD), anche avvalendosi del modello predisposto dall'Autorità (cfr. doc. web n. 1089924).

In questa prospettiva, nelle comunicazioni individuali si sono invitati i segnalanti a non escludere la possibilità, quantomeno in taluni casi, della liceità del contatto commerciale sulla base di un consenso prestato, anche per inavvertenza, a vantaggio del medesimo operatore economico nel cui interesse si è contattati (come, in occasione dell'acquisto di beni o servizi forniti) o a terzi (ad es., partecipando a concorsi a premi, o autorizzando tali usi su siti web di natura più varia per l'utilizzo, magari senza corrispettivo, di alcuni servizi), anche sulla base di un consenso, talora illegittimamente acquisito, come nei casi di cd. consenso obbligato (materia sulla quale il Garante ha continuato ad intervenire anche nel 2019: v. ad es. provv.ti 12

10

giugno 2019, n. 130, doc. web n. 9120218, e 20 giugno 2019, n. 133, doc. web n. 9124420).

Comunicazioni puntuali sono state regolarmente inviate anche con riferimento alle numerose e reiterate segnalazioni riguardanti telefonate promozionali provenienti da soggetti, od effettuate per conto di committenti, non individuati, o per le quali non è stata indicata la/e numerazione/i chiamante/i o altri elementi (come la data e l'ora dei contatti indesiderati), elementi essenziali ai fini dell'attività di controllo dell'Autorità.

Nella gestione delle variegate doglianze spesso è emerso il problema dell'irreperibilità di vari titolari extra-UE che, pur avendo l'obbligo di nomina di un rappresentante nell'Unione, non vi ottemperano (il RGPD non prevede sanzioni al riguardo) ovvero non rendono noto di avervi ottemperato. Peraltro, in base alla normativa vigente, il rappresentante può essere nominato in qualsiasi Stato dell'Unione, con l'effetto che risulta impossibile determinare, di fatto, l'autorità di protezione dati competente a ricevere l'eventuale comunicazione relativa all'avvenuta nomina. Si segnala che, in molti casi, è risultato molto difficile far comprendere ai reclamanti che il Garante dispone di mezzi istruttori e d'indagine decisamente limitati rispetto a queste tipologie di violazioni.

Accertamenti presso operatori telefonici ed energetici

L'attività di controllo in relazione al fenomeno in parola anche nel 2019 – pur con le difficoltà operative legate all'eccezionale mole dei reclami pervenuti – è stata intensa e contrassegnata, ricorrendone gli estremi, anche dall'adozione di ordinanze-ingiunzione. Richieste di informazioni, in grande numero e senza soluzione di continuità, sono state rivolte – a seconda della tipologia e gravità della violazione ipotizzata, in via cumulativa, al fine di ottenere utili indicazioni per la verifica dell'adeguatezza delle misure poste in atto rispetto alle prescrizioni del RGPD, ma anche in relazione a casi singoli – alle società telefoniche, essendo tra le principali destinatarie di segnalazioni per l'invio di telefonate e sms promozionali indesiderati, talora anche dopo l'opposizione fatta valere (non di rado reiteratamente) dagli interessati.

Sono altresì proseguiti gli accertamenti ispettivi, effettuati ai sensi degli artt. 157 e, talora, 158 del Codice, anche per il tramite del Nucleo speciale *privacy* e frodi tecnologiche della Guardia di finanza, presso le sedi legali e operative di tali società e/o dei loro *dealer*, incaricati dello svolgimento delle campagne promozionali sulla base delle liste fornite dalle committenti o nell'autonoma disponibilità degli stessi. Specifica attenzione occorre riconoscere alle attività istruttorie, di seguito descritte, condotte nei confronti di due primari operatori, rispettivamente del settore telefonico e del settore energetico, anche in considerazione della misura elevata delle sanzioni pecuniarie, in funzione anche deterrente, comminate ai sensi dell'art. 83 del RGPD e degli specifici criteri utilizzati per la loro commisurazione.

Trattamenti di dati nel settore energetico

A chiusura di un'istruttoria riguardante trattamenti a fini di *telemarketing* effettuata anteriormente alla piena operatività del RGPD è stato adottato, nei confronti di un'importante società del settore energetico, un provvedimento dichiarativo dell'illecito trattamento dei dati personali dell'interessato, essendo emersa la natura promozionale e non meramente informativa (come asserito dalla società) del contatto oggetto di accertamento in assenza del necessario consenso o di altra valida base giuridica (provv. 14 febbraio 2019, n. 45, doc. web n. 9102927).

Nei confronti del medesimo operatore è stato adottato un ulteriore provvedimento con il quale è stata comminata una sanzione di 8,5 milioni di euro riguardo a trattamenti illeciti nelle attività di *telemarketing* e *teleselling* riscontrati nel corso di accertamenti e ispezioni, a seguito di diverse decine di segnalazioni e reclami, ricevuti all'indomani della piena applicazione del RGPD.

Dalle verifiche è altresì emerso un circoscritto numero di casi rivelatori di con-

dotte "di sistema" poste in essere dalla società che hanno evidenziato gravi criticità relative al generale trattamento dei dati. Tra le violazioni accertate risultano quelle relative alle telefonate pubblicitarie effettuate senza il consenso della persona contattata o nonostante il diniego opposto a ricevere chiamate promozionali, oppure senza attivare le specifiche procedure di verifica del Registro pubblico delle opposizioni; l'assenza di misure tecnico-organizzative in grado di recepire le manifestazioni di volontà degli utenti; i tempi di conservazione dei dati, superiori a quelli consentiti; l'acquisizione dei dati dei potenziali clienti da soggetti (*list provider*) che non avevano acquisito il consenso per la comunicazione. Con il provvedimento, dichiarata l'illiceità delle condotte rilevate, si è ingiunto alla società di implementare procedure e sistemi per verificare, anche tramite l'esame di un campione rilevante di nominativi, lo stato dei consensi delle persone inserite nelle liste dei contatti prima dell'inizio delle campagne promozionali. La società dovrà inoltre provvedere alla definitiva automatizzazione dei flussi di dati dal proprio *database* alla *black list* di chi non intende essere contattato per finalità promozionali. È stato altresì vietato l'uso dei dati forniti dai *list provider* che non avessero acquisito uno specifico consenso alla loro comunicazione alla società.

Si segnala che quest'ultima risulta aver oblato la sanzione pecuniaria e avviato un percorso di adeguamento delle proprie procedure e dei connessi trattamenti alla vigente normativa, per il tramite delle misure correttive stabilite dal Garante (provv. 11 dicembre 2019, n. 232, doc. web n. 9244365).

Analoghi accertamenti sono stati contestualmente avviati nei confronti di altre compagnie telefoniche, i cui esiti (salvo quanto già si dirà al par. 11.1) si auspica di definire a breve, anche in vista dell'adozione delle opportune misure correttive.

11 Internet e servizi di comunicazione elettronica

11.1. *Trattamenti di dati nel settore telefonico*

È stato adottato un provvedimento, ad ampio spettro di contenuti, nei confronti di una primaria compagnia telefonica con il quale è stata comminata una sanzione di circa 28 milioni di euro, ad oggi la più elevata nella storia del Garante, pur considerati il periodo di prima applicazione delle sanzioni previste dal RGPD e il necessario bilanciamento con le esigenze dell'impresa, incluse quelle connesse alla continuità aziendale. Le verifiche hanno preso le mosse da centinaia di segnalazioni relative alla ricezione di chiamate promozionali indesiderate effettuate senza consenso o nonostante l'iscrizione delle utenze telefoniche nel Registro pubblico delle opposizioni, oppure in tempi successivi all'esercizio del diritto di opposizione nei confronti della società. Irregolarità nel trattamento dei dati venivano lamentate anche nell'ambito del sito web e nella modulistica.

Muovendo da tali elementi, l'Ufficio ha svolto una più ampia attività istruttoria (non limitata al solo ambito delle chiamate promozionali) dalla quale sono emerse le seguenti numerose gravi violazioni (peraltro in parte reiterate, essendo stati già adottati provvedimenti riguardanti analoghi trattamenti illegittimi): telefonate promozionali effettuate senza il consenso delle persone contattate, talvolta fino a 155 volte nel mese; assenza di controllo da parte della società sull'operato di alcuni *partner*; errata gestione e mancato aggiornamento delle *black list*; telefonate promozionali verso numerazioni non presenti nelle liste di contattabilità; acquisizione obbligata del consenso a fini promozionali per poter aderire al programma di fedeltà *online*; informazioni non corrette, né trasparenti sul trattamento dei dati e modalità di acquisizione del consenso non valide nella gestione di alcune *app* destinate alla clientela; utilizzo di modulistica cartacea con richiesta di un consenso unico per finalità diverse; gestione inidonea dei *data breach*; progettazione (*design*) e gestione inadeguata dei sistemi che trattano dati personali; inadeguata capacità di comprovare alcuni trattamenti e relativi adempimenti (*accountability*).

Con il provvedimento in questione, che contiene ben 20 misure tra divieti e prescrizioni, si è vietato alla compagnia telefonica l'uso dei dati a fini di *marketing* di quanti avevano espresso il proprio diniego a ricevere telefonate commerciali e dei soggetti presenti in *black list* o dei "non clienti" conservati per altri motivi nel *database* dei clienti. La società non potrà più utilizzare neanche i dati della clientela raccolti mediante le *app* per finalità diverse dall'erogazione dei servizi senza un consenso libero e specifico. Fra le prescrizioni impartite, è stato ingiunto di verificare la consistenza delle *black list* utilizzate e di acquisire tempestivamente quelle eventualmente prodotte dai *partner* per riversarle nella propria.

Alla compagnia è stato prescritto anche di rivedere le modalità di trattamento dei dati in relazione al programma fedeltà, rendendo libero l'accesso dei clienti a sconti e concorsi a premi ed eliminando il consenso obbligato al *marketing*. La società dovrà anche rivedere la procedura relativa alle proprie *app* e specificare, con linguaggio chiaro e comprensibile (anche in considerazione del tipo di utenza e quindi con specifica necessaria attenzione agli utenti minori di età), i trattamenti svolti con l'indicazione delle finalità perseguite e delle modalità di trattamento uti-

lizzate, nonché acquisire un valido consenso per i vari trattamenti. Le è stato altresì ingiunto di implementare le misure tecniche ed organizzative relative alla gestione delle istanze di esercizio dei diritti degli interessati e di rafforzare le misure volte ad assicurare la qualità, l'esattezza e il tempestivo aggiornamento dei dati personali trattati dai diversi sistemi in uso.

Si segnala infine che l'Autorità, nell'ambito del medesimo provvedimento, è intervenuta, con approccio anche innovativo, su questioni fattuali e giuridiche alquanto dibattute dagli operatori del settore, quali: il legittimo interesse al *marketing*, stabilendo che, in conformità a quanto previsto dal RGPD, questa base giuridica può sostituire il consenso solo ricorrendo certe condizioni ed entro certi limiti; la possibile contitolarità del trattamento fra committente della campagna promozionale e *call center* incaricati del loro svolgimento; l'utilizzo di numeri "fuori lista", con particolare riferimento ai soggetti *lead* (ossia soggetti che abbiano rilasciato i propri dati in un determinato *form online* oppure abbiano chiesto di essere ricontattati dall'operatore) e a quelli cd. referenziati (numerazioni cioè "suggerite" da soggetti presenti in liste di utenze contattabili); la (non) negoziabilità del consenso al trattamento (in particolare, per le finalità promozionali).

Si segnala che la società ha oblato la sanzione pecuniaria e, quel che più conta, risulta aver avviato un percorso di adeguamento alla normativa dei propri sistemi, delle proprie procedure e dei connessi trattamenti, finalizzato ad implementare le numerose e puntuali misure correttive stabilite dal Garante (provv. 15 gennaio 2020, n. 7, doc. web n. 9256486).

Comunicazione di dati all'estero

Nell'ambito di un'istruttoria di carattere generale, avviata nel 2017 per verificare le modalità di controllo dei grandi operatori (di telefonia e *utilities*) sulla filiera del trattamento effettuato per attività di *telemarketing*, è stato effettuato un accertamento ispettivo presso una società fornitrice di servizi di *call center*. Ne è emerso che le attività da questa condotte per conto di un operatore di telefonia avevano comportato una comunicazione di dati personali ad un soggetto terzo, operante quale subfornitore, senza il preventivo consenso del titolare del trattamento. Inoltre, data l'ubicazione dello stabilimento dell'impresa in Albania, tale comunicazione ha integrato anche un trasferimento all'estero dei dati personali. Rilevata l'illiceità del trattamento, la società è stata ammonita a conformare il trattamento di dati personali alle disposizioni della disciplina vigente. Al contempo, l'Autorità ha avviato nei confronti della medesima società, un distinto procedimento sanzionatorio ai fini della contestazione della sanzione amministrativa di cui al testo previgente dell'art. 162, comma 2-*bis*, del Codice, con specifico riguardo alla comunicazione non autorizzata di dati personali in violazione del testo previgente degli artt. 23 e 24 del Codice, nonché all'illecito trasferimento all'estero dei dati personali, in violazione del testo previgente dell'art. 45 del Codice (provv. 18 dicembre 2019, n. 223, doc. web n. 9220727).

11.2. *Raccolta dei dati* online *per finalità di* marketing *e profilazione*

E-commerce e *fidelity card*

Provvedimenti inibitori e prescrittivi sono stati adottati, definendo istruttorie complesse, condotte anche mediante accertamenti ispettivi *in loco*, in vigenza della normativa anteriore alla piena operatività del RGPD e riguardanti il reiterato trattamento indesiderato di dati riferiti a milioni di individui a fini promozionali.

Fra questi, si segnala il provvedimento adottato il 20 giugno 2019, n. 133 (doc. web n. 9124420) nei confronti di una nota piattaforma di *e-ecommerce*, concernente la raccolta di dati mediante *fidelity card* presso i propri punti vendita e l'effettua-

11

zione di comunicazioni promozionali indesiderate, sia in ragione della raccolta di un consenso non libero per le finalità promozionali tramite moduli contraddistinti da un unico indistinto consenso anche per finalità contrattuali (moduli risultati utilizzati per un certo lasso temporale e poi sostituiti da nuovi moduli conformi alla normativa in materia), sia in ragione di alcuni contatti promozionali risultati effettuati in assenza del necessario specifico consenso.

In tale occasione, la società è stata ammonita a non svolgere il trattamento per finalità promozionali dei dati personali degli interessati raccolti mediante i moduli relativi alle *fidelity card* in assenza di un comprovato consenso libero e specifico. Inoltre – anche a fronte di alcune doglianze risultate fondate e delle difficoltà manifestate dalla società nel reperire ed esibire la documentazione relativa alle proprie *fidelity card* nonchè all'acquisizione del consenso degli interessati per le varie finalità di trattamento – è stato ingiunto alla stessa di: implementare misure organizzative e tecniche adeguate per garantire la corretta gestione dei diritti degli interessati, ed in particolare il diritto di opposizione al trattamento per finalità promozionali; assicurare il tracciamento puntuale e documentato, rispetto a ciascun interessato, degli adempimenti imposti dalla normativa, anche alla luce dei principi di *accountability* e di *privacy by design*.

Nell'ambito di tale procedimento di rilevante impatto su procedure e sistemi della società, è stata anche contestata la sanzione amministrativa concernente la mancata acquisizione di un valido consenso (in base al previgente art. 162, comma 2-*bis*, del Codice).

Fidelizzazione

Nell'ambito delle predette verifiche, si evidenzia inoltre l'adozione del provvedimento 12 giugno 2019, n. 130 (doc. web n. 9120218), nei confronti di una nota società del settore dell'igiene intima di bimbi ed adulti, con particolare riguardo alla raccolta e al successivo trattamento di dati personali mediante un programma di raccolta punti *online*, per poter partecipare al quale gli utenti risultavano obbligati a rilasciare due consensi generici per finalità promozionali, uno per la società e uno per i marchi collegati.

Oltre a disporre il divieto, si è ingiunto alla società, nel caso avesse inteso continuare a svolgere attività promozionali, di modificare il *form* di raccolta dati presente sul proprio sito web, al fine di consentire agli utenti di esprimere un consenso libero e informato per tale finalità. Anche in questo caso è stata contestata la sanzione amministrativa concernente la mancata acquisizione di un valido consenso.

Portabilità e remunerazione dei dati personali

Nel corso dell'anno sono pervenute al Garante diverse segnalazioni, provenienti in prevalenza da operatori della grande distribuzione, con le quali si lamentava la ricezione di numerose richieste, concernenti l'esercizio del diritto alla portabilità dei dati, non inviate direttamente dagli interessati ma generate per loro conto da una *app* che offre ai propri iscritti una remunerazione in cambio del conferimento di dati personali.

La problematica connessa al riconoscimento di un valore economico dei dati, fattasi più evidente con il massiccio utilizzo che di questi viene fatto nei servizi digitali, pone interrogativi in merito alla questione del bilanciamento fra la tutela di un diritto fondamentale, qual è quello alla protezione dei dati personali, e l'esigenza di favorire lo sviluppo di nuovi servizi necessari a garantire il pluralismo e la competitività del mercato unico digitale nonché, ancor prima, la libertà d'iniziativa economica e d'impresa, che pur trova esplicita tutela nella maggior parte degli ordinamenti del sistema UE. Ciò in linea anche con il percorso legislativo avviato in sede europea in materia di tutela del consumatore e della concorrenza nell'ambito della più generale strategia per il mercato unico digitale (cfr. il pacchetto di misure presentate dalla Commissione europea nell'ambito della Comunicazione, Un "New Deal" per i consumatori, COM(2018) 183 dell'11 aprile 2018).

Tali valutazioni sono, inoltre, strettamente connesse alla difficoltà di individuare un'idonea base giuridica per siffatti trattamenti, in grado di garantire un'adeguata tutela alla persona in termini di diritto all'autodeterminazione e protezione dal pregiudizio e dalle potenziali discriminazioni, anche alla luce del fondamentale principio della libertà e specificità del consenso degli interessati per le finalità promozionali, come ribadito dal RGPD (v. artt. 4 e 7, in particolare).

Data la portata evidentemente transnazionale delle questioni emerse dall'istruttoria preliminare, il Garante ha interessato il Comitato al fine di pervenire ad un orientamento condiviso in sede europea per garantire, per quanto possibile, l'uniforme applicazione della normativa in vigore.

11.3. *Attività svolta in relazione ai trattamenti di dati personali a fini di propaganda elettorale*

In vista delle consultazioni elettorali europee del 2019, anche alla luce del nuovo quadro normativo introdotto dal RGPD, il Garante ha approvato il provvedimento 18 aprile 2019, n. 96 (doc. web n. 9105201) che fissa le regole per il corretto uso dei dati relativi agli elettori da parte di partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati (cfr. par. 14.5.3), soffermandosi altresì sull'uso di messaggi politici e propagandistici inviati agli utenti dei *social network* (quali Facebook e Linkedin) o su altre piattaforme di messaggistica (come Skype, Whatsapp, Messenger). In tale occasione si è ribadito che, anche alla luce di casi recenti di profilazione massiva degli elettori (il cd. *micro-targeting*), pure in quest'ambito il trattamento dei dati deve rispettare la cornice normativa esistente, sì da proteggere il processo elettorale ed evitare rischi di interferenze e turbative esterne. Le preoccupazioni di un utilizzo improprio dei dati personali per sofisticate attività di profilazione su larga scala e di invio massivo di comunicazioni o, ancora, per orientare campagne personalizzate volte a influenzare l'orientamento politico e/o la scelta di voto degli interessati sulla base degli interessi personali, dei valori, delle abitudini e dello stile di vita dei singoli rendono infatti urgente garantire la corretta applicazione delle norme in materia di protezione dei dati, soprattutto *online*, anche al fine di proteggere il processo elettorale da interferenze e turbative esterne.

In tale quadro, va ribadito che il trattamento dei dati personali finalizzato all'invio di messaggi politici e propagandistici agli utenti di *social network* (come Facebook o Linkedin), in privato come pubblicamente sulla bacheca virtuale degli stessi, sono sottoposti alla disciplina in materia di protezione dei dati (artt. 5, 6, 7, 13, 24 e 25 del RGPD). La medesima disciplina è altresì applicabile ai messaggi inviati utilizzando altre piattaforme, come Skype, WhatsApp, Viber, Messenger, rispetto alle quali i rischi sopra evidenziati risultano ancor più elevati in considerazione delle peculiari condizioni di servizio imposte unilateralmente dalle piattaforme di comunicazione e *social networking*, anche mediante i dispositivi mobili utilizzati. Talora, infatti, esse prevedono la condivisione indifferenziata (e senza il necessario consenso specifico) di tutti o gran parte dei dati personali memorizzati negli *smartphone* e nei *tablet* (quali rubrica, contatti, sms, foto, dati della navigazione internet) o l'accesso del fornitore a tali informazioni.

Come stabilito nel provvedimento generale in parola, ove i titolari procedano, per finalità di propaganda elettorale e connessa comunicazione politica, al trattamento di dati personali presenti sui *social* (o reperiti altrove), nel rispetto dei principi e dei presupposti di liceità sopra individuati (artt. 5, 6, 13 e ss., del RGPD), è necessario comunque evitare comunicazioni massive e insistenti, nonché

11

condotte non corrette quali: contatti mediante telefonate o sms in orario notturno; comunicazioni che mirino ad acquisire informazioni personali degli interessati eccedenti e non pertinenti con la finalità di propaganda elettorale e comunicazione politica. Coerentemente con i principi sopra ribaditi, ove nei *social network*, come anche in *blog* e *forum* utilizzati dalla comunità degli iscritti ai servizi *social*, risultino visualizzabili numeri di telefono o indirizzi di posta elettronica, i suindicati titolari, che intendano inviare messaggi finalizzati alla comunicazione politica/elettorale, dovranno aver previamente acquisito, per ciascun di tali "contatti", un preventivo consenso libero, specifico, documentato ed informato per la finalità in questione oppure basarsi su un altro eventuale presupposto di liceità (v. art. 6 del RGPD).

Elezioni europee 2019

Anche sulla base di tale provvedimento, l'Ufficio ha condotto, con riferimento alle consultazioni elettorali europee svoltesi nel maggio 2019, un'ampia attività di monitoraggio circa il corretto trattamento di dati personali da parte dei candidati politici ed amministrativi. Le istruttorie sono state avviate sulla scorta di segnalazioni e reclami pervenuti all'Ufficio nonché sulla base di notizie di stampa apparse nel periodo considerato e hanno riguardato sia numerose comunicazioni propagandistiche a mezzo *e-mail* (e, in misura alquanto minore, posta cartacea), sia la raccolta di dati personali mediante concorsi a premi organizzati sui *social*. Nella maggior parte dei casi si è proceduto ad inviare ai titolari del trattamento la comunicazione di avvio del procedimento per l'eventuale adozione di provvedimenti correttivi e sanzionatori (artt. 166, comma 5, del Codice e 12 reg. Garante n. 1/2019), con contestuale notifica delle presunte violazioni; istruttorie il cui esito si attende per l'anno in corso.

Cambridge Analytica

Il trattamento di dati in vista di competizioni elettorali è emerso anche nella più ampia istruttoria compiuta nei confronti di Facebook a seguito del noto caso Cambridge Analytica: essa ha inizialmente riguardato il trattamento di dati personali di cittadini italiani, fruitori dei servizi Facebook, da parte della società Cambridge Analytica per estendersi, successivamente, a due ulteriori servizi di Facebook, attivati in occasione delle elezioni politiche svoltesi in Italia il 4 marzo 2018: il prodotto "Candidati" e il promemoria sulle elezioni del 4 marzo 2018.

Con riferimento a Cambridge Analytica, l'aspetto problematico emerso sotto il profilo della protezione dei dati ha riguardato l'uso della funzione "Facebook Login", pensata per accedere alle *app* di terze parti attraverso la piattaforma Facebook. La comunicazione dei dati degli utenti da parte di Facebook a tali *app* è stata dichiarata illegittima in quanto fondata su un'informativa parziale e generica e avvenuta in assenza di un valido consenso degli interessati. Il provvedimento, tuttavia, si è limitato all'esame della sola *app* "Thisisyourdigitallife" (contenente un test della personalità ideato per raccogliere le informazioni personali oggetto di profilazione): è risultato che i dati dei cittadini italiani acquisiti tramite l'*app*, benché non trasmessi a Cambridge Analytica, erano stati comunque trattati in modo illecito, in assenza di un'idonea informativa e di uno specifico consenso.

Il prodotto "Candidati" offerto da Facebook consentiva agli elettori che fornivano il proprio indirizzo postale di ricevere informazioni sui candidati della propria circoscrizione elettorale e sui loro programmi. Facebook, pur affermando di non registrare informazioni su come gli utenti si fossero orientati su tali profili, conservava i *file* di log delle loro azioni per un periodo di 90 giorni, per poi estrarne non meglio definite matrici aggregate. Inoltre, per quanto riguarda il promemoria sulle elezioni del 4 marzo 2018, nel giorno delle elezioni appariva sul *newsfeed* degli utenti di Facebook un messaggio che sollecitava la condivisione dell'essersi o meno recati al voto e a condividere opinioni sull'importanza del voto espresso.

Il Garante ha rilevato che questi due servizi di Facebook, specificamente con-

cepiti e rivolti ai cittadini italiani in prossimità delle elezioni politiche per il Parlamento non rientravano tra le finalità indicate nella *data policy* della piattaforma. Si è quindi ritenuto che Facebook, attraverso detti servizi, abbia effettuato trattamenti di dati personali potenzialmente idonei a rilevare le opinioni politiche degli interessati che vi hanno aderito, in violazione dei previgenti artt. 13 e 23 del Codice. Per tali ragioni è stato vietato a Facebook il trattamento dei dati eventualmente raccolti mediante le descritte modalità così come quello relativo alle valutazioni espresse dagli utenti a seguito del messaggio sopra indicato (provv. 10 gennaio 2019, n. 5, doc. web n. 9080914).

Quale conseguenza della ravvisata illiceità, rispetto a talune delle violazioni accertate è intervenuto il pagamento in misura ridotta, pari a 52.000 euro, ai sensi dell'art. 16, l. n. 689/1981; per le violazioni rispetto alle quali non è prevista tale facoltà, il Garante ha adottato un provvedimento sanzionatorio applicando una sanzione di un milione di euro (cfr. ordinanza-ingiunzione 14 giugno 2019, n. 134, doc. web n. 9121486).

La medesima violazione relativa al prodotto "Canditati" è stata ravvisata anche in occasione delle elezioni europee. Infatti, in data 26 maggio 2019, giornata in cui anche in Italia si sono svolte le elezioni politiche europee, nella "sezione notizie" di Facebook è stato pubblicato un messaggio dal titolo "È tempo di votare!" con il quale si invitavano gli utenti a condividere il fatto di aver votato. Nella stessa giornata, in alcune regioni ed in molti comuni italiani si sono svolte anche le consultazioni per il rinnovo dei relativi organi di governo e pertanto la condivisione del fatto di aver votato risultava indistintamente riferibile anche a tale partecipazione. L'ambito di tale condivisione è legato alle impostazioni del profilo di ciascun utente, con conseguente possibilità di rendere nota la suddetta informazione, oltre che ai gestori della piattaforma, alla propria cerchia di "amici" (profilo chiuso), ovvero ad un numero indeterminato di soggetti (profilo pubblico).

La condivisione dell'informazione circa l'aver votato è potenzialmente idonea a rivelare le opinioni politiche dell'interessato e quindi annoverabile all'interno delle "categorie particolari di dati personali" (art. 9 del RGPD); pertanto, considerato che vi è stata da parte di Facebook un'acquisizione e conservazione di tali tipologie di dati personali, senza idonea informativa, il Garante ha ravvisato la configurabilità di una violazione dell'art. 13 del RGPD e ha chiesto all'autorità irlandese di condurre ogni utile accertamento.

L'attività dell'Ufficio nei riguardi delle grandi piattaforme web, come si evince anche dal caso appena riportato, è stata profondamente innovata dall'entrata in vigore del RGPD e, in particolare, dall'introduzione delle procedure di cooperazione previste dagli art. 60 ss.

Trattandosi nella quasi totalità di casi riguardanti soggetti extra-UE stabiliti in altri Paesi europei, infatti, ha trovato applicazione il meccanismo dello *One Stop Shop*, individuando l'autorità capofila ed operando con essa e le altre autorità coinvolte mediante la piattaforma di interscambio di informazioni e documenti (IMI) di cui si dà più ampiamente conto, in ragione della sua significatività, nel seguente paragrafo (cfr. anche par. 21.1).

11.4. *Procedure IMI relative a trattamenti di dati in internet e in materia di comunicazioni elettroniche*

Il coinvolgimento dell'Autorità nelle procedure di cooperazione europea, che si incardinano in presenza di un trattamento transfrontaliero di dati personali, ha

11

costituito una porzione cospicua dell'attività svolta con riferimento ad internet ed alle comunicazioni elettroniche. La vocazione globale del web determina, infatti, un inevitabile impatto dei trattamenti di dati personali che afferiscono alla fornitura dei tipici servizi della società dell'informazione (*e-commerce, online advertising*, servizi offerti da *hosting* e *content provider*) con le disposizioni introdotte dal RGPD in tema di cooperazione e coerenza.

Se il livello coerente ed elevato della protezione dei dati personali è una delle finalità perseguite dal RGPD (cons. 10) e le autorità di controllo il mezzo attraverso cui attuarla (cons. 123), è evidente come tali trattamenti, per loro natura transfrontalieri (nel senso che incidono o probabilmente incidono in modo sostanziale su interessati residenti in più di uno Stato membro), rappresentino il primo e fondamentale settore in cui trovano applicazione i meccanismi previsti dal Capo VII.

Come rilevato altrove (par. 21.1), nel corso del 2019 le procedure di cooperazione sono state sottoposte ad una sorta di rodaggio, cui tutte le autorità di controllo europee hanno partecipato con spirito collaborativo, affrontando, anche attraverso la partecipazione a gruppi di lavoro insediati presso il Comitato, le non poche né semplici questioni giuridiche emerse dall'esperienza. Trattandosi di procedure tese alla definizione di procedimenti amministrativi (pur aventi carattere transnazionale), l'evoluzione delle varie fasi non può che essere progressiva: dalla quella preliminare del principio del *One Stop Shop* fino alla decisione del caso, attraverso i le fasi intermedie della cooperazione informale, assistenza reciproca e delle (eventuali) operazioni congiunte.

Per quanto riguarda i trattamenti in internet o nel contesto delle comunicazioni elettroniche, come facilmente prevedibile, nell'anno in riferimento, la stragrande maggioranza delle procedure pervenute all'Ufficio ha riguardato la fase preliminare relativa all'individuazione, ai sensi dell'art. 56 del RGPD, dell'autorità capofila (*Lead Supervisory Authority* - LSA) e delle autorità interessate (*Concerned Supervisory Authority* - CSA). La quasi totalità di tali procedure originano dalla presentazione di un reclamo, alcune scaturiscono da indagini di ufficio e poche, residue, da notizie di stampa. Un altro dato che assume particolare interesse, in quanto strettamente connesso al meccanismo di coerenza di cui all'art. 65, par. 1, lett. *b*), del RGPD, riguarda la mancanza (nel 2019) di opinioni contrastanti in merito alla competenza dell'autorità di controllo interessata per lo stabilimento principale. In altri termini, l'individuazione dell'autorità capofila, così come proposto dall'autorità interessata che ha aperto la procedura ex art. 56 e su cui le altre autorità sono tenute a pronunciarsi, non è mai stata oggetto di contrasti formali o di particolari dibattiti endoprocedimentali.

Sono invece emersi alcuni casi in cui le autorità interessate hanno ritenuto non applicabile il meccanismo dello sportello unico in quanto il titolare nei cui confronti era stata aperta la procedura non era stabilito in Unione europea, sulla scorta del disposto di cui all'art. 27 del RGPD, come interpretato dal Gruppo Art. 29 nelle linee guida n. 244 (rev. 01), in base alle quali, se una società non dispone di uno stabilimento nell'Unione europea, la semplice esistenza di un rappresentante designato nello Stato membro non comporta l'applicazione del principio del *One Stop Shop* ed il titolare dovrà interfacciarsi con le autorità di controllo di ciascuno Stato membro per il tramite del rappresentante designato.

La distribuzione dei casi relativi a trattamenti transfrontalieri valutata sulla scorta dell'autorità capofila competente evidenzia, anche in ragione dello specifico ambito in considerazione, una preponderante assegnazione e conseguente trattazione dei casi in capo alla *Data Protection Commission*, l'autorità irlandese di protezione dei dati personali, seguita (in virtù della tradizionale *liaison* commerciale tra i Paesi

anglosassoni e gli Stati Uniti d'America, ove hanno sede le principali *big tech company*) dall'*Information Commissioner's Office*, l'autorità inglese di protezione dei dati personali e, a scalare, ma in misura omogenea, dalle altre principali autorità di controllo europee.

Lo stabilimento di un considerevole numero di titolari nel Regno Unito comporterà non indifferenti problemi nella gestione delle procedure di cooperazione già avviate in conseguenza della Brexit.

Con riferimento alla posizione assunta dall'Autorità in merito alle procedure ex art. 56 relative al settore internet e comunicazioni elettroniche, si rileva che nell'80% dei casi la stessa si è dichiarata autorità interessata al trattamento transfrontaliero, prevalentemente ai sensi dell'art. 4, n. 22, lett. *b*), del RGPD, ovverosia in quanto gli interessati che risiedono in Italia sono o potrebbero essere influenzati in modo sostanziale dal trattamento. I casi in cui è stata espressa una dichiarazione di non interesse hanno riguardato principalmente trattamenti, formalmente a carattere europeo, ma di fatto circoscritti nell'ambito territoriale di Stati membri confinanti o accumunati da storici legami sociali, politici o economici (ad es. i Paesi scandinavi, i Paesi baltici e alcuni Paesi dell'est Europa).

Passando alla vera e propria fase di cooperazione, si osserva preliminarmente come l'articolato di cui all'art. 60 del RGPD ricomprenda diverse modalità di cooperazione che, sebbene logicamente progressive, sono assai diverse tra loro e riconducibili alle seguenti ipotesi: 1) consultazione informale (art. 60 IC); 2) progetto di decisione (art. 60 DD); 3) progetto di decisione revisionato (art. 60 RDD); 4) decisione finale (art. 60 FD).

Le procedure di consultazione informale, oltre che per il mero scambio di informazioni relative ai singoli casi in esame, sono state utilizzate e, verosimilmente, lo saranno sempre di più in futuro, al fine di agevolare lo scambio informale di pareri e valutazioni tra autorità di controllo in relazione a questioni, in fatto o in diritto, particolarmente delicate o controverse, ovvero relative a casi particolarmente importanti. Si tratta di una modalità pratica di utilizzo di tale procedura che è stata suffragata e promossa dallo stesso Comitato al fine di anticipare, in maniera informale e sfruttando al meglio la cooperazione tra autorità, eventuali discussioni sui progetti di decisione, che costituiscono il passo successivo delle procedure di cooperazione. Tale opzione è stata accolta con favore dalle autorità di controllo attesi i tempi strettissimi (quattro settimane) previsti dall'art. 60, par. 4, del RGPD per sollevare eventuali obiezioni motivate e pertinenti al progetto di decisione proposto dall'autorità capofila da parte delle autorità interessate, limitando, al contempo, le ipotesi di possibile intervento del Comitato, in sede decisoria, per la composizione di eventuali controversie all'interno del meccanismo di coerenza, ai sensi dell'art. 65, par. 1, lett. *a*), del RGPD.

Con riferimento alle procedure relative ai progetti di decisione, quelle giunte alla fase decisionale sono ancora quantitativamente assai ridotte rispetto al numero di procedure ex art. 56 nelle quali l'Autorità si è dichiarata autorità interessata. Si rileva inoltre, a conferma dell'assunto secondo cui l'approccio ai meccanismi di cooperazione e coerenza da parte di tutte le autorità di controllo europee è stato molto cauto e ponderato, trattandosi di procedure amministrative del tutto nuove ed innovative nell'*acquis* comunitario, come i progetti di decisione "caricati" sulla piattaforma IMI nell'anno 2019 abbiano prevalentemente riguardato reclami relativi ad ipotesi di violazione della normativa in tema di protezione dei dati personali di lieve entità per i quali, spesso, le competenti autorità capofila hanno proposto l'archiviazione del procedimento.

Per quanto concerne l'intervento dell'Autorità nelle procedure di cooperazione

11

relative ai progetti di decisione, nella maggioranza dei casi il progetto proposto dall'autorità capofila è stato ritenuto pienamente condivisibile; nei rimanenti casi, sono stati spesso formalizzati semplici commenti contenenti rilievi di forma o di merito.

Nelle ipotesi in cui è stato ritenuto, con procedura ai sensi dell'art. 18 del reg. Garante n. 1/2019, di sollevare una "obiezione motivata e pertinente", la competente autorità capofila ha sempre recepito tali indicazioni, procedendo ad una rivalutazione del provvedimento. In nessun caso si è quindi addivenuti all'attivazione del meccanismo di coerenza di cui all'art. 65, par. 1, lett. *a*), del RGPD, in forza del quale il Comitato adotta una decisione vincolante qualora un'autorità capofila non intenda dare seguito ad un'obiezione pertinente e motivata o l'abbia rigettata in quanto non pertinente o non motivata.

Per quanto riguarda infine le procedure di mutua assistenza ai sensi dell'art. 61 del RGPD, sempre con riferimento al settore di internet e delle comunicazioni elettroniche, si rileva che esse hanno nella loro totalità riguardato richieste di confronto su questioni concernenti profili (di carattere generale) interpretativi o applicativi del RGPD.

12 Il trattamento dei dati personali da parte di movimenti politici e associazioni

L'Autorità ha portato a conclusione la complessa istruttoria avviata nell'agosto 2017 in occasione del *data breach* relativo ad alcuni siti web connessi al Movimento 5 Stelle e che aveva coinvolto un elevato numero di cittadini iscritti ed attivi su tali piattaforme informatiche (cfr. Relazione 2017, p. 107 e Relazione 2018, p. 116). Al riguardo, l'effettivo adempimento delle diverse e numerose prescrizioni impartite dal Garante con il primo provvedimento del 21 dicembre 2017, n. 548 (doc. web n. 7400401) ha comportato un'articolata e progressiva attività di implementazione tecnologica da parte del titolare del trattamento. Tale attività, per la sua delicatezza, è stata anche oggetto di verifica (non solo di tipo documentale, ma anche attraverso accertamenti *in loco*) da parte dell'Autorità che, con il provvedimento 4 aprile 2019, n. 83 (doc. web n. 9101974), ha formulato le sue considerazioni conclusive.

Il Garante, pur ritenendo che le attività poste in essere abbiano comportato un significativo innalzamento dei livelli di sicurezza dei trattamenti effettuati nell'ambito dei siti web oggetto del citato provvedimento del 21 dicembre 2017, ha comunque rilevato il persistere di alcune importanti vulnerabilità in relazione alle quali, in base ai poteri attribuiti dal RGPD, è intervenuta rispetto a due ordini di profili. Da un lato, fissando termini ulteriori per l'adempimento, ha prescritto nei confronti dell'Associazione Movimento 5 Stelle e dell'Associazione Rousseau (quali, rispettivamente, titolare e responsabile del trattamento) l'adeguamento e la rivisitazione dei sistemi di sicurezza informatica adottati nonché, tenuto conto dell'importanza e della delicatezza della "piattaforma Rousseau" per la partecipazione democratica dei cittadini alle scelte politiche, l'effettuazione di una valutazione d'impatto sulla protezione dei dati, con specifico riferimento al sistema di *e-voting*. Dall'altro, avendo accertato rispetto ad alcune carenze nei sistemi di sicurezza la violazione dell'art. 32 del RGPD, ha ingiunto all'Associazione Rousseau il pagamento di una somma a titolo di sanzione amministrativa.

Sulla base degli elementi informativi e della documentazione fatta pervenire dai soggetti coinvolti, l'Autorità ha quindi svolto, nella seconda parte dell'anno, un'ulteriore attività di verifica dell'effettivo adempimento delle prescrizioni di cui al citato provvedimento 4 aprile 2019, n. 83, dalla quale è emersa una sostanziale implementazione delle misure di sicurezza impartite nonché un incremento dei relativi standard di sicurezza: di qui la chiusura del procedimento (cfr. nota 5 dicembre 2019).

Come già rappresentato in passato (cfr. Relazione 2018, p. 116), con provvedimento 10 gennaio 2019, n. 3 (doc. web n. 9082416), il Garante si è pronunciato nei confronti del Partito democratico - Coordinamento cittadino di Firenze che aveva subìto un'intrusione a danno dei propri sistemi informatici con conseguente violazione dei dati personali di circa 600 iscritti. Con il citato provvedimento l'Autorità, nel valutare le misure di sicurezza adottate e il ruolo svolto dalla società della cui infrastruttura tecnica il Pd Firenze si era avvalso, ha rilevato che la stessa avrebbe dovuto essere designata quale responsabile del trattamento e che tale mancata designazione ha configurato l'illiceità del trattamento; ciò in ragione dell'avvenuta comunicazione dei dati personali degli iscritti a un soggetto terzo, in mancanza del consenso degli interessati. Successivamente, a conclusione del procedimento sanzionatorio avviato secondo le previgenti disposizioni del Codice, il Garante, con

12

ordinanza del 31 ottobre 2019, n. 204 (doc. web n. 9207876), ha riconosciuto l'illiceità del trattamento per violazione dell'art. 26 del Codice e ha comminato la relativa sanzione amministrativa pecuniaria.

13 La protezione dei dati personali nel rapporto di lavoro privato e pubblico

13.1. *La protezione dei dati nell'ambito del rapporto di lavoro privato tra vecchia e nuova disciplina*

Anche in relazione ai trattamenti di dati personali effettuati nell'ambito del rapporto di lavoro, l'Autorità ha continuato a dare corso agli adempimenti previsti dal RGPD e dalla disciplina di adeguamento del Codice (contenuta nel decreto legislativo n. 101/2018) nonché a fornire chiarimenti ai soggetti coinvolti dall'applicazione delle disposizioni in materia di protezione dei dati (titolari, interessati, associazioni di categoria e rappresentative di interessati) sulle novità normative, in particolare con riferimento al trattamento dei dati biometrici e dei dati giudiziari (v., relativamente a tale ultima tipologia di dati, Relazione 2018, p. 127).

Il trattamento dei dati biometrici è ora sottoposto a garanzie più rigorose rispetto al passato. Infatti l'art. 9, par. 1, del RGPD ha inserito i dati biometrici nel novero dei dati "particolari" per i quali vige un generale divieto di trattamento. Esso può essere superato solo qualora ricorrano alcune tassative condizioni di liceità che, ove il trattamento avvenga nell'ambito del rapporto di lavoro, consistono nella necessità di "assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. *b*), e cons. da 51 a 53, del RGPD).

Allo stato sono espressamente previste dal legislatore nazionale due ipotesi di trattamento di dati biometrici nel contesto del rapporto di lavoro. In primo luogo, l'art. 2-*septies*, comma 7, del Codice consente il trattamento dei dati biometrici nell'ambito dell'accesso fisico e logico ai dati da parte di soggetti autorizzati; merita evidenziare che non rientrano in tale ambito i trattamenti effettuati per finalità di controllo dell'autenticazione all'accesso ad aree particolari e riservate, così come quelli finalizzati alla rilevazione della presenza in servizio nell'ambito del lavoro privato.

La seconda ipotesi riguarda esclusivamente il lavoro pubblico. La legge 19 giugno 2019, n. 56, recante interventi per la concretezza delle azioni delle pp.aa. e la prevenzione dell'assenteismo (in relazione alla quale non è stata adottata la necessaria normativa secondaria di attuazione) ha infatti previsto l'utilizzo di sistemi biometrici per finalità di verifica dell'osservanza dell'orario di lavoro. Al riguardo, come già anticipato, il Garante ha manifestato riserve sulla compatibilità di tale disciplina rispetto ai principi e alle disposizioni in materia di tutela dei dati personali sia in sede di audizione del Presidente del Garante nel corso dell'*iter* legislativo – presso la Commissione Lavoro pubblico e privato, previdenza sociale del Senato, 27 novembre 2018 (doc. web n. 9064421) e presso le Commissioni riunite Affari costituzionali e Lavoro della Camera dei deputati, 6 febbraio 2019 (doc. web n. 9080870) –, sia nel parere reso sullo schema di d.P.C.M. concernente la disciplina di attuazione della disposizione di cui all'art. 2, l. 19 giugno 2019, n. 56 (provv. 19 settembre 2019, n. 167, doc. web n. 9147290; v. già il parere su uno schema di

13

disegno di legge recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo", 11 ottobre 2018, n. 464, doc. web n. 9051774) (cfr. par. 2.2 n. 14).

In proposito l'Autorità ha avviato i lavori per la predisposizione del provvedimento che individua le misure di garanzia ex art. 2-*septies* del Codice relativamente al trattamento, nell'ambito lavorativo, di dati biometrici e di dati relativi allo stato di salute.

Il Garante ha poi continuato ad occuparsi dei trattamenti effettuati mediante la posta elettronica aziendale ed altri dispositivi tecnologici utilizzati nell'ambito del rapporto di lavoro, indicando le condizioni per conformare i trattamenti ai principi di protezione dei dati (cfr. *infra* par. 13.3).

13.2. *Il trattamento di categorie particolari di dati nell'ambito del rapporto di lavoro: dall'autorizzazione generale al provvedimento prescrittivo del Garante ex art. 21, d.lgs. n. 101/2018*

Nel quadro degli adempimenti attribuiti al Garante dalla disciplina di adeguamento del Codice al RGPD e, in particolare, in base a quanto stabilito dall'art. 21, d.lgs. n. 101/2018, con provvedimento di carattere generale, l'Autorità ha portato a termine (cfr. già Relazione 2018, p. 119 s.) il procedimento con il quale sono state individuate le prescrizioni contenute nelle autorizzazioni generali riferite ai trattamenti di categorie particolari di dati (ora elencati nell'art. 9, par. 1, del RGPD e nel sistema previgente definiti dati sensibili) effettuati nell'ambito del rapporto di lavoro, relative alle situazioni di trattamento di cui agli artt. 6, par. 1, lett. *c*) ed *e*), 9, par. 2, lett. *b*), e 4 nonché al Capo IX del RGPD, risultate compatibili con le disposizioni comunitarie e il decreto che ha novellato il Codice, provvedendo altresì al loro aggiornamento (provv. 13 dicembre 2018, n. 497, doc. web n. 9068972; v. anche Relazione 2018, pp. 119 e 120). Lo schema di provvedimento, sottoposto a consultazione pubblica, è stato definitivamente adottato con provvedimento 5 giugno 2019, n. 146 (doc. web n. 9124510).

Premesso che nel quadro normativo delineato dal RGPD i trattamenti dei dati personali nel contesto lavorativo sono disciplinati unitariamente, sia se effettuati da datori di lavoro pubblici che privati (cfr. artt. 88 e 9, par. 2, lett. *b*), del RGPD), il provvedimento prescrittivo definisce le "garanzie appropriate" richieste dall'art. 9, par. 2, lett. *b*), del RGPD per i trattamenti di categorie particolari di dati effettuati dai soggetti che a vario titolo trattano dati nell'ambito del rapporto di lavoro e nella fase pre-assuntiva.

Nell'ordinamento vigente il trattamento di categorie particolari di dati personali non fondato su uno dei presupposti indicati dall'art. 9, par. 2, del RGPD è vietato. I trattamenti per finalità di gestione del rapporto di lavoro (anche successivamente all'interruzione dello stesso) o in fase pre-assuntiva possono essere effettuati solo in quanto necessari per l'adempimento di obblighi previsti da leggi e regolamenti oppure da un contratto collettivo nei limiti previsti dall'ordinamento (v. art. 9, par. 2, lett. *b*), del RGPD). Allo stato, il trattamento di dati particolari contenuti nei *curricula* di candidati può essere quindi effettuato solo in presenza del consenso esplicito dell'interessato (v. art. 9, par. 2, lett. *a*), del RGPD).

Il sistema prevede che, in ogni caso, restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa dell'UE che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali. Considerato che il datore di lavoro tratta i dati personali nel rispetto delle disposizioni nazionali "più specifi-

che per assicurare la protezione dei diritti e delle libertà" (art. 88 del RGPD), deve essere osservato quanto stabilito dall'art. 113 del Codice che fa salvo l'art. 8, l. 20 maggio 1970, n. 300 (in base al quale il datore di lavoro non può, ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore), e l'art. 10, d.lgs. 10 settembre 2003, n. 276 (che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, all'affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute e ad eventuali controversie con i precedenti datori di lavoro, nonché di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo). In proposito rileva altresì quanto previsto dall'art. 15, l. 20 maggio 1970, n. 300 (che dispone la nullità di patti o atti "diretti a fini di discriminazione politica, religiosa, razziale, di lingua o di sesso, di handicap, di età o basata sull'orientamento sessuale o sulle convinzioni personali") e dall'art. 6, l. 5 giugno 1990, n. 135 (che vieta ai datori di lavoro lo svolgimento di indagini volte ad accertare, nei dipendenti o in persone prese in considerazione per l'instaurazione di un rapporto di lavoro, l'esistenza di uno stato di sieropositività) nonché dalle altre norme in materia di pari opportunità o volte a prevenire discriminazioni.

Si segnala che in occasione della predisposizione del provvedimento di carattere generale, il Garante ha precisato la portata di alcune prescrizioni già contenute nella precedente autorizzazione n. 1/2016 e ne ha introdotte di nuove (alla luce del potere attribuitogli dal legislatore di disporre aggiornamenti), attingendo alla casistica dei provvedimenti adottati nel tempo in materia. In particolare, è stato chiarito che il trattamento di categorie particolari di dati effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, posto che una diversa interpretazione che consentisse di prendere in considerazione anche astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento (v. punto 1.3, lett. *d*), provv. 5 giugno 2019, n. 146, doc. web n. 9124510).

Con riferimento al trattamento di dati che rivelano le opinioni politiche, è stato stabilito che in caso di partecipazione di dipendenti ad operazioni elettorali in qualità di rappresentanti di lista, in applicazione del principio di necessità, il datore di lavoro non deve trattare, nell'ambito della documentazione da presentare al fine del riconoscimento di benefici di legge, dati che ne rivelino le opinioni politiche (ad es., non deve essere richiesto il documento che designa il rappresentate di lista essendo allo scopo sufficiente la certificazione del presidente di seggio; v. punto 1.4.2, lett. *c*), provv. 5 giugno 2019, n. 146).

Infine, sono state fornite prescrizioni specifiche relative alle modalità del trattamento di tale categoria di dati, precisando che in occasione dell'utilizzo di forme di comunicazione individualizzate nei confronti dell'interessato, anche avvalendosi di personale autorizzato, qualora si proceda alla trasmissione del documento cartaceo, questo dovrà essere trasmesso, di regola, in plico chiuso, salva la necessità per il datore di lavoro di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto (v. punto 1.5, lett. *b*), provv. 5 giugno 2019, n. 146). In caso di trasmissione di documenti contenenti categorie particolari di dati ad altri uffici o funzioni interne che risultino in concreto legittimati a conoscerli in base

13

alle rispettive attribuzioni, è necessario verificare che la trasmissione riguardi esclusivamente le informazioni necessarie allo svolgimento della funzione, astenendosi dall'allegare, se non strettamente indispensabile, documentazione integrale o stralci di documentazione non pertinente e non necessaria (v. punto 1.5, lett. *c*), provv. 5 giugno 2019, n. 146).

Come già stabilito in alcuni provvedimenti dell'Autorità, è stato altresì espressamente prescritto che, qualora per concrete ragioni organizzative si proceda a mettere a disposizione i turni di servizio di una pluralità di colleghi interessati (ad es., mediante affissione in bacheca), il datore di lavoro non deve esplicitare, anche attraverso l'uso di acronimi o sigle, le causali dell'assenza dal servizio dalle quali sia possibile conoscere categorie particolari di dati riferiti a soggetti identificabili (es. permessi sindacali o dati relativi alla salute) (v. punto 1.5, lett. *d*), provv. 5 giugno 2019, n. 146).

La violazione delle prescrizioni contenute nel provvedimento generale è soggetta alla sanzione amministrativa di cui all'art. 83, par. 5, del RGPD (ex art. 21, comma 5, d.lgs. n. 101/2018).

13.3. *Controlli sulla posta elettronica aziendale successivamente alla cessazione del rapporto di lavoro*

Con un reclamo è stato lamentato il persistente funzionamento, cessato il rapporto di lavoro, di un *account* di posta elettronica aziendale di tipo individualizzato assegnato ad un lavoratore. Accertata la fondatezza del reclamo – posto che per circa un anno e sette mesi il titolare del trattamento ha avuto accesso alle comunicazioni pervenute, tramite reindirizzamento automatico delle stesse ad altro *account*, provvedendo a cancellarlo solo a seguito di diffida presentata dal reclamante –, il Garante ha ritenuto illecito il trattamento. Peraltro, è stato constatato che tale trattamento è avvenuto in assenza di alcuna informativa predisposta dal titolare del trattamento e, quindi, senza che gli interessati fossero stati informati in merito alle specifiche modalità dei trattamenti effettuati sugli *account* loro assegnati. Sia il trattamento effettuato nei confronti del reclamante sia la prassi aziendale della società non sono stati quindi ritenuti conformi ai principi di liceità, necessità e proporzionalità; in considerazione di tali violazioni il trattamento – non più in essere al momento dell'adozione del provvedimento – è stato dichiarato illecito e il titolare del trattamento è stato ammonito sulla necessità di conformare i trattamenti effettuati sugli *account* di posta elettronica aziendale dopo la cessazione del rapporto di lavoro alle disposizioni e ai principi in materia di protezione dei dati personali. Il Garante, richiamato quanto enunciato nelle linee guida per posta elettronica e internet (provv. 1° marzo 2007, n. 13, doc. web n. 1387522), ha affermato che "il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i *file* allegati – riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali" e che la trasposizione di tale principio in ambito lavorativo comporta la possibilità che il lavoratore – o terzi soggetti coinvolti – possano vantare una legittima aspettativa di confidenzialità rispetto ad alcune forme di comunicazione, anche nel caso in cui venga a cessare il rapporto di lavoro. Ha pertanto intimato al datore di lavoro di rimuovere gli *account* di posta elettronica aziendale riconducibili a persone identificate o identificabili dopo la cessazione del rapporto di lavoro, previa disattivazione degli stessi e contestuale adozione di sistemi

automatici volti ad informare i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento, provvedendo altresì ad adottare misure idonee ad impedire la visualizzazione di messaggi in arrivo durante il periodo in cui tale sistema automatico è in funzione (provv. 20 dicembre 2019, n. 216, doc. web n. 9215890).

13.4. *Il trattamento di dati dei dipendenti effettuato mediante dispositivi tecnologici indossabili*

All'esito di un'attività di controllo avviata d'ufficio dall'Autorità a seguito della pubblicazione di notizie di stampa è emerso che, nell'ambito dello svolgimento del servizio di spazzamento su strada svolto per conto della concessionaria dei servizi ambientali di un comune, una società ha attivato un sistema basato sul trattamento dei dati dei lavoratori effettuato mediante dispositivi tecnologici indossabili (sul polso, tipo braccialetto), idonei ad effettuare la lettura di etichette elettroniche (*tag*) mediante tecnologia Rfid ed altresì dotati di funzionalità di localizzazione geografica mediante sistema Gps.

Diversamente da quanto rappresentato dalla società, nel corso del procedimento è stato verificato che i dati trattati dal sistema erano riferiti ad interessati identificabili, sussistendo la possibilità di individuare il dipendente grazie alla rilevazione dei *tag* e della relativa localizzazione geografica mediante Gps attraverso il raffronto con altri dati raccolti (es. turni di lavoro).

In occasione di diverse interlocuzioni con il titolare del trattamento, l'Autorità ha preso atto che, secondo quanto dichiarato, la società si era limitata ad avviare la sperimentazione del sistema senza raccogliere e memorizzare alcun dato. Inoltre si è preso atto che, successivamente all'avvio del procedimento, l'azienda aveva provveduto a sottoscrivere un accordo ai sensi dell'art. 4, comma 1, l. 20 maggio 1970, n. 300 (la cui osservanza costituisce condizione di liceità del trattamento ai sensi dell'art. 114 del Codice), in base al quale la funzionalità di localizzazione sarà attivata al massimo per un turno di lavoro a settimana. Tale previsione è stata ritenuta conforme ai principi di necessità e proporzionalità in relazione alle finalità perseguite (v. art. 5, par. 1, lett. *c*), del RGPD).

L'Autorità ha poi ritenuto necessaria l'individuazione da parte della società, di una tipologia di dispositivo, anche per le sue caratteristiche esteriori, non lesivo della dignità del dipendente e che comunque non risulti tale nella percezione degli interessati, conformemente peraltro a quanto stabilito nel predetto accordo stipulato in base alla disciplina giuslavoristica in materia di controlli a distanza.

In relazione alle caratteristiche del sistema che si intende adottare, è stata altresì rammentata al titolare del trattamento la necessità di individuare i tempi di conservazione dei registri contenenti i turni di lavoro, la zona di spazzamento e l'identità dei lavoratori entro i limiti strettamente necessari rispetto alla finalità perseguita (cd. consuntivazione dell'attività svolta), di indicare preventivamente e tassativamente i casi nei quali si renderà necessario interconnettere le informazioni al fine di ricostruire fatti oggetto di eventuale contestazione da parte della stazione appaltante nonché di adottare misure organizzative e tecnologiche per mantenere distinte le basi di dati qualora non sia più necessaria l'interconnessione per la ricostruzione di fatti oggetto di contestazione, ma sia comunque necessaria l'ulteriore conservazione dei registri dei turni per fini amministrativi. Si è altresì evidenziato che, ai sensi dell'art. 35 del RGPD, la società dovrà effettuare una valutazione di impatto sulla protezione dei dati alla luce delle concrete caratteristiche del sistema

13

tecnologico che intende adottare (nota Segretario generale 28 febbraio 2019, doc. web n. 9094427).

13.5. *Il trattamento di dati contenuti in una relazione investigativa relativi ad un terzo*

A seguito di reclamo, il Garante si è pronunciato in merito alla liceità del trattamento posto in essere da un datore di lavoro avente ad oggetto i dati (riferiti ad un soggetto diverso da quello sottoposto ad investigazione), tratti dai dispositivi informatici e mobili assegnati ad una propria dipendente, contenuti in una relazione investigativa commissionata al fine di acquisire elementi di prova dell'uso improprio dei dispositivi stessi da parte di quest'ultima. Premesso che l'accertamento dell'Autorità ha riguardato esclusivamente il trattamento dei dati riferiti al reclamante (soggetto terzo rispetto al rapporto di lavoro in questione), è risultato che tali dati, in particolare le immagini, ritraevano l'interessato in contesti di vita privata ed intima, e che la relazione investigativa era stata consegnata, in versione integrale, a diversi esponenti di vertice del soggetto datoriale.

L'Autorità ha ritenuto non conforme ai principi di liceità, proporzionalità e non eccedenza il trattamento effettuato (v., nel testo previgente, gli artt. 3 e 11, comma 1, lett. *a*) e *d*), del Codice) ed ha ammonito il datore di lavoro in ordine alla necessità di conformare i trattamenti di dati personali, anche per la finalità di tutela dei propri diritti in giudizio, ai principi ed alle disposizioni in materia di protezione dei dati personali. Il fine per il quale sono stati trattati i dati oggetto di reclamo poteva, infatti, essere utilmente perseguito provvedendo ad oscurare alcune immagini di natura privatissima o, quantomeno, a non rendere riconoscibili i terzi presenti nelle immagini riprodotte tratte dai dispositivi oggetto di relazione tecnica, considerata anche la necessità di tutelare la dignità del reclamante oltre che della dipendente. Si sarebbe dovuto, per tale motivo, fare in modo che la documentazione a supporto dell'avvio dell'azione disciplinare nei confronti della dipendente contenesse esclusivamente i dati a tal fine necessari. Il trattamento, inoltre, è stato effettuato nei confronti del reclamante in assenza di idonei criteri di legittimazione al trattamento: non era, infatti, "necessario" ai sensi del previgente art. 24, comma 1, lett. *f*), del Codice e non è stato rispettato quanto enunciato dall'art. 26, par. 4, lett. *c*), del Codice in base al quale, in relazione alla finalità di fare valere un diritto in giudizio, il titolare può trattare i dati sensibili solo se necessari al perseguimento della finalità nonché rispettando il cd. principio del pari rango ("Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile") (provv. 2 ottobre 2019, n. 182).

13.6. *Compiti e responsabilità dei professionisti che effettuano trattamenti di dati personali su incarico del datore di lavoro*

Con nota 22 gennaio 2019 indirizzata al Consiglio nazionale dei consulenti del lavoro, l'Autorità ha fornito alcuni chiarimenti, sollecitati dallo stesso organismo rappresentativo della categoria e da numerosi professionisti (commercialisti, avvocati, consulenti legali), in ordine ad alcuni aspetti affrontati dalla circolare 23 luglio 2018, n. 1150, adottata dal medesimo Consiglio nazionale, con particolare riferimento alla individuazione del ruolo di titolare, responsabile o contitolare relativamente alle attività svolte da tale categoria di professionisti.

Una volta sottolineato che il RGPD non ha introdotto innovazioni sostanziali

rispetto alle disposizioni previgenti relativamente alle definizioni di titolare del trattamento e responsabile del trattamento (v. art. 4, nn. 7) e 8), RGPD), l'Autorità ha chiarito, che mentre in relazione alle attività di trattamento che riguardano dati dei propri dipendenti e dei propri clienti il consulente del lavoro (o altro professionista) determina puntualmente le finalità e i mezzi del trattamento sulla base dei criteri di legittimazione applicabili (contratto, discipline di settore applicabili), operando pertanto in qualità di titolare del trattamento, nel caso in cui effettui attività "esternalizzate" dal datore di lavoro per conto di quest'ultimo riveste necessariamente il ruolo di responsabile del trattamento. L'affidamento a professionisti qualificati dell'effettuazione di segmenti di attività relativi alla gestione del rapporto di lavoro (dall'elaborazione delle buste paga agli adempimenti previsti dalle discipline previdenziali e assistenziali, dalla gestione degli obblighi in fase di assunzione a quelli relativi al fine rapporto) comporta il conferimento al professionista di una pluralità di dati, anche afferenti a categorie particolari, che nell'ambito del rapporto di lavoro possono essere raccolti e successivamente trattati in base a quanto previsto dalle norme di legge e di regolamento applicabili e in base al contratto collettivo di lavoro (v. artt. 6, 9, par. 2, lett. *b*), e 88 del RGPD). Pertanto il professionista tratta le informazioni relative ai lavoratori (dipendenti dei propri clienti) utilizzando i dati raccolti dal datore di lavoro nel perseguimento di finalità legittime nonché in base ai criteri e alle direttive da questo impartite relativamente alla gestione del rapporto di lavoro sottostante. Tale ricostruzione è confermata anche dalla normativa di settore relativa all'attività del consulente del lavoro (l. 11 gennaio 1979, n. 12, norme per l'ordinamento della professione di consulente del lavoro) laddove prevede che il consulente iscritto all'Albo dei consulenti del lavoro può assumere "gli adempimenti in materia di lavoro, previdenza ed assistenza sociale dei lavoratori dipendenti, quando non sono curati dal datore di lavoro, direttamente od a mezzo di propri dipendenti". Peraltro in capo al datore di lavoro, anche a seguito del conferimento dell'incarico e dell'eventuale consegna della documentazione necessaria al suo svolgimento, permane la responsabilità prevista dall'ordinamento in caso di violazione degli obblighi posti in materia di lavoro, previdenza ed assistenza sociale (v. art. 7, l. n. 12/1979).

L'incarico al consulente è affidato mediante la sottoscrizione di un "contratto o altro atto giuridico" stipulato dalle parti tenendo conto dei compiti in concreto affidati, del contesto, delle finalità e modalità del trattamento e non in base a modelli imposti unilateralmente. A sua volta il consulente potrà avvalersi di collaboratori di fiducia, che operino sotto la sua autorità, inquadrabili nella figura prevista all'art. 2-*quaterdecies* del Codice. Il consulente potrà altresì avvalersi di sub-responsabili qualora sia loro demandata "l'esecuzione di specifiche attività di trattamento per conto del titolare" (v. art. 28, par. 4, del RGPD); in tal caso il relativo atto di incarico deve essere autorizzato, anche in via generale, dal titolare.

Considerato che, rispetto al quadro previgente, l'art. 28 del RGPD ha precisato i compiti che possono essere attribuiti dal titolare al responsabile, individuando l'ambito delle rispettive responsabilità e gli obblighi di cooperazione cui è tenuto il responsabile, l'Autorità ha sottolineato che anche sul responsabile grava l'adempimento delle disposizioni poste in materia di misure di sicurezza (ex art. 32 del RGPD), in particolare per quanto riguarda la gestione dell'archivio. Infine è stato chiarito che al termine del rapporto professionale i dati contenuti negli archivi dovranno essere cancellati (oppure anonimizzati) e/o consegnati al titolare conformemente alle condizioni individuate nel contratto di affidamento dell'incarico (nota 22 gennaio 2019, doc. web n. 9080970).

13

13.7. *La limitazione dell'esercizio dei diritti dopo le modifiche al Codice*

In sede di decisione di un reclamo avente ad oggetto l'esercizio del diritto di accesso del lavoratore ai dati contenuti in una relazione investigativa commissionata dal datore di lavoro ad un'agenzia privata nel periodo in cui il reclamante era in malattia (in relazione a fatti avvenuti prima dell'applicazione del RGPD), il Garante ha fornito alcuni chiarimenti sulle disposizioni che disciplinano la limitazione dei diritti degli interessati in applicazione di quanto previsto dall'art. 23 del RGPD. Tale disposizione individua alcuni specifici requisiti che la disciplina nazionale deve indefettibilmente contenere laddove ponga limitazioni alla "portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34", in vista della salvaguardia, tra l'altro, della tutela "dei diritti e delle libertà altrui", sempre che tali limitazioni rispettino l'essenza dei diritti e delle libertà fondamentali e siano una misura necessaria e proporzionata in una società democratica.

A tale disposizione ha dato attuazione l'art. 2-*undecies* del Codice, in base al quale i diritti di cui agli artt. da 15 a 22 del RGPD non possono essere esercitati con richiesta al titolare del trattamento o con reclamo nel caso in cui, tra le altre ipotesi, "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". Anche relativamente a tale ipotesi il successivo comma 3 specifica che "i diritti […] sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'art. 23, par. 2, del RGPD. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato".

L'Autorità ha in proposito ritenuto che la disciplina in parola si pone in linea di continuità con quanto già stabilito dal previgente art. 8, comma 2, lett. *e*), del Codice in applicazione del quale il Garante ha ritenuto – avuto riguardo alle circostanze del caso concreto – di accogliere le istanze di limitazione dell'esercizio del diritto di accesso "limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per l'esercizio del diritto in sede giudiziaria" (provv. ti 21 gennaio 2016, n. 11, doc. web n. 4715667 e 13 dicembre 2012, n. 412, doc. web n. 2273474). Nel caso considerato, posto che l'istanza di accesso è stata presentata in data successiva alla conclusione del procedimento disciplinare, in fase precontenziosa, e che, dato il particolare regime probatorio del processo del lavoro – che prevede l'onere della prova a carico del datore di lavoro –, la comunicazione dei dati trattati nell'ambito dell'attività investigativa avrebbe comportato un "pregiudizio effettivo e concreto […] all'esercizio di un diritto in sede giudiziaria", è stata ritenuta applicabile la limitazione all'esercizio del diritto prevista dal richiamato art. 2-*undecies* del Codice. Il Garante ha comunque precisato che la limitazione è circoscritta al periodo strettamente necessario ad evitare un pregiudizio all'esercizio del diritto da parte del titolare. Pertanto, fermi restando i poteri del giudice del lavoro in ordine alla produzione ed esibizione di atti e documenti nel corso del procedimento giurisdizionale, una volta venute meno le ragioni del pregiudizio nessun ostacolo potrà essere frapposto all'esercizio del diritto previsto dall'art. 15 del RGPD (provv. 31 gennaio 2019, n. 20, doc. web n. 9086480).

13

App

13.8. *Il trattamento di dati di dipendenti pubblici e di utenti mediante il sistema di prenotazione e gestione dei servizi*

Nell'ambito di verifiche compiute in relazione sull'uso delle *app* nel settore pubblico, il Garante ha adottato un provvedimento nei confronti di Roma Capitale in relazione ai trattamenti di dati personali dei dipendenti e degli utenti posti in essere mediante il sistema denominato "TuPassi", fornito da una società terza, per la gestione delle prenotazioni dei servizi erogati al pubblico e delle code allo sportello (cfr. par. 4.6). Il sistema utilizzato dall'Ente costituisce, nella ricostruzione effettuata dal Garante, uno strumento per perseguire il miglioramento dell'efficienza ed economicità dell'attività amministrativa attraverso la gestione delle prenotazioni degli appuntamenti dei servizi erogati allo sportello e delle attese; di conseguenza, i trattamenti di dati personali effettuati possono essere considerati necessari per l'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. *e*), del RGPD) contemplato dall'ordinamento (art. 97 Cost.; art. 1, l. n. 241/1990; artt. 1, 10 e 11, d.lgs. n. 165/2001). Tuttavia, dalle risultanze istruttorie è emerso che il titolare del trattamento effettuava, mediante detto sistema, operazioni di trattamento di dati personali riferiti ad utenti e dipendenti non conformi alla disciplina in materia di protezione dei dati personali, con riguardo sia al quadro normativo vigente al momento della messa in funzione del sistema (risalente al 2015), sia a quello delineato dal RGPD e dal decreto legislativo n. 101/2018. In particolare, è stato accertato che in nessuna delle fasi di prenotazione/erogazione del servizio gli utenti ricevevano informazioni circa i trattamenti dei dati personali loro riferiti effettuati dall'Ente. Analogamente, non è risultato essere stata resa ai dipendenti la dovuta informativa circa le modalità e le finalità delle operazioni di trattamento rese possibili dal sistema, né in forma individualizzata, a ciascun lavoratore, né con documenti informativi resi noti alla generalità dei dipendenti (artt. 5, par. 1, lett. *a*) nonché 13 e 14 del RGPD e, non diversamente, il previgente art. 13 del Codice; cfr. quanto stabilito in Corte EDU, Grande Camera, case of Bărbulescu v. Romania, ricorso n. 61496/08, 5 settembre 2017).

Peraltro, con riguardo alla funzione di estrazione di *report* e statistiche sull'erogazione dei servizi, il Garante ha precisato che tale trattamento avrebbe potuto integrare un controllo a distanza sui lavoratori da parte dell'Amministrazione ed ha al riguardo dichiarato che, nel perseguimento delle specifiche finalità, il trattamento debba avvenire nell'osservanza delle condizioni di garanzia prescritte dall'art. 4, comma 1, l. n. 300/1970 (accordo sindacale o autorizzazione pubblica), anche per effetto del rinvio operato dall'art. 114 del Codice, che costituisce condizione di liceità del trattamento dei dati personali (artt. 5 e 6 par. 1, lett. *c*), e 88, par. 2, del RGPD e 114 del Codice).

Inoltre la società fornitrice del sistema, che assicura anche il servizio di assistenza e manutenzione non aveva stipulato con l'Ente un accordo per la protezione dei dati personali. Il Garante sul punto ha chiarito che, ai fini del rispetto della normativa in materia di protezione dei dati personali, assume rilievo identificare con precisione i soggetti che, a diverso titolo, possono trattare i dati personali e definire chiaramente le rispettive attribuzioni, in particolare quella di titolare e di responsabile del trattamento (art. 4, par. 1, punto 7, del RGPD e, con riferimento ai trattamenti effettuati sino al 24 maggio 2018, artt. 28 e 29 del Codice). Atteso che le funzioni svolte dall'Ente per assicurare l'assistenza e la manutenzione del sistema comportano anche un trattamento di dati personali di cui lo stesso è titolare (dati personali dei dipendenti ed eventualmente degli utenti che non abbiano effettuato la prenotazione direttamente tramite i servizi della società fornitrice del sistema), il Garante

13

ha concluso che, anche sotto questo profilo, il trattamento dei dati personali non risulta conforme alla disciplina di riferimento (art. 29 del Codice in relazione ai trattamenti effettuati fino al 24 maggio 2018 e, successivamente, art. 28 del RGPD), dando luogo a una comunicazione illecita di dati personali (cfr. la nozione di "terzo" di cui all'art. 4, par. 1, punto 10, del RGPD; art. 2-*ter* del Codice).

Il Garante ha inoltre ritenuto che le misure tecniche e organizzative adottate dall'Ente non fossero adeguate agli specifici rischi connessi al trattamento; per tali ragioni, ha ingiunto al titolare di conformare il trattamento alle disposizioni menzionate del RGPD e del Codice e di adottare adeguate azioni correttive volte ad eliminare le criticità tecniche e organizzative (provv. 7 marzo 2019, n. 81, doc. web n. 9121890).

13.9. *Comunicazione di dati dei dipendenti a un ordine professionale*

È stato affrontato anche il tema della comunicazione, da parte del datore di lavoro, dei dati personali dei dipendenti per consentire agli ordini professionali l'esercizio delle funzioni disciplinari nei confronti di figure professionali per le quali sia richiesta l'iscrizione ad uno specifico albo.

Nel definire il procedimento – avviato ai sensi dell'art. 2-*ter*, comma 2, del Codice da un'azienda ospedaliera che aveva ricevuto da parte di un ordine interprovinciale delle professioni infermieristiche una richiesta di comunicazione di dati personali dei propri dipendenti in servizio con la qualifica di infermieri (nominativi e residenza) al fine di poter effettuare i controlli previsti dalla vigente normativa (cfr. d.lgs. del Capo provvisorio dello Stato 13 settembre 1946, n. 233, come modificato dalla l. 11 gennaio 2018, n. 3, ricostituzione degli ordini delle professioni sanitarie e per la disciplina dell'esercizio delle professioni stesse) – l'Ufficio ha ribadito che il Codice, come modificato dal decreto legislativo 10 agosto 2018, n. 101, prevede che la comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli di cui agli artt. 9 e 10 del RGPD, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, è ammessa se prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e di funzioni istituzionali e ad essa può darsi corso spirato il termine di quarantacinque giorni dalla comunicazione al Garante senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati (art. 2-*ter*, comma 2, del Codice).

Nel merito della questione sollevata, nel prendere atto che, in base alla disciplina di settore, l'onere di iscrizione all'albo incombe sul singolo professionista (cfr. art. 5, comma 2, d.lgs. CpS n. 233/1946, come modificato nel 2018) e che il quadro normativo applicabile prevede che gli ordini delle professioni sanitarie esercitino istituzionalmente poteri di vigilanza e disciplinari nei confronti di "tutti gli iscritti all'albo", ha concluso che, in tale quadro, non risultano attribuite agli ordini specifiche competenze per il compimento di generalizzate attività di ricerca e raccolta di informazioni personali riferite a soggetti diversi da coloro che abbiano già richiesto l'iscrizione all'albo.

Sotto diverso profilo – impregiudicate le specifiche responsabilità, anche sotto il profilo penale, che incombono su coloro che esercitino le professioni sanitarie in assenza di iscrizione all'albo, il cui accertamento è rimesso ordinariamente in capo ad altri organi pubblici – il datore di lavoro deve svolgere le necessarie verifiche sul possesso dei particolari requisiti previsti per l'accesso a specifici impieghi per finalità

di assunzione e nel corso dell'esecuzione del contratto di lavoro (cfr. art. 88, par. 1, del RGPD), nei limiti previsti dalle norme vigenti (ad es., artt. 43, 46 e 71, d.P.R. n. 445/2000) nonché consultando gli albi professionali che sono pubblici e reperibili anche *online*.

Per le citate ragioni, l'Ufficio ha concluso che non sussistono le condizioni necessarie a legittimare la preventiva e massiva comunicazione all'ordine professionale, da parte dell'azienda sanitaria datore di lavoro, dei dati personali relativi a tutto il personale infermieristico impiegato (cfr. nota 16 gennaio 2019, doc. web n. 9084551).

13.10. *Inconfigurabilità del silenzio-assenso nel procedimento di autorizzazione amministrativa all'installazione ed utilizzo di impianti audiovisivi dai quali possa derivare la possibilità di controllo a distanza dei lavoratori*

L'Ufficio ha fornito riscontro ad un quesito, formulato dal Ministero del lavoro e delle politiche sociali, in relazione ad un'istanza di interpello presentata dal Consiglio nazionale dei consulenti del lavoro, in merito alla formazione del silenzio assenso in caso di mancato riscontro, da parte dell'Ispettorato nazionale del lavoro, ad una richiesta di autorizzazione amministrativa all'installazione ed utilizzo di impianti audiovisivi o altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori.

L'Autorità, nel rilevare che l'art. 4 dello Statuto dei lavoratori considera esplicitamente illecita (e penalmente sanzionabile) l'installazione di impianti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di un controllo a distanza dei lavoratori in assenza delle previste procedure di garanzia, ha rilevato che, in relazione al procedimento di autorizzazione, la cui conclusione è fissata in 60 giorni (d.P.C.M. 22 dicembre 2010, n. 275, tabella B), non è prevista la formazione del silenzio assenso.

Peraltro, l'Ufficio ha chiarito che la procedura autorizzativa pubblica – che deve essere esperita dal datore di lavoro quando sia risultata infruttuosa quella condeterminata con le rappresentanze sindacali – costituisce (anche alla luce dei consolidati orientamenti della giurisprudenza) uno strumento di tutela sostanziale, attraverso il quale l'Ispettorato nazionale del lavoro, contemperando la richiesta del datore di lavoro con la necessità di preservare le libertà fondamentali e la dignità dei dipendenti, valuta, in concreto, la liceità di quanto richiesto, fornendo al datore di lavoro indicazioni e limitazioni circa le modalità e le condizioni di utilizzo di tali sistemi potenzialmente idonei ad effettuare un controllo a distanza dei lavoratori (nota 8 aprile 2019).

13.11. *I trattamenti di dati nell'ambito dell'acquisizione e gestione delle segnalazioni in materia di* whistleblowing

Il Garante ha adottato il parere sullo schema di linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro dell'Anac, ai sensi dell'art. 54-*bis*, comma 5, d.lgs. 30 marzo 2001, n. 165 (Tutela del dipendente pubblico che segnala illeciti), come modificato dall'art. 1, comma 2, l. n. 179/2017.

Il testo, già sottoposto a consultazione pubblica sul sito web dell'Anac, ha recepito le principali indicazioni fornite dall'Autorità nel corso di alcuni incontri tenutisi con i rappresentanti di Anac al fine di garantire il necessario coordinamento tra la disciplina di settore e il quadro normativo in materia di protezione dei dati personali

13

nell'ambito dalle procedure di acquisizione e gestione delle segnalazioni di presunti illeciti. Ciò anche alla luce della particolare tutela accordata dalla disciplina in materia di *whistleblowing* all'identità del segnalante e, in generale, degli specifici rischi per i diritti e le libertà degli interessati nel contesto lavorativo (art. 88 del RGPD).

In tale prospettiva, le linee guida – rivolte ai datori di lavoro in ambito pubblico, ma contenenti anche indicazioni per l'inoltro di segnalazioni da parte di dipendenti di imprese fornitrici di beni o servizi per la pubblica amministrazione – sostituiranno le precedenti linee guida adottate con la determinazione Anac del 28 aprile 2015, n. 6. Nella prospettiva promossa dal Garante e accolta dall'Anac, le linee guida individueranno le misure tecniche e organizzative di base che i titolari del trattamento devono adottare nell'ambito delle procedure informatiche per l'acquisizione e gestione delle segnalazioni, lasciando comunque agli stessi la definizione del proprio specifico modello di gestione delle segnalazioni, in coerenza con il principio di responsabilizzazione e i principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (artt. 5, parr. 1, lett. *f*), e 2, 24, 25 e 32 del RGPD).

Al fine di rafforzare la tutela che deve caratterizzare il riserbo sull'identità del segnalante e sulle informazioni che facilitano l'individuazione di fenomeni corruttivi nella p.a., il Garante, nel prendere atto del recepimento dei principali suggerimenti formulati durante i lavori – frutto anche degli esiti di un ciclo di attività ispettive condotte nel corso dell'anno che ha consentito di esplorare, presso alcuni fornitori di servizi informatici e titolari del trattamento, le principali funzionalità di alcuni tra gli applicativi per l'acquisizione e gestione delle segnalazioni più diffusamente impiegati nel settore pubblico (cfr. provv. 12 settembre 2019, n. 166, doc. web n. 9147297) –, ha comunque evidenziato alcuni profili di criticità, rispetto ai quali ha segnalato la necessità di integrare e modificare lo schema di linee guida.

Al fine di incrementare l'utilizzo di tale istituto, il Garante ha evidenziato l'opportunità che nelle linee guida vengano meglio circoscritte e definite le condotte oggetto di segnalazione, così da prevenire trattamenti di dati personali non sorretti da un'idonea base giuridica in quanto riferiti a casi non previsti dalla normativa anticorruzione. Si è altresì ritenuto indispensabile provvedere a specificare le modalità per l'esercizio dei diritti degli interessati nella prospettiva della tutela dell'identità del segnalante nonché, allo stesso scopo, a rafforzare le misure tecniche e organizzative, utilizzando, ad esempio, protocolli sicuri per la trasmissione dei dati, abilitando accessi selettivi ai dati contenuti nelle segnalazioni ed evitando che la piattaforma invii al segnalante notifiche sullo stato della pratica, in quanto tali messaggi potrebbero pregiudicare la riservatezza della segnalazione (provv. 4 dicembre 2019, n. 215, doc. web n. 9215763).

13.12. *Il trattamento di dati biometrici dei dipendenti pubblici per finalità di rilevazione delle presenze*

A seguito di numerosi quesiti pervenuti, anche in relazione all'*iter* normativo della legge 19 giugno 2019, n. 56 (recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo), il Garante ha fornito chiarimenti in merito al trattamento dei dati biometrici dei dipendenti per finalità di rilevazione delle presenze, muovendo dal particolare rilievo attribuito dal RGPD ai dati biometrici, ricompresi ora nel novero delle categorie particolari di dati (cfr. art. 9, par. 1, del RGPD).

Entro tale cornice, il trattamento di dati biometrici (di regola vietato) è consen-

tito in ambito lavorativo (sia pubblico che privato) solo quando sia "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro […], nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. *b*), del RGPD; v. pure, art. 88, par. 1, e cons. 51-53, del RGPD). Il quadro normativo vigente prevede altresì che il trattamento, per poter essere lecitamente posto in essere, debba avvenire nel rispetto delle "ulteriori condizioni, comprese limitazioni" (cfr. art. 9, par. 2, lett. *b*), e par. 4, del RGPD) che, nell'ordinamento nazionale, consistono anche nella "conformità alle misure di garanzia disposte dal Garante", ai sensi dell'art. 2-*septies* del Codice.

Con specifico riguardo al settore del pubblico impiego, è stato precisato che è tuttora in corso l'*iter* di approvazione dello schema di d.P.C.M. recante le modalità attuative della legge 19 giugno 2019, n. 56, in relazione all'utilizzo di sistemi di rilevazione di dati biometrici per finalità di rilevazione delle presenze.

Su tale schema di regolamento e, prima ancora, sullo schema di disegno di legge, il Garante ha reso il proprio parere, ai sensi degli artt. 36, par. 4 e 57, par. 1, lett. *c*), del RGPD, evidenziando criticità con riguardo alla proporzionalità delle misure introdotte con il menzionato intervento normativo. In generale, è stato rilevato che le disposizioni risultano incompatibili con il canone di proporzionalità di cui all'art. 52 della CDFUE in quanto prospettano l'introduzione sistematica, generalizzata e indifferenziata per tutte le pp.aa. di sistemi di rilevazione biometrica delle presenze, in ragione dei vincoli posti dall'ordinamento europeo sul punto, a motivo dell'invasività di tali forme di verifica e delle implicazioni derivanti dalla particolare natura del dato (cfr. provv. 19 settembre 2019, n. 167, doc. web n. 9147290; v. già, audizione del Presidente dell'Autorità nell'ambito dell'esame del disegno di legge C. 1433 recante interventi per la concretezza delle azioni delle pp.aa. e la prevenzione dell'assenteismo, doc. web n. 9080870 e provv. 11 ottobre 2018, n. 464, doc. web n. 9051774).

In merito all'intervento regolatorio in questione, i rilievi formulati dal Garante non possono essere superati neanche dall'eventuale consenso dei dipendenti che, peraltro, non costituisce un valido presupposto di liceità per il trattamento dei dati personali in ambito lavorativo, indipendentemente dalla natura pubblica o privata del datore di lavoro (cons. 43; art. 4, punto 11 e art. 7, parr. 3 e 4, del RGPD; v. l'orientamento consolidato in sede europea, Gruppo Art. 29, parere 2/2017 sul trattamento dei dati sul posto di lavoro, WP 249, p. 7 e 26, e le linee guida sul consenso ai sensi del Regolamento UE 2016/679, WP 259, adottate il 28 novembre 2017 e modificate il 10 aprile 2018).

Per tali ragioni è stato rappresentato che, allo stato, il quadro normativo non consente al datore di lavoro il trattamento dei dati biometrici dei dipendenti per la finalità di rilevazione delle presenze (artt. 5, par. 1, lett. *a*) e *c*), art. 6, lett. *c*), nonché art. 9, par. 2, lett. *b*), e par. 4, del RGPD) (nota 24 ottobre 2019) (parr. 2.2 e 3.1.4).

13.13. *Il trattamento di dati nell'ambito di procedimenti disciplinari e delle procedure di protocollazione degli atti*

L'Ufficio ha definito alcuni reclami concernenti il trattamento di dati personali dei dipendenti nell'ambito di procedimenti disciplinari oggetto di non corrette procedure di protocollazione dei relativi atti.

13

In particolare, in un caso un dipendente di un ente locale aveva lamentato che una nota contenente una segnalazione, da cui avrebbe avuto origine il procedimento disciplinare nei propri confronti, sarebbe stata protocollata "senza gli attributi di riservatezza, così da essere disponibile ad una pluralità di soggetti" e che, in ragione dell'ampia circolazione che il documento avrebbe avuto all'interno dell'amministrazione, la stessa sarebbe stata, successivamente, oggetto di scambio tra il personale dell'ente attraverso messaggi di posta elettronica e *social network*.

All'esito dell'attività istruttoria, il Garante ha ribadito che l'amministrazione, in qualità di datore di lavoro, può trattare i dati personali dei dipendenti che siano necessari per dare esecuzione al rapporto di lavoro o per attuare previsioni di legge e adempiere obblighi correlati alla gestione del rapporto di lavoro mediante il personale incaricato o comunque autorizzato e debitamente istruito in merito all'accesso ai dati (art. 30 del Codice, vedi anche, artt. 4, par. 10, 29, 32, par. 4, del RGPD). Il Garante ha inoltre chiarito, anche con provvedimenti di carattere generale i cui principi si confermano tuttora validi, che devono essere prescelte soluzioni che permettano di svolgere le funzioni di gestione dei dati dei lavoratori in modo da eliminare ogni occasione di non necessaria conoscibilità degli stessi, anche adottando cautele particolari per evitare l'indebita circolazione di informazioni personali in capo a soggetti non autorizzati, non solo verso l'esterno, ma anche all'interno dei contesti lavorativi (cfr. punti 2, 4, 5.1 e 5.3 delle linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico del 14 giugno 2007, doc. web n. 1417809). In proposito è stato chiarito che il personale "incaricato alle operazioni di trattamento deve essere debitamente istruito in ordine all'accesso e all'utilizzo delle informazioni personali di cui può venire a conoscenza nello svolgimento della propria prestazione lavorativa" (cfr. punti 2, 4, 5.1 e 5.3, linee guida cit.).

In tale quadro, anche nell'ambito dei trattamenti di dati personali effettuati mediante i sistemi informatici di gestione dei documenti, è necessario adottare procedure differenziate e/o riservate con riguardo, ad esempio, a tutti i documenti attinenti ai procedimenti disciplinari dei dipendenti nonché agli atti prodromici all'attivazione degli stessi, in ragione di informazioni delicate che possono essere contenute in tali atti (sul punto, v. anche alcune decisioni con le quali il Garante ha dichiarato illecito il trattamento dei dati personali dei dipendenti da parte di colleghi in ragione della scorretta configurazione del protocollo informatico: provvedimenti 11 ottobre 2012, n. 280, doc. web n. 2097560 e 12 giugno 2014, n. 298, doc. web n. 3318492).

Nel caso di specie, l'ente aveva specificato che la segnalazione, in quanto atto prodromico all'avvio del procedimento disciplinare, e quindi formalmente estranea allo stesso, non dovesse essere soggetta alla protocollazione riservata. Tuttavia, proprio tale mancata valutazione dello specifico contenuto della segnalazione, successivamente utilizzata per dare avvio al procedimento disciplinare a carico del reclamante, e la sua conseguente protocollazione senza gli attributi di riservatezza, ha reso accessibile il documento, contenente informazioni particolarmente delicate riferite ad un collega, ad una pluralità di altri dipendenti non autorizzati allo specifico trattamento, dando luogo a un illecito trattamento di dati personali (nota 26 settembre 2019).

In un altro caso, il reclamante aveva lamentato che, a seguito di un proprio esposto alla Procura generale della Corte dei conti in merito a presunte condotte illecite del comune presso il quale prestava servizio nella gestione dell'affidamento di incarichi a consulenti esterni, sarebbe stato attivato nei suoi confronti un procedimento culminato con l'adozione di una sanzione disciplinare. Ritenendo tale sanzione un atto ritorsivo, in violazione dell'art. 54-*bis*, d.lgs. n. 165/2001, il reclamante aveva

denunciato i predetti fatti all'Anac e, conformemente alla normativa vigente, anche all'Ispettorato per la Funzione pubblica presso la Presidenza del Consiglio dei ministri. A seguito delle verifiche effettuate, l'Ispettorato aveva trasmesso la nota contenente gli esiti dell'istruttoria, indirizzandola all'interessato e al segretario comunale, all'epoca Responsabile della prevenzione della corruzione e della trasparenza.

È stato al riguardo rilevato che il mancato rispetto delle procedure in sede di protocollazione avesse determinato la trasmissione, in copia, della nota in questione a un ufficio cui la comunicazione non era diretta (Servizio gestione del personale), nonché la possibilità che tutti i dirigenti comunali potessero consultare il documento, cagionando un illecito trattamento di dati personali del reclamante. In tale contesto l'Ufficio ha dato rilievo anche alla circostanza che il procedimento, cui la nota dell'Ispettorato della Funzione pubblica faceva riferimento, è disciplinato dalla specifica normativa in materia di tutela del dipendente che segnala illeciti di cui all'art. 54-*bis*, d.lgs. n. 165/2001 (cfr. par. 13.11), che prevede (anche nella versione anteriore alle modifiche intervenute per effetto dell'art. 1, comma 2, l. n. 179/2017) misure volte a proteggere l'identità del segnalante, allo scopo di prevenire l'adozione di atti discriminatori nei confronti dello stesso (nota 13 maggio 2019).

13.14. *I trattamenti di dati da parte del medico competente*

In merito ad un quesito formulato dalla Società italiana di medicina del lavoro (Siml) in ordine al trattamento dei dati personali posto in essere da parte del medico competente ai sensi della disciplina in materia di igiene e sicurezza sul luogo di lavoro, l'Ufficio, richiamando i precedenti dell'Autorità, ha precisato che la disciplina di settore (d.lgs. 9 aprile 2008, n. 81) individua la funzione del medico competente come autonoma rispetto a quella che, pure in tale ambito, deve essere svolta dal datore di lavoro, assegnando specifici e distinti obblighi in capo all'una e all'altra figura, così delineando l'ambito del rispettivo trattamento consentito. In particolare, nello svolgimento dei compiti che la legge gli attribuisce in via esclusiva (attività di sorveglianza sanitaria e tenuta delle cartelle sanitarie e di rischio dei singoli lavoratori), il professionista è l'unico legittimato *ex lege* a trattare in piena autonomia e competenza tecnica i dati personali di natura sanitaria indispensabili per tale finalità, non potendo essere in alcun modo trattate dal datore di lavoro informazioni relative, ad esempio, alla diagnosi o all'anamnesi familiare del lavoratore, se non con riferimento al solo giudizio di idoneità alla mansione specifica ed alle eventuali prescrizioni che il professionista fissa come condizioni di lavoro. Anche sotto il profilo sanzionatorio, il quadro normativo nazionale distingue chiaramente le responsabilità che ricadono sul datore di lavoro da quelle che invece sono direttamente imputabili al medico competente, sia quando opera in qualità di libero professionista o per conto di strutture convenzionate, sia quando opera in qualità di dipendente del datore di lavoro. Sulla base di tali valutazioni, il Garante ha tradizionalmente considerato il medico competente un autonomo titolare e, nonostante gli accertamenti volti a verificare l'idoneità alla mansione specifica del dipendente siano obbligatori per legge e svolti a spese e a cura del datore di lavoro (artt. 39, comma 5 e 41, comma 4, d.lgs. n. 81/2008), essi devono essere effettuati esclusivamente tramite il professionista. Egli è, infatti, l'unico soggetto legittimato a trattare i dati sanitari dei lavoratori per le finalità indicate dalla disciplina di settore, come chiarito dal Garante in un provvedimento nel quale è stato precisato, tra gli altri profili, che il medico competente tratta dati personali di natura sanitaria indispensabili ai fini dell'applicazione della normativa in materia di igiene e di sicurezza

13

del lavoro in qualità di titolare del trattamento (provv. 27 aprile 2016, n. 194, doc. web n. 5149198; ma v. pure, con particolare riguardo alla tenuta delle cartelle sanitarie e di rischio da parte del medico competente e alla diversa attività di tenuta e aggiornamento dei fascicoli personali dei dipendenti da parte del datore di lavoro, le linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro, in particolare ai punti 8.1 e 8.4, doc. web n. 1364939; da ultimo, provv. 5 giugno 2019, n. 146, doc. web n. 9124510). Tanto, anche in considerazione del fatto che lo stesso RGPD considera in via autonoma le funzioni del medico competente con riguardo ai trattamenti necessari per le finalità di medicina del lavoro (art. 9, lett. *h*), del RGPD), diversamente dai trattamenti del datore di lavoro necessari per adempiere i propri obblighi normativi in materia di salute e sicurezza sul lavoro (artt. 9, lett. *b*), e 88 del RGPD) (nota 19 marzo 2019).

14 Le attività economiche

14.1. *Configurazione dei ruoli* privacy *nelle gare per l'affidamento dei servizi assicurativi*

È stato fornito un parere in merito al ruolo di titolare o responsabile del trattamento rivestito dalle società che offrono servizi assicurativi a soggetti pubblici (doc. web n. 9169688). In particolare, una compagnia assicuratrice si è rivolta al Garante rappresentando che, successivamente all'entrata in vigore del RGPD, nei bandi di gara promossi da alcuni enti pubblici e/o società controllate o partecipate per l'affidamento dei servizi assicurativi (polizze infortuni, responsabilità civile di terzi, ecc.) era previsto che la compagnia assicuratrice aggiudicataria assumesse il ruolo di responsabile del trattamento ai sensi dell'art. 28 del RGPD.

Il Garante, nel precisare che la vigente disciplina in materia di protezione dei dati personali si pone in linea di continuità con il quadro normativo previgente rispetto all'individuazione dei ruoli di titolare e di responsabile, ha chiarito che la compagnia assicurativa aggiudicataria assume la posizione di titolare autonomo del trattamento non ponendo in essere un trattamento di dati per conto dell'ente aggiudicante rispetto al quale persegue interessi separati e distinti. L'attività delle compagnie assicuratrici, che operano sotto la vigilanza di un'autorità di controllo di settore, è disciplinata da una specifica normativa (artt. 1882 ss. c.c.; d.lgs. n. 209/2005, codice delle assicurazioni; regolamento Ivass n. 40/2018) che definisce in maniera dettagliata tutti gli aspetti dell'attività assicurativa, individuando gli obblighi che ricadono su ognuna delle parti contraenti.

14.2. *Il trattamento dei dati in ambito bancario e assicurativo*

Il notevole afflusso di segnalazioni, reclami, quesiti e richieste di parere registratosi negli ultimi anni in materia di trattamento di dati personali effettuato da banche, società finanziarie, sistemi di informazione creditizia, Centrale dei rischi gestita dalla Banca d'Italia, Centrale di allarme interbancaria, concessionari di pubblici servizi (in particolare Poste italiane s.p.a.) è proseguito anche nel corso del 2019.

Gran parte delle istanze pervenute ha riguardato, come in passato, profili su cui il Garante si era già ripetutamente espresso anche a mezzo di provvedimenti collegiali, in particolare con le linee guida adottate con il provvedimento 25 ottobre 2007, n. 53 (doc. web n. 1457247), i cui princìpi sono già stati ritenuti compatibili con il quadro regolatorio di recente introduzione (v. Relazione 2018, p. 138 ss.). Più in dettaglio, alcune di esse hanno riguardato il trattamento dei dati personali effettuato in occasione delle operazioni di adeguata verifica della clientela prescritte dalla normativa vigente in materia di antiriciclaggio (già oggetto di disamina da parte del Garante, da ultimo e per i profili di propria competenza, con parere 9 marzo 2017, n. 125, doc. web n. 6124534, di cui si è data ampia informazione nelle ultime Relazioni dell'Autorità), con particolare riferimento alle modalità di identificazione degli interessati attraverso l'acquisizione di fotocopie dei documenti di riconoscimento. Al riguardo, l'Ufficio ha precisato che i soggetti tenuti all'applicazione di tale istituto sono obbligati per legge a identificare adeguatamente il cliente prima della stipula

14

di contratti o dell'esecuzione di operazioni, nonché ad effettuare appositi interventi, tra i quali il monitoraggio e il controllo continuativo del rapporto. In tale quadro, l'acquisizione di copia di un valido documento di identità degli interessati, costituendo attuazione degli adempimenti previsti dal decreto legislativo n. 90/2017 e, più in generale, dalla stessa normativa in materia di antiriciclaggio (su cui l'Autorità ha fornito indicazioni, per i profili di propria competenza, sin dal 2003, attraverso pareri, l'ultimo dei quali del 24 luglio 2019, n. 150, doc. web n. 9126288), non è risultata, nei casi esaminati, in violazione della normativa in materia di protezione dei dati personali, trattandosi di attività svolta dagli operatori bancari in esecuzione di obblighi di legge e con modalità non lesive, in concreto, dei principi di correttezza o dignità o di altre disposizioni rilevanti della disciplina *de qua* (cfr. par. 3.1.2).

Sono state altresì esaminate istanze aventi ad oggetto le operazioni di raccolta di informazioni realizzate mediante questionari in occasione dell'esecuzione di servizi di consulenza effettuati da istituti di credito e imprese di investimento volte a valutare l'adeguatezza e l'appropriatezza delle operazioni o dei servizi offerti alla clientela. Anche a questo riguardo si è precisato che le banche e gli intermediari danno applicazione alle disposizioni vigenti in materia (d.lgs. 3 agosto 2017, n. 129, adottato in attuazione della direttiva 2014/65/UE del Parlamento europeo e del Consiglio del 15 maggio 2014), peraltro oggetto di successivi interventi di normazione secondaria da parte delle autorità di settore (Banca d'Italia e Consob). In termini generali, è stato poi evidenziato che gli obiettivi di trasparenza e di tutela dei risparmiatori/investitori previsti dalla normativa vigente possono essere conseguiti dai soggetti chiamati alla loro applicazione anche attraverso un'adeguata profilazione della clientela, purché tale attività sia opportunamente ispirata (e improntata) al perseguimento del miglior interesse della stessa. Si è ricordato, infine, che la materia è attualmente all'attenzione del Cedp (ex Gruppo Art. 29) che si è impegnato a intervenire, per i profili di competenza, attraverso l'apposito sottogruppo *Financial matters*.

Nel merito, l'Ufficio ha confermato che le banche e le imprese di investimento, nel trattare i dati personali necessari a valutare l'adeguatezza e l'appropriatezza delle operazioni o dei diversi servizi di investimento, devono utilizzare dati pertinenti e non eccedenti rispetto alla finalità perseguita, misurandone la rispondenza in rapporto alle circostanze concrete relative alle singole operazioni effettuate o ai servizi resi alla clientela; è stato inoltre precisato che i dati in esame non possono essere utilizzati dai medesimi soggetti per finalità incompatibili con quelle che ne hanno determinato la raccolta (art. 5, par. 1, lett. *b*), del RGPD). Si è provveduto a specificare, comunque, che non sussiste alcun obbligo in capo al cliente stesso o all'utente di fornire le informazioni richieste attraverso la compilazione del questionario, ferme restando, in tal caso, le conseguenze previste dalla normativa di riferimento (delibera Consob 15 febbraio 2018, n. 20307).

Numerose trattazioni, infine, hanno riguardato la (tradizionalissima) questione della differenza tra il diritto di accesso ai dati personali, disciplinato dall'art. 15 del RGPD (e in relazione alle persone decedute, dall'art. 2-*terdecies* del Codice), e il diritto di accesso ad atti e documenti previsto dalla normativa bancaria (art. 119, comma 4, d.lgs. n. 385/1993), tematica sui cui il Garante è tornato a ribadire, con rinnovata determinazione, la propria incompetenza a pronunciarsi a fronte di istanze fondamentalmente rivolte a ottenere questi ultimi.

Specularmente, per quanto riguarda il settore assicurativo, una delle principali questioni portate all'attenzione dell'Autorità dagli interessati ha riguardato l'alterità tra il suddetto diritto di accesso ai dati personali e il diritto di accesso agli atti assicurativi previsto e disciplinato dall'art. 146, d.lgs. n. 209/2005; le numerosissime

istanze pervenute, infatti, pur avendo ad oggetto precedenti richieste formulate ai titolari dei trattamenti con richiami, spesso solo indiretti, alla disciplina di protezione dei dati personali, erano, invero, inequivocabilmente preordinate, alla luce delle espressioni chiaramente utilizzate e delle finalità ad esse sottese (difficilmente perseguibili attraverso l'esercizio del diritto di accesso ai dati personali), a ottenere copia di atti e/o documenti contrattuali e assicurativi da utilizzare contro le stesse società di assicurazioni per la tutela di eventuali diritti in sede giudiziaria. Nel richiamare, anche in tale ambito, l'orientamento già espresso dall'Autorità in precedenti pronunce collegiali (tutte disponibili sul sito del Garante), l'Ufficio non ha potuto che esprimersi nei termini sopra richiamati, ferma restando la possibilità per gli interessati di accedere comunque ai propri dati.

Particolarmente critico è risultato il profilo relativo all'accesso ai dati personali contenuti nelle perizie medico-legali, con particolare riferimento alle informazioni di tipo valutativo-soggettivo e/o ai giudizi ivi contenuti; ciò anche in considerazione del fatto che l'attuale disciplina, a differenza di quella previgente (v. l'art. 8, comma 4, del Codice, abrogato dal d.lgs. n. 101/2018), nulla dice in merito all'accessibilità di dati diversi da quelli di carattere "oggettivo". Nei casi esaminati, pur ribadendosi, sulla base del consolidato orientamento del Garante, che le informazioni contenute nelle perizie medico-legali contengono dati personali suscettibili di accesso ai sensi della disciplina in esame, si è tuttavia precisato che il diritto di cui all'art. 15 del RGPD incontra alcune limitazioni puntualmente individuate, in attuazione dell'art. 23 del medesimo Regolamento, dall'art. 2-*undecies* del Codice. Tenuto conto del contesto di riferimento descritto dagli istanti – sovente di natura aspramente contenziosa o pre-contenziosa – si è ritenuta applicabile in numerosi casi la limitazione di cui alla lett. *e*), secondo cui il diritto di accesso non può essere esercitato qualora ne possa derivare un pregiudizio effettivo e concreto allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria. Considerato, peraltro, che molte delle istanze pervenute avevano ad oggetto, in verità, l'acquisizione in forma integrale (e senza oscuramenti) di copia integrale delle singole perizie, l'Ufficio ha provveduto a rimarcare, ancora una volta, la diversità tra il diritto di accesso ai dati personali e il diritto di accesso ad atti e documenti.

Sempre in relazione all'esercizio del diritto di accesso ai dati personali in ambito assicurativo, ma con riferimento alla possibilità di acquisire anche (o solo) informazioni relative a soggetti terzi – nella specie, i nominativi dei beneficiari di polizze stipulate in vita da persone decedute –, l'Autorità è tornata a ribadire, anche alla luce del nuovo quadro regolatorio, la necessità di distinguere tra istanze (legittime) volte a ottenere l'accesso ai dati personali riferiti al *de cuius* (art. 2-*terdecies* del Codice) e istanze, invece, finalizzate a ottenere, specificamente e direttamente, dati personali relativi a terzi, non suscettibili di accoglimento sulla base dei diritti accordati dalla disciplina in materia di protezione dei dati (si veda, in proposito, anche quanto stabilito da Cass. civ., 8 settembre 2015, n. 17790).

Numerose istanze, sotto altro profilo, hanno poi riguardato, spesso genericamente, la circolazione dei dati personali all'interno della cd. catena assicurativa; al riguardo, l'Ufficio, nel richiamare il provvedimento generale 26 aprile 2007 (doc. web n. 1410057) per i profili compatibili con il novellato quadro di riferimento, ha ribadito che le peculiarità del settore in esame sono spesso alla base dei (talora inevitabili) flussi comunicativi che si registrano in tale ambito, sovente tali da giustificare un'ampia conoscibilità delle informazioni all'interno della medesima catena assicurativa; è stato precisato, tuttavia, che la circolazione dei dati personali degli interessati deve comunque avvenire nel rispetto della disciplina di legge, avuto specifico riguardo, per quanto di interesse nei singoli casi, alle responsabilità cui sono

tenuti tutti i partecipanti relativamente alle operazioni di trattamento dagli stessi effettuate nell'ambito di detta catena.

14.2.1. Data breach *nel settore bancario*

Anche il settore bancario è stato interessato da alcuni *data breach* che hanno richiesto approfondimenti da parte dell'Autorità. In particolare, con provvedimento 28 marzo 2019, n. 87 (doc. web n. 9104006), il Garante ha definito l'istruttoria aperta nel luglio 2017, quando un'intrusione informatica ai danni di un primario istituto bancario ha determinato accessi non autorizzati ai dati personali di circa 800.000 clienti; tali accessi abusivi sono stati effettuati in due momenti temporali distinti tramite le credenziali assegnate ad alcuni dipendenti e collaboratori di un *partner* commerciale esterno cui era affidata la gestione delle richieste di finanziamento relative alla cessione del quinto dello stipendio.

Gli approfondimenti tecnici eseguiti dall'istituto di credito già nell'immediatezza dell'evento (*audit report*) e le risultanze di un accertamento ispettivo dell'Autorità hanno consentito, da un lato, di accertare l'esistenza di alcune vulnerabilità di sicurezza dell'applicativo oggetto dell'intrusione e la mancata adozione delle misure di sicurezza necessarie di cui al provvedimento 12 maggio 2011, n. 192 (Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie), con conseguente individuazione delle fattispecie di illiceità che hanno, quindi, formato oggetto di un autonomo procedimento per la contestazione delle sanzioni amministrative di cui all'art. 162, commi 2-*bis* e 2-*ter*, del Codice; dall'altro, di verificare come l'istituto di credito, a seguito dell'incidente, abbia effettivamente adottato le necessarie misure tecniche e organizzative atte ad evitare il ripetersi di accadimenti similari.

14.3. *Dai codici di deontologia nel settore economico e finanziario ai codici di condotta*

Particolarmente rilevante è stata l'attività svolta dal Garante per "incoraggiare" il passaggio e la "trasformazione" in codici di condotta, coerenti con il disposto degli artt. 40 e 41 del RGPD, dei preesistenti codici di deontologia e di buona condotta in materia di sistemi di informazione creditizia e di informazioni commerciali (di cui gli all. A.5 ed A.7 del testo previgente del Codice).

Il percorso normativo orientato a tale scopo (chiaramente volto ad assicurare una continuità sostanziale nel regime di trattamento dei dati e nelle correlate tutele) è stato indicato nell'art. 20, d.lgs. n. 101/2018. I termini previsti da tale disposizione sono stati rispettati in entrambi gli ambiti e si sono potuti approvare due schemi di codici di condotta prima dell'invalicabile scadenza del 19 settembre 2019.

Dal punto di vista formale si è trattato di un'approvazione con riserva, dal momento che il percorso (eurounitario) di determinazione di criteri comuni per l'accreditamento degli organismi di monitoraggio (istituto specificamente previsto dall'art. 41 del RGPD) non si era ancora concluso al momento della definizione dei due codici di condotta in questione. Realisticamente, l'approvazione definitiva dei due importanti testi potrà avvenire intorno alla metà del 2020, ma le disposizioni in essi contenute (che si pongono in forte continuità con l'assetto regolatorio precedente) sono comunque già applicate dai titolari del trattamento implicati in queste tipologie di attività e costituiscono, anche per l'Autorità, i parametri di riferimento per l'esame del contenzioso in materia. Di seguito si evidenziano, in estrema sintesi, gli elementi caratterizzanti dei due codici.

14.3.1. Il codice di condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale

Il testo (approvato con provv. 12 giugno 2019, n. 127, doc. web n. 9119868) rielabora ed aggiorna, secondo la "grammatica" del RGPD, i contenuti del codice di deontologia del 2014. Del resto, si trattava di un atto di recente adozione che aveva dimostrato, negli anni di applicazione, di corrispondere alle necessità del settore economico di riferimento.

Naturalmente, alla luce delle nuove disposizioni, il trattamento dei dati personali degli imprenditori e degli altri soggetti ricadenti nella platea delle persone censite negli archivi delle imprese di informazione commerciale è ora basato sul legittimo interesse dei fornitori di tali servizi (non potendo ovviamente configurarsi la possibilità di basare questo trattamento sul consenso degli interessati).

Molto significativa (e dettagliata) è l'elencazione, all'art. 4, delle fonti di provenienza delle informazioni in oggetto, nella quale, alle tradizionali fonti pubbliche, si affiancano le cd. fonti pubblicamente e generalmente accessibili, fra le quali sono stati presi in considerazione, con una serie di necessari limiti, anche i quotidiani e le testate giornalistiche *online*.

Data la specificità della materia, è decisivo il disposto dell'art. 8 (sostanzialmente confermato nella sua architettura), che regolamenta la cd. associazione dei nominativi di alcune categorie di interessati ad una serie di eventi negativi (procedure concorsuali, ipoteche, protesti, ecc.) coinvolgenti le imprese e le società cui gli interessati medesimi sono a vario titolo riconducibili.

Non meno rilevanti sono poi l'art. 8, commi 4 e 5, e l'art. 9 che, al fine di assicurare chiarezza e certezza nel trattamento dei dati, disciplinano accuratamente il tempo di conservazione delle informazioni.

14.3.2. Il codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti

La redazione di questo codice di condotta (approvato con provv. 12 settembre 2019, n. 163, doc. web n. 9141941) ha richiesto a tutte le categorie interessate uno sforzo notevole e la necessaria convergenza su un testo che si ponesse come punto di incontro fra esigenze contrapposte (specie con riguardo alla volontà chiaramente espressa da alcune importanti associazioni di categoria, come Abi ed Assofin, di ampliare notevolmente il novero degli operatori economici interessati dal codice). Un testo che comunque precisa ed "allarga" la tipologia di rapporti censiti (e, conseguentemente, anche la platea dei soggetti partecipanti) includendo ipotesi di facilitazione finanziaria quali il noleggio a lungo termine, il *leasing* operativo, la cessione di crediti, le dilazioni di pagamento ed il prestito tra privati gestito attraverso piattaforme digitali (cd. *peer to peer lending*).

Il nuovo codice tiene poi conto di alcune novità legislative e giurisprudenziali. In tal senso, si colloca la previsione del ruolo dei soggetti che solo accedono ai SIC senza porsi, allo stato, come contributori degli stessi (fornitori di servizi di comunicazione elettronica, imprese di assicurazione, soggetti autorizzati a svolgere l'attività di vendita a clienti finali di energia elettrica e di gas naturale).

Particolarmente significative le modifiche che, in chiave di tutela degli interessati e di chiarezza del disposto codicistico, hanno fissato in due appositi allegati (n. 1 e n. 2) le disposizioni di dettaglio in ordine al preavviso di segnalazione ed ai tempi di conservazione dei dati.

Per il primo aspetto, alla luce dell'esperienza maturata e degli orientamenti espressi dalla Corte di cassazione e dall'Arbitro bancario finanziario, è stata espressamente prevista una serie di modalità, anche cumulabili fra loro, che assicurano

14

ai soggetti partecipanti la possibilità di inoltrare, in modo agevole e non oneroso, il citato preavviso, dando altresì prova della sua ricezione da parte dell'interessato segnalato (cfr. Cass. civ., sez. I, 13 giugno 2017, n. 14685).

Per il secondo aspetto, si è invece allineata la tempistica di conservazione dei dati positivi agli orientamenti espressi, anche a livello internazionale, dalle autorità di vigilanza, in ambito creditizio, mantenendo invece inalterata (e sufficientemente contenuta) la tempistica di conservazione dei dati personali relativi ad eventi negativi sia regolarizzati che non regolarizzati.

14.4. *La videosorveglianza in ambito privato*

Continuano a pervenire numerosi i reclami concernenti l'utilizzo di sistemi di videosorveglianza da parte di soggetti privati anche in ambito condominiale. Il Garante, nel richiamare i principi contenuti nel provvedimento generale in materia di videosorveglianza adottato l'8 aprile 2010 (doc. web n. 1712680), ha evidenziato che il trattamento di dati personali, correlato all'utilizzo di videocamere, se effettuato da persone fisiche per fini esclusivamente personali, non è soggetto all'ambito di applicazione della normativa in materia di protezione dati, sempre che l'angolo visuale di ripresa sia limitato agli spazi di esclusiva pertinenza (ingressi, accessi alla zona autorimessa, ecc.).

Non può tuttavia configurarsi un trattamento di dati per fini personali nell'ipotesi in cui le telecamere riprendano aree o porzioni di aree gravate da servitù prediali (v. peraltro in materia gli orientamenti maturati dalla CGUE, 11 dicembre 2019, C-708/18, caso TK c. Asociatia de Proprietari bloc M5A-ScaraA).

Il Garante ha fornito dettagliate indicazioni anche con riferimento all'installazione di impianti di videosorveglianza da parte di compagini condominiali, specificando che le telecamere possono riprendere solo le aree comuni (in corrispondenza ad accessi, *garage*, ecc.) e non i luoghi circostanti o particolari non rilevanti (strade, edifici, esercizi commerciali ecc.). L'Autorità ha altresì rammentato che, in ossequio a quanto disposto dalle norme del codice civile in materia di condominio negli edifici, le deliberazioni concernenti l'installazione di impianti di videosorveglianza sulle parti comuni devono essere approvate dall'assemblea con un numero di voti che rappresenti la maggioranza degli intervenuti e almeno la metà del valore dell'edificio (artt. 1122-*ter* e 1136 c.c.).

14.5. *Trattamenti di dati in ambiti e settori particolari*

14.5.1. Riconoscimento facciale dei passeggeri presso gli aeroporti di Roma Fiumicino e Milano Linate

Aeroporti di Roma s.p.a. ha sottoposto al Garante un progetto sperimentale che prevede l'installazione in alcune aree dell'aeroporto di Roma Fiumicino di dispositivi idonei a rilevare le caratteristiche biometriche del volto dei passeggeri contestualmente all'acquisizione elettronica di ulteriori informazioni contenute nei relativi documenti di riconoscimento e nelle carte di imbarco; ciò al fine di velocizzare le operazioni di riconoscimento ai varchi dei controlli di sicurezza e ai *gate* di imbarco.

In questa fase sperimentale il progetto è rivolto esclusivamente ai passeggeri in partenza su alcune tratte selezionate in area Schengen e il trattamento dei dati biometrici è basato sul consenso preventivo degli interessati (art. 9, par. 2, lett *a*), del

RGPD) rilasciato sulla base di previa e idonea informativa ai sensi dell'art. 13 del RGPD. Completata la fase di imbarco, i dati rilevati dal sistema sono conservati nel *database* sino a un'ora dopo la partenza del volo per poi essere cancellati.

Uno specifico e distinto consenso degli interessati potrà legittimare la conservazione dei dati per un periodo di tempo compreso tra i 6 e i 12 mesi al fine di consentire agli stessi di utilizzare il servizio, senza ripercorrerne i relativi passaggi, in occasione di successivi voli in partenza dall'aeroporto di Fiumicino.

Resta comunque salva per gli utenti la possibilità di continuare ad utilizzare le ordinarie modalità di accesso tramite gli appositi varchi dei controlli di sicurezza.

Contemporaneamente, si è tenuto un incontro con rappresentanti della Società per azioni esercizi aeroportuali S.E.A. (cui è rimessa la gestione del sistema aeroportuale di Milano), la quale ha presentato all'Autorità un altro progetto sperimentale che prevede anch'esso l'installazione, in alcune aree dell'aeroporto di Linate, di dispositivi idonei a rilevare le caratteristiche biometriche del volto dei passeggeri contestualmente all'acquisizione elettronica di ulteriori informazioni contenute nei relativi documenti di riconoscimento e nelle carte di imbarco, limitatamente alla tratta Milano-Roma operata da Alitalia (collegamento utilizzato principalmente dai cd. *frequent flyer*).

Anche in questo caso, il progetto risponde all'esigenza di velocizzare le operazioni di riconoscimento ai varchi dei controlli di sicurezza e ai *gate* di imbarco e il trattamento dei dati biometrici è fondato sul consenso preventivo dei passeggeri, rilasciato sulla base di previa e idonea informativa, lasciando tuttavia agli stessi sempre la possibilità di effettuare i controlli in modo tradizionale.

Una volta prestato il consenso, sarà espressamente richiesto agli interessati se conservare i propri dati personali per un solo viaggio (con cancellazione entro le 24 ore successive alla partenza) oppure per tutta la durata della fase pilota, e cioè dall'8 gennaio fino al 31 dicembre 2020.

14.5.2. Fornitura di energia elettrica e gas e trattamento di dati personali della clientela

Con provvedimento 11 dicembre 2019, n. 231 (doc. web n. 9244358) il Garante si è pronunciato nei confronti di una società operante nel settore energetico a seguito della ricezione di diversi reclami aventi ad oggetto il trattamento dei dati personali di clienti nell'ambito della fornitura di energia elettrica e gas mediante la conclusione di contratti non richiesti nel mercato libero. In particolare, i reclamanti avevano lamentato di aver preso conoscenza della stipula del contratto solo a seguito della ricezione della comunicazione di cessazione del rapporto in essere da parte del proprio fornitore o in occasione di recapito delle prime fatture da parte della società subentrata (sulla quale si sono appuntati i reclami), asserendo di non aver mai avuto alcun contatto né personale né a distanza con detta società, né di essersi mai recati presso alcun punto vendita o agenzia della stessa. In svariati casi, inoltre, è stato rappresentato che la documentazione contrattuale in possesso della società recava dati personali inesatti (in particolare, numero di telefono, indirizzo di fornitura, estremi del documento di identità) nonché sottoscrizioni apocrife.

Dall'attività istruttoria è emerso che i trattamenti sopra menzionati sono stati posti in essere dalla società, in qualità di titolare del trattamento, per il tramite di alcune agenzie, designate responsabili dei medesimi trattamenti. In particolare, le misure tecniche e organizzative adottate dal titolare nell'ambito dei processi di acquisizione dei dati della clientela per il tramite del cd. canale agenzia non sono risultate adeguate alla natura, al contesto, alle finalità e ai rischi del suddetto trattamento, configurando una violazione del principio di responsabilizzazione nonché

14

dei principi di correttezza, esattezza, aggiornamento dei dati, integrità e riservatezza (artt. 5, par. 1, lett. *a*), *d*) ed *f*), e par. 2, 24 e art. 32 del RGPD). Sulla base del recente impianto normativo introdotto dal RGPD, infatti, il titolare è il soggetto cui è attribuita la "responsabilità generale" del trattamento posto in essere direttamente o per il tramite di altri, gravando sullo stesso l'onere di attuare un sistema organizzativo e gestionale contraddistinto da misure reali ed efficaci di protezione dei dati nonché comprovabili (v. cons. 74 e artt. 5, par. 2 e 24 del RGPD); ciò soprattutto mediante l'implementazione di procedure e prassi organizzative atte a conformare i trattamenti di dati personali al RGPD (es. processi di mappatura dei trattamenti, regole per l'attribuzione di responsabilità, programmi di formazione del personale, procedure per la gestione delle richieste di esercizio dei diritti e dei reclami, *policy* per la gestione e comunicazione di violazioni di sicurezza, previsione di *audit* interni ed esterni con cadenza periodica, ecc.: cfr. Gruppo Art. 29, WP 173, 13 luglio 2010, *Opinion 3/2010 on the principle of accountability*, p. 11-12). Nella fattispecie oggetto di contestazione sono state invece accertate diverse carenze nelle *privacy policy* della società, *policy* che sono apparse lacunose e poco efficaci soprattutto in termini di garanzia dell'esattezza dei dati trattati, di sicurezza del trattamento nonché di controllo dell'operato delle persone autorizzate a trattarli; l'inadeguatezza e la lacunosità di tali modalità procedurali ha consentito ad alcuni soggetti (nella specie, agenti e venditori) di operare per un considerevole lasso di tempo in violazione delle istruzioni impartite dal titolare con ripercussioni sulla legittimità dei relativi trattamenti, in particolare in termini di correttezza degli stessi e di qualità dei dati trattati.

È stata pertanto sancita l'illiceità delle condotte sopra descritte, sono state ingiunte specifiche prescrizioni di carattere correttivo ed è stata applicata la sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. *a*), del RGPD.

14.5.3. Propaganda elettorale

Come in parte anticipato (parr. 4.7 e 11.3), il Garante, con provvedimento 18 aprile 2019, n. 96 (doc. web n. 9105201), ha illustrato le principali novità introdotte dal RGPD in materia di trattamenti per finalità di propaganda elettorale e connessa comunicazione politica, richiamando l'attenzione di organismi politici, comitati di promotori e sostenitori nonché di singoli candidati sulle modalità di trattamento dei dati personali per i predetti scopi.

Al riguardo, *in primis* sono stati puntualmente definiti i casi in cui i trattamenti per finalità di propaganda elettorale possono essere effettuati: con il consenso degli interessati, con riguardo alle informazioni inerenti a iscritti ad organismi associativi a carattere non politico, simpatizzanti, persone contattate in occasione di singole iniziative, sovventori (v. provv. cit., punto 2); sulla base del legittimo interesse del titolare, in particolare rispetto ai dati provenienti dalle cd. fonti pubbliche (v. provv. cit., punto 3, n. 1) o agli aderenti e soggetti che hanno contatti regolari con partiti, movimenti e altre formazioni a carattere politico (v. punto 3, n.2); oppure in virtù di altri presupposti di legittimità (art. 9, par. 2, lett. *d*) ed *e*), del RGPD: cfr. provv. cit., punto 3, n.2).

In ordine agli obblighi di trasparenza, è stato rilevato che, fermo restando l'onere per i titolari di rilasciare idonea informativa ai sensi dell'art. 13 del RGPD, nei casi in cui i dati non siano raccolti presso l'interessato, essi possono esimersi dal rendere le predette informazioni ove ciò risulti impossibile o implichi uno sforzo sproporzionato e previa adozione di "misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni" (art. 14, par. 4, lett. *b*), e par. 5, lett. *b*), del RGPD: v. provv. cit., par. 6).

Infine, nel richiamare il necessario rispetto dei diritti dell'interessato (v. provv.

cit., punto 7) nonché il rigoroso regime sanzionatorio di recente istituzione (v. provv. cit., punto 8), è stato ribadito che i titolari del trattamento (partiti; movimenti politici; comitati; singoli candidati) sono tenuti a predisporre, alla luce dei principi di *accountability* e *privacy by design*, misure organizzative e tecniche adeguate, tali da garantire l'esercizio effettivo, puntuale e tempestivo dei diritti degli interessati e devono essere in grado di comprovare con idonea documentazione le suddette misure nonché il procedimento valutativo seguito per la loro individuazione (ivi inclusa la predisposizione di idonea valutazione dei rischi).

14.6. *Procedure IMI relative a trattamenti di dati in ambito economico*

Come già evidenziato in relazione ai trattamenti effettuati in internet o nel contesto delle comunicazioni elettroniche (cfr. par. 11.4), i trattamenti effettuati in ambito economico possono presentare caratteristiche transfrontaliere ed essere quindi trattati da una pluralità di autorità di controllo mediante la piattaforma IMI (i cui caratteri sono descritti al par. 21.1).

Nel solo ambito (economico e produttivo) qui direttamente preso in esame, va rilevato che le procedure trattate nel corso del 2019 – numerose, considerato che il Garante si è dichiarato autorità interessata in 170 procedure ex art. 56 del RGPD e opera quale "autorità capofila" in altre 12 – hanno comportato una complessa attività istruttoria al fine di individuare la rilevanza transfrontaliera del trattamento di dati e per partecipare quindi alle istruttorie in qualità di autorità di controllo interessata o, come si è visto in un numero limitato di casi, di autorità capofila.

In relazione alla peculiare prospettiva dei trattamenti effettuati in ambito economico, si è comunque assistito ad una diminuzione delle procedure IMI volte ad identificare l'autorità capofila ai sensi dell'art. 56 del RGPD, specialmente con riferimento ai cd. *over the top*, avendo ormai le relative autorità capofila aperto sulla piattaforma IMI già diversi "casi" – locuzione che non identifica necessariamente un singolo reclamo o una singola procedura, ma individua un "punto di partenza centrale" da cui possono originare diverse procedure aventi scopi differenti, ad esempio relative ad una pluralità di reclami proposti nei confronti dello stesso titolare per violazioni analoghe ma dinanzi a distinte autorità di controllo nazionali o, ancora, procedure di assistenza reciproca o procedure di "sportello unico" ex art. 60 del RGPD – in relazione ai trattamenti transfrontalieri che coinvolgono tali titolari. Ciò ha comportato che, per effetto della regola del "raggruppamento" (cd. *bundling*), l'autorità di controllo destinataria di un reclamo provvede prima a verificare se esistano "casi" analoghi già aperti nel sistema IMI dall'autorità capofila nei confronti del titolare in questione e, in caso positivo, a trasmettere il reclamo all'autorità capofila attraverso la procedura di assistenza reciproca volontaria. Tale prassi, ormai consolidata, ha consentito di evitare il "caricamento" di numerose procedure IMI non più necessarie, con una riduzione del carico di lavoro per tutte le autorità di controllo.

Tuttavia, nell'ipotesi di trattamenti transfrontalieri con impatto solo "locale" (vale a dire esclusivamente nazionale), le autorità di controllo dinanzi alle quali è stato proposto un reclamo ai sensi dell'art. 77 del RGPD ricorrono ancora in misura insufficiente alla procedura specificamente prevista in IMI per informare l'autorità capofila, ai sensi dell'art. 56, par. 3, del RGPD, della propria intenzione di trattare il caso a livello locale (senza il coinvolgimento in questa fase delle altre autorità di controllo che potrebbero essere chiamate a partecipare al processo decisionale ove l'autorità capofila ritenesse invece di trattare il caso secondo il meccanismo dello

14

"sportello unico"); analogamente, omettono di svolgere quell'attività preistruttoria con lo stabilimento locale del titolare che consentirebbe, in molte ipotesi, di addivenire ad una definizione dei reclami in una fase preliminare informando esclusivamente l'autorità capofila dell'esito degli stessi.

Va inoltre ricordata la modifica della procedura di assistenza reciproca volontaria che allo stato consente di rivolgere la richiesta a più autorità di controllo in una sola volta condividendo allo stesso tempo con le autorità selezionate anche le risposte ricevute. Tale procedura viene però tuttora frequentemente utilizzata per ottenere informazioni sulle normative nazionali in tema di protezione dei dati, informazioni queste che potrebbero invece essere reperite attraverso i tradizionali mezzi di comunicazione oppure in *forum* di discussione già previsti, tanto che lo stesso Cepd ha invitato le autorità di controllo ad un uso più puntuale di tale procedura per evitare un aggravio di lavoro per le autorità destinatarie delle richieste.

Casistica

Venendo al merito delle procedure IMI nel settore privato, con specifico riferimento all'attività economica e produttiva, le stesse continuano a riguardare casistiche eterogenee riferite ad una variegata pluralità di titolari del trattamento di cui circa una decina aventi lo stabilimento principale o unico in Italia, rispetto alle quali, quindi, il Garante si è dichiarato autorità capofila. Si segnala, ad esempio, un reclamo presentato all'autorità di controllo del Regno Unito nei confronti di una casa automobilistica con il quale un cittadino inglese ha lamentato la violazione del diritto di accesso sia alle trascrizioni delle telefonate intercorse tra lo stesso e il servizio clienti in relazione ad un malfunzionamento del suo veicolo, sia ad ogni altro documento o annotazione relativa alla vicenda. In un altro caso, una compagnia aerea italiana è stata destinataria di due reclami presentati alle autorità di controllo di due *Länder* tedeschi per la violazione del diritto di accesso e di cancellazione dei dati fatta valere da alcuni passeggeri; non diversamente rispetto ad un reclamo presentato all'autorità di controllo spagnola nei confronti di un'azienda di abbigliamento italiana in relazione alla violazione dei dati personali riguardanti alcune operazioni effettuate dalla reclamante sul sito web del titolare del trattamento.

In relazione a tali reclami l'Autorità ha avviato l'attività istruttoria all'esito della quale sarà adottato un progetto di decisione da condividere con le altre autorità interessate le quali, partecipando al processo decisionale dello sportello unico previsto dall'art. 60 del RGPD, potranno esprimere i propri commenti o eventuali obiezioni pertinenti e motivate.

Infine, il Garante ha aperto una procedura volta ad accertare l'autorità capofila ai sensi dell'art. 56 del RGPD con riferimento ad una pluralità di reclami presentati all'autorità di controllo italiana nei confronti di una società di *due diligence* con stabilimento principale nel Regno Unito. Tale società risulta disporre di una banca dati reputazionale di rilevanti dimensioni alimentata da dati acquisiti da fonti pubbliche o pubblicamente accessibili, utilizzata per lo più da banche e istituti finanziari nell'adempimento degli obblighi di controllo volti a contrastare la criminalità organizzata, soprattutto in campo finanziario, la corruzione, il riciclaggio di denaro ed il terrorismo.

14.7. *Accreditamento e certificazioni*

È proseguita l'attività di collaborazione con le altre autorità europee per la protezione dei dati in ordine al tema concernente l'accreditamento e la certificazione. I lavori si sono concentrati sulla stesura definiva dei documenti concernenti, rispettivamente, le *Guidelines 1/2018 on certification and identifying certification criteria*

in accordance with Articles 42 and 43 of the Regulation 2016/679, il relativo all. 2, che individua gli aspetti che le autorità di controllo e il Cepd prenderanno in esame ai fini dell'approvazione di criteri di certificazione, nonché l'all. 1 alle *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)*, che fornisce indicazioni sui requisiti aggiuntivi per l'accreditamento degli organismi di certificazione che dovranno essere stabiliti dalle autorità di controllo (cfr. par. 21.1).

A livello nazionale, nell'ambito della collaborazione ormai avviata a partire dal 2017 (v. Relazione 2018, p. 146) tra il Garante e Accredia, l'Ente nazionale di accreditamento, in rapporto alle attività di accreditamento e certificazione previste dal RGPD (v. artt. 42 e 43) è stata sottoscritta una convenzione, della durata di un anno con tacito rinnovo per un ulteriore anno, volta a favorire lo scambio di informazioni in merito a tali attività nonché a valorizzare le reciproche competenze. In base a tale accordo, Accredia comunicherà all'Autorità gli accreditamenti rilasciati, i ricorsi e le decisioni assunte, le scadenze dei certificati, i provvedimenti sanzionatori, l'elenco delle certificazioni e le relative revoche e sospensioni rilasciate dagli organismi di certificazione. Il Garante comunicherà ad Accredia gli aggiornamenti della normativa, le novità sugli schemi di certificazione approvati a livello nazionale ed europeo, nonché le informazioni su problematiche che potrebbero emergere da reclami sottoposti all'attenzione dell'Autorità.

15 Il trattamento dei dati personali nell'ambito del condominio

Chiarimenti sono stati forniti rispetto ai profili attinenti al tema del trattamento di dati personali a fronte di vari reclami e segnalazioni pervenuti in materia di condominio anche nell'ottica di promuovere, nell'ambito dei poteri attribuiti al Garante dalla nuova normativa, la consapevolezza dei titolari e dei responsabili del trattamento coinvolti nel settore riguardo gli obblighi imposti loro dal RGPD.

È stata colta l'occasione per confermare, in termini generali, quanto già indicato nel provvedimento 18 maggio 2006 (doc. web n. 1297626) in merito al trattamento di dati personali nell'ambito dell'amministrazione di condomini e per ribadire che le informazioni personali riferibili a ciascun partecipante possono essere trattate per la finalità di gestione ed amministrazione del condominio e che possono essere per tali ragioni condivise all'interno della compagine condominiale, tenendo anche conto che i condomini devono essere considerati contitolari di un medesimo trattamento dei dati (v. ora art. 4, par. 1, n. 7 e Capo IV, in particolare art. 26 del RGPD) di cui l'amministratore, agendo in eventuale veste di responsabile del trattamento, ha la concreta gestione (v. ora art. 4, par. 1, n. 8 e Capo IV del RGPD). Quest'ultimo, in base a quanto ora previsto dagli artt. 28, par. 3, lett. *b*), e 29 del RGPD, può individuare persone autorizzate al trattamento dei dati personali che agiscono sotto la sua autorità, purché si siano impegnate alla riservatezza e siano state loro fornite le relative istruzioni.

Inoltre, come già rappresentato (cfr. Relazione 2018, p. 149), l'Autorità ha fatto nuovamente presente 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 stabilite nell'ordinamento, richiamando in tal senso le disposizioni introdotte con la legge 11 dicembre 2012, n. 220, recante la "Riforma in materia di condominio negli edifici" (cfr., in particolare, quelle contenute negli artt. 1130, comma 1, nn. 6 e 7, 1129, comma 2, e 1130-*bis*, comma 1, c.c.), che sono state oggetto anche nel corso di quest'anno di numerosi reclami e quesiti.

L'Autorità ha avuto altresì modo di precisare che eventuali responsabilità derivanti da mancati adempimenti in ordine alle attribuzioni affidate all'amministratore di condominio dalle menzionate norme del codice civile concernono comunque profili di carattere prettamente civilistico rispetto alle quali non le è riconosciuta alcuna competenza.

16 Violazione dei dati personali

Nel 2019 sono pervenute all'Autorità 1.443 notifiche di violazione dei dati personali, che hanno riguardato, come titolari del trattamento, soggetti pubblici (nel 27% dei casi) e soggetti privati (nel restante 73%).

Le tipologie di violazione dei dati personali più frequenti, parte non irrilevante delle quali (avendo carattere transfrontaliero) sono state istruite mediante la piattaforma IMI (par. 21.1), hanno riguardato:

- attacchi informatici volti all'acquisizione di dati personali (quali credenziali di accesso, dati relativi a strumenti di pagamento, dati di contatto);
- accesso non autorizzato a caselle di posta elettronica (ordinaria e certificata);
- perdita o indisponibilità di dati personali causata da *malware* di tipo *ransomware*;
- smarrimento o furto di dispositivi digitali o documenti cartacei contenenti dati personali;
- comunicazione o diffusione accidentale di dati personali.

Le attività istruttorie svolte dall'Ufficio a seguito della notifica di una violazione dei dati personali hanno avuto come obiettivo prioritario la valutazione 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 per gli interessati nonché la valutazione della necessità di effettuare la comunicazione dell'avvenuta violazione agli interessati, fornendo loro indicazioni specifiche sulle misure da adottare per proteggersi da eventuali conseguenze pregiudizievoli.

L'Ufficio ha provveduto ad acquisire, laddove non compiutamente rappresentati dal titolare del trattamento, gli elementi necessari alla valutazione del rischio derivante dalle violazioni oggetto di notifica, sia attraverso acquisizione documentale, sia attraverso specifiche attività ispettive presso i titolari o i responsabili del trattamento. Nei casi in cui la violazione ha messo in luce una possibile inadeguatezza delle misure adottate dal titolare, l'Ufficio ha avviato l'attività ispettiva per acquisire gli elementi necessari a individuare le lacune organizzative e tecniche da cui hanno avuto origine le violazioni notificate (v. anche par. 14.2.1). Tale attività di approfondimento ha portato all'adozione di alcuni provvedimenti collegiali di tipo prescrittivo e, nei casi più gravi, sanzionatorio.

Così, con provvedimento 30 luglio 2019, n. 157 (doc. web n. 9126951), il Garante – nell'eliminare talune prescrizioni in materia di comunicazione delle violazioni dei dati personali relative a determinate tipologie di trattamento o categorie di titolari del trattamento (doc. web nn. 1813953, 2388260, 3556992, 4084632, 4129029) richieste sulla base della disciplina previgente all'applicazione del RGPD – ha individuato le informazioni minime che i titolari del trattamento devono fornire al Garante per effettuare una notifica di violazione dei dati personali ai sensi dell'art. 33 del RGPD o dell'art. 26, d.lgs. 18 maggio 2018, n. 51.

17 Il trasferimento di dati personali all'estero

L'attività del Garante nel settore dei trasferimenti di dati personali verso Paesi terzi è stata prevalentemente incentrata su quella svolta in materia dal Cepd e dalla Commissione UE (cfr. par. 21.1). Come sottolineato in passato (v. Relazione 2018, p. 150), le novità legislative introdotte con il RGPD hanno delimitato gli ambiti nei quali il Garante può intervenire con provvedimenti autorizzatori a livello nazionale – circoscritti ad ipotesi specifiche per lo più caratterizzate da peculiari circostanze (come nel caso dell'autorizzazione resa alla Consob per sottoscrivere un accordo amministrativo per il trasferimento di dati personali tra le autorità di vigilanza finanziaria dello Spazio economico europeo (See) e le corrispondenti autorità extra-See: cfr. par. 4.8) – e al contempo hanno previsto una sua maggiore partecipazione, per il tramite dei meccanismi di cooperazione, al procedimento di elaborazione e di approvazione delle "garanzie adeguate" previste al Capo V del RGPD.

Intenso e costante è stato comunque l'impegno dell'Autorità nel fornire chiarimenti ai quesiti pervenuti in merito a quanto previsto nel Capo V del RGPD: dalle richieste relative al possibile utilizzo di clausole tipo quale strumento per il trasferimento dei dati, soprattutto del set di clausole già approvate a suo tempo dalla Commissione in ragione di quanto stabilito dall'art. 46, par. 5, del RGPD, a quelle inerenti le decisioni di adeguatezza sinora adottate (sulla più recente, relativa al Giappone, v. Relazione 2018, p. 191) e, infine, alle frequenti istanze in merito alle norme vincolanti d'impresa (cd. Bcr) e alle modalità per la loro approvazione.

Proprio con riferimento a tale ultimo profilo, chiarimenti sono stati forniti ad alcuni gruppi di imprese interessate ad avviare un procedimento volto all'adozione delle Bcr, facendo presente che il gruppo richiedente deve compilare l'*application form* secondo quanto indicato nel documento WP 264, per le *Bcr for controller*, e nel documento WP 265, in ordine alle *Bcr for processor*, rivolgendosi all'autorità capofila (*Lead Authority*), individuata sulla base dei criteri indicati nel par. 1 del WP 263. La procedura di approvazione delle Bcr è infatti condotta dall'autorità capofila la quale dialoga, in rappresentanza delle autorità di controllo, con il gruppo multinazionale interessato al fine di predisporre un progetto di decisione condiviso da sottoporre al Cepd ai sensi dell'art. 64, par. 1, lett. *f*), del RGPD. Il Garante ha precisato che, ove sia chiamato ad operare quale autorità capofila, l'istanza – cui deve essere allegato il testo di cui si compongono le Bcr con i rispettivi allegati, ivi compresa la *check list* di cui al WP 256 debitamente compilata – va trasmessa all'Autorità ai sensi dell'art. 46, par. 1, lett. *b*), del RGPD. Al termine della fase istruttoria, che può comportare la richiesta di maggiori informazioni o di ulteriore documentazione, verrà comunicato al richiedente e alle altre autorità di controllo interessate lo schema di decisione adottato.

18 L'attività ispettiva

18.1. *I poteri di indagine e il nuovo regolamento del Garante n. 1/2019*

Se la cornice normativa all'interno della quale si inscrivono i poteri di indagine del Garante è stata puntualmente descritta nella Relazione 2018, alla quale può quindi farsi rinvio (cfr. p. 170 ss.), merita qui soffermarsi sulle novità concernenti le modalità di svolgimento dell'istruttoria dei procedimenti sanzionatori previsti dal RGPD e dal decreto legislativo 10 agosto 2018, n. 101, rinvenibili nel regolamento n. 1/2019 (regolamento concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali – in G.U. 8 maggio 2019, n. 106).

Tale nuovo regolamento interno ha infatti declinato, valorizzandole, le attività ispettive e di controllo nonché le attività di revisione, previste dall'art. 58, par. 1, lett. *b*), del RGPD – all'insegna di un complessivo rafforzamento dei poteri istruttori delle autorità di protezione dei dati – effettuabili, anche con l'ausilio della Guardia di finanza (v. *infra*), presso il titolare o il responsabile del trattamento ovvero presso la sede dell'Autorità. In tale ambito sono state infatti introdotte alcune novità riguardanti le modalità di svolgimento delle attività di controllo realizzate a cura del Dipartimento attività ispettive prevedendo che, con l'ordine di servizio sottoscritto dal dirigente, sia possibile, in particolare:

- controllare, estrarre ed acquisire copia dei documenti, anche in formato elettronico;
- richiedere informazioni e spiegazioni;
- accedere alle banche dati ed agli archivi;
- acquisire copia delle banche dati e degli archivi su supporto informatico.

In capo al suddetto Dipartimento sono inoltre poste le attività di revisione sulla protezione dei dati personali che potranno essere avviate ai sensi dell'art. 58, par. 1, lett. *b*), del RGPD, presso il titolare o il responsabile del trattamento ovvero presso la sede dell'Autorità.

18.2. *La collaborazione con la Guardia di finanza*

Come anticipato, il Garante ha continuato ad avvalersi della preziosa e consolidata collaborazione della Guardia di finanza per lo svolgimento delle attività di controllo oggetto di un protocollo di intesa che dovrebbe essere aggiornato nel corso del 2020. Ciò sia per adeguare il testo alle sopravvenute modifiche di carattere normativo, sia per tener conto del nuovo assetto organizzativo dei Reparti speciali che, a decorrere da luglio 2018, ha visto la soppressione del Nucleo speciale *privacy* e l'istituzione del Nucleo speciale tutela *privacy* e frodi tecnologiche.

Il nuovo protocollo d'intesa prevederà la messa a disposizione di nuove unità di personale della Guardia di finanza presso l'Autorità e, inoltre, dal punto di vista strategico, la possibilità per il Garante di avvalersi di personale specializzato del Corpo anche per la conduzione di ispezioni congiunte con altre autorità estere.

Da un punto di vista più strettamente operativo, invece, l'adozione del protocollo

18

ha finora consentito: una sempre maggiore semplificazione dei flussi documentali tra l'Ufficio e il Nucleo speciale tutela *privacy* e frodi tecnologiche (attraverso l'uso sistematico di strumenti di trasmissione telematici); l'introduzione di modalità di verifica *online* di possibili violazioni della normativa in materia di protezione dei dati personali (attraverso l'esame diretto di siti web, senza necessità di ispezioni *in loco*). Sulla base del suddetto protocollo, le informazioni e i documenti acquisiti nell'ambito degli accertamenti effettuati dal Corpo sono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge. Qualora nell'ambito dell'ispezione emergano violazioni penali, la Guardia di finanza procede direttamente alla segnalazione della notizia di reato all'Autorità giudiziaria, come accaduto nel 2019.

Come previsto dal ricordato protocollo d'intesa, è proseguita l'attività di formazione del personale del Corpo al fine di approfondire la conoscenza del complessivo quadro normativo in materia di protezione dei dati personali (soprattutto in ragione delle novità legislative introdotte dal RGPD e dal decreto legislativo n. 101/2018) e dei provvedimenti dell'Autorità.

Si può quindi osservare che, grazie alla sinergia ormai collaudata con il Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza, il Garante ha potuto giovarsi di un dispositivo di controllo flessibile ed articolato, in grado di integrare l'attività ispettiva svolta direttamente dal competente dipartimento dell'Autorità, consentendo così lo svolgimento, efficace e tempestivo, di tutte le verifiche *in loco* che si rendono necessarie per garantire il rispetto della protezione dei dati personali su tutto il territorio nazionale.

18.3. *La programmazione dell'attività ispettiva*

Quanto alle attività svolte, le ispezioni, pari a 147 nel 2019, sono state effettuate sulla base di programmi elaborati, secondo linee di indirizzo stabilite dal Collegio, con delibere di programmazione recanti gli ambiti del controllo e gli obiettivi numerici da conseguire. Come di consueto, le linee generali della programmazione dell'attività ispettiva sono state rese pubbliche attraverso il sito web del Garante (*Newsletter* 25 marzo 2019, n. 451, doc. web n. 9094437; *Newsletter* 28 ottobre 2019, n. 458, doc. web n. 9172442) e, sulla base dei criteri così fissati, l'Ufficio ha individuato i titolari dei trattamenti da sottoporre a controllo e ha istruito i conseguenti procedimenti. Il programma relativo al 2019 ha previsto che l'attività ispettiva fosse indirizzata, in particolare, nei seguenti settori:

- trattamenti effettuati dall'Istat, per una verifica preliminare sul SIM (Sistema Integrato di Microdati) e altri sistemi informativi statistici come da parere sul programma statistico nazionale del 20 ottobre 2015;
- trattamenti di dati personali effettuati per il rilascio dell'identità federata (Spid);
- trattamenti di dati personali effettuati da istituti bancari, con particolare riferimento ai flussi di cui all'Anagrafe dei conti correnti;
- trattamenti di dati personali effettuati da società per attività di *marketing*;
- trattamenti di dati personali effettuati da enti pubblici, con riferimento a banche dati di notevoli dimensioni;
- trattamenti di dati personali effettuati da società con particolare riferimento all'attività di profilazione degli interessati che aderiscono a carte di fidelizzazione;
- trattamenti di dati personali effettuati mediante applicativi per la gestione

delle segnalazioni di condotte illecite (cd. *whistleblowing*);
- trattamenti di dati personali effettuati da intermediari per la fatturazione elettronica;
- trattamenti di dati personali effettuati da società rientranti nel settore della cd. *food delivery*;
- trattamenti di dati personali in ambito sanitario effettuati da parte di società private.

Come più estesamente specificato al par. 18.4, nel periodo di riferimento sono state effettuate verifiche, anche in altri settori concernenti:
- l'adozione di misure di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di particolari categorie di dati personali;
- la liceità e correttezza dei trattamenti di dati personali, con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso, nei casi in cui questo è necessario, nonché alla durata della conservazione dei dati nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee.

In tutta l'attività è stata prestata particolare attenzione ai profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate, nonché al rispetto del generale principio di responsabilizzazione posto in capo al titolare del trattamento dall'art. 5 del RGPD.

18.4. *I principali settori oggetto di controllo*

Oltre a quanto già riportato al par. 18.2, le ispezioni effettuate dall'Autorità nel 2019 hanno riguardato le seguenti categorie di titolari del trattamento:
- grandi gruppi alberghieri, in relazione al trattamento di dati personali della clientela, anche qualora svolto tramite siti web, al fine di verificare, nell'ambito dei diversi servizi offerti, le categorie di dati raccolti e le tipologie di trattamenti effettuati, tra cui l'eventuale profilazione o attività di *marketing* nei confronti degli interessati, le misure di sicurezza previste e l'eventuale comunicazione di dati personali a soggetti terzi;
- soggetti esercenti l'attività di *call center*, con riferimento al trattamento dei dati personali delle persone contattate, al fine di verificare, in particolare, le modalità di rilascio dell'informativa e di acquisizione del consenso o di registrazione del diniego, nonché le fonti di acquisizione delle liste dei destinatari delle chiamate telefoniche e l'effettività del riscontro delle stesse con il Registro delle opposizioni;
- gruppi societari, per la verifica delle modalità di trattamento dei dati personali in relazione al rilascio di carte di fidelizzazione, delle modalità dell'eventuale profilazione della clientela, anche a fini di *marketing*, nonché della sussistenza dei relativi presupposti giuridici;
- società di intermediazione immobiliare di rilevanza nazionale, in relazione al trattamento di dati personali della clientela, anche qualora svolto tramite siti web, al fine di verificare, nell'ambito dei diversi servizi offerti, le categorie di dati raccolti e le tipologie di trattamenti effettuati, tra cui l'eventuale attività di *marketing* nei confronti degli interessati o di comunicazione dei dati personali a soggetti terzi, le modalità ed i tempi di conservazione dei dati trattati;
- *tour operator* di rilevanti dimensioni, in relazione al trattamento di dati personali della clientela, anche qualora svolto tramite siti web, al fine di verificare, nell'ambito dei diversi servizi offerti, le categorie di dati raccolti e

le tipologie di trattamenti effettuati, tra cui l'eventuale attività di *marketing* nei confronti degli interessati o di comunicazione dei dati personali a soggetti terzi, le modalità ed i tempi di conservazione dei dati trattati;

- circoli sportivi, in relazione al trattamento di dati personali della clientela, anche qualora svolto tramite siti web, al fine di verificare le categorie di dati raccolti (eventualmente, anche di tipo particolare ai sensi dell'art. 9 del RGPD) e le modalità di rilascio dell'informativa e dell'acquisizione del consenso della clientela, l'eventuale attività di *marketing* nei confronti degli interessati o di comunicazione dei dati personali a soggetti terzi, nonché l'eventuale utilizzo di impianti di videosorveglianza.

In relazione a quanto emerso dagli accertamenti, effettuati anche nei confronti di singoli titolari del trattamento per esigenze istruttorie connesse a segnalazioni e reclami pervenuti, sono state effettuate numerose proposte di adozione di provvedimenti inibitori e/o prescrittivi per conformare il trattamento alla legge, a fronte delle quali il Garante, come riportato nel prossimo paragrafo, ha adottato alcuni provvedimenti particolarmente significativi.

18.5. *I provvedimenti adottati dal Garante a seguito dell'attività ispettiva*

A seguito dei controlli ispettivi e di connesse penetranti attività istruttorie l'Autorità ha realizzato:

- interventi sui trattamenti illeciti mediante provvedimenti cautelari previsti dalla legge (blocco e divieto) definendo altresì le misure necessarie da prescrivere per rendere il trattamento conforme alla legge (contrasto dell'illecito);
- verifiche sullo stato di attuazione delle prescrizioni adottate dal Garante nei diversi contesti applicando sanzioni all'esito di accertati inadempimenti al fine di prevenire futuri illeciti (attività preventiva);
- acquisizioni di tutti gli elementi utili a comprendere nuovi fenomeni emergenti che impattano sul diritto alla protezione dei dati personali degli interessati, in modo da definire tempestivamente le misure e gli accorgimenti che devono essere adottati da tutti i soggetti che sono coinvolti nei trattamenti (attività conoscitiva).

Nei casi in cui l'Autorità ha accertato la violazione di norme del Codice o del RGPD che prevedono una sanzione amministrativa, sono stati avviati anche i relativi procedimenti sanzionatori.

19 L'attività sanzionatoria

Come meglio illustrato nel successivo par. 19.5, l'applicabilità del RGPD e l'approvazione del decreto legislativo n. 101/2018 hanno profondamente modificato il quadro sanzionatorio in materia di protezione dei dati personali.

Dal punto di vista dell'operatività, mentre nel 2018 l'Autorità ha dovuto gestire l'attività straordinaria di definizione agevolata dei procedimenti sanzionatori in materia di protezione dei dati personali pendenti alla data del 25 maggio 2018, nel 2019 il Garante ha dovuto provvedere alla gestione straordinaria dell'avvio delle procedure di riscossione coattiva per tutti i procedimenti sanzionatori non definiti in via agevolata o per i quali non fossero state presentate nuove memorie difensive.

Al riguardo, occorre rammentare che l'art. 18, d.lgs. n. 101/2018 aveva introdotto la facoltà per i trasgressori, in deroga all'art. 16, l. 24 novembre 1981, n. 689, di definire in via agevolata, mediante il pagamento in misura ridotta di una somma pari a due quinti del minimo edittale, i procedimenti sanzionatori riguardanti le violazioni di cui agli artt. 161, 162, 162-*bis*, 162-*ter*, 163, 164, 164-*bis*, comma 2 e agli artt. 33 e 162, comma 2-*bis*, che non risultassero, alla data di applicazione del RGPD, già definiti con l'adozione dell'ordinanza-ingiunzione. Tale pagamento, per i soggetti interessati, andava effettuato entro il termine del 18 dicembre 2018. Per coloro che, invece, non avessero voluto avvalersi di tale facoltà, restava la possibilità di presentare nuove memorie difensive entro l'ulteriore termine del 16 febbraio 2019. In assenza di entrambe le condizioni, cioè in caso di inerzia dei trasgressori, l'art. 18 del citato d.lgs. n. 101/2018 prevede che l'atto con il quale sono stati notificati gli estremi della violazione o l'atto di contestazione immediata assumessero il valore dell'ordinanza-ingiunzione di cui all'art. 18, l. n. 689/1981, senza obbligo di ulteriore notificazione (art. 18, comma 2, d.lgs. n. 101/2018).

Vediamo quindi, di seguito, con particolare riferimento ai procedimenti facenti riferimento a condotte tenute vigente la normativa anteriore al RGPD (per quelle successive al 25 maggio 2018 se ne è dato conto nella Relazione in sede di trattazione dei vari settori di interesse), il dettaglio delle attività portate a compimento nel 2019.

19.1. *Violazioni penali*

In relazione alle istruttorie effettuate nel 2019 sono state trasmesse n. 9 segnalazioni di violazioni penali all'Autorità giudiziaria, di cui:

- quattro per inosservanza di un provvedimento del Garante;
- quattro per falsità nelle dichiarazioni al Garante;
- una per accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.).

19.2. *Sanzioni amministrative adottate in relazione alla disciplina previgente*

Sono stati avviati n. 32 procedimenti sanzionatori amministrativi relativamente a violazioni commesse anteriormente alla data di applicabilità del RGPD. I relativi atti di contestazione sono stati adottati sulla base della disciplina prevista dalla legge

19

n. 689/1981, in virtù del relativo rimando operato dal Codice prima dell'entrata in vigore del decreto legislativo n. 101/2018. Come anticipato, tutti i suddetti procedimenti sanzionatori hanno riguardato l'accertamento di violazioni delle norme in materia di protezione dei dati personali avvenute prima del 25 maggio 2018, cioè nella piena vigenza del Codice nella sua formulazione precedente alle modifiche introdotte dal decreto legislativo n. 101/2018, sì che, in applicazione del principio *tempus regit actum*, le violazioni sono state contestate secondo la procedura prevista dalla citata legge n. 689/1981. All'accertamento delle violazioni amministrative previste dal Codice poteva procedere:

- il personale dell'Ufficio del Garante addetto all'attività ispettiva a cui, sulla base di quanto previsto dall'art. 156, comma 9, del Codice, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, è attribuita la qualifica di ufficiale o agente di polizia giudiziaria;
- fino al 25 maggio 2018, chiunque rivestisse, nell'esercizio delle proprie funzioni, la qualifica di ufficiale o agente di polizia giudiziaria, in base a quanto previsto dall'art. 13, l. n. 689/1981.

Le 32 violazioni in relazione alle quali sono stati avviati procedimenti sanzionatori nel 2019 hanno riguardato:

- 15 casi di trattamento illecito per violazione delle disposizioni contenute nell'art. 167 (es., trattamento di dati senza il consenso degli interessati; diffusione di dati sui siti internet delle p.a.; comunicazioni elettroniche indesiderate), sanzionati dall'art. 162, comma 2-*bis*;
- 9 casi di omessa o inidonea informativa all'interessato, sanzionati dall'art. 161;
- 2 casi di omessa o incompleta notificazione ai sensi degli artt. 37 e 38, sanzionati dall'art. 163;
- 2 casi di violazione di disposizioni del Codice in relazione a banche dati di particolare rilevanza o dimensioni, sanzionati dall'art. 164-*bis*, comma 2;
- 1 caso di omessa adozione delle misure minime di sicurezza di cui all'art. 33, sanzionato dall'art. 162, comma 2-*bis*;
- 1 caso di inosservanza di un provvedimento del Garante, sanzionato dall'art. 162, comma 2-*ter*;
- 1 caso di omessa informazione o esibizione di documenti al Garante, sanzionato dall'art. 164;
- 1 caso di cui agli artt. 24 e 25, d.lgs. n. 101/2018, relativo all'applicabilità di sanzioni amministrative a violazioni penali commesse anteriormente.

I procedimenti sanzionatori definiti nell'anno 2019 con provvedimento di ordinanza adottato dall'Autorità, relativamente a violazioni contestate (anche) negli anni precedenti al 2019 e non definite all'epoca attraverso il pagamento spontaneo in misura ridotta da parte del contravventore, sono stati 476. Di questi, 272 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 3.315.990 euro) e 204 si sono invece conclusi con l'archiviazione in quanto la parte ha potuto dimostrare nel procedimento di non aver commesso la violazione contestata o che la violazione non era ad essa imputabile.

Relativamente alle suddette ordinanze-ingiunzione adottate dall'Autorità, appare necessario evidenziare alcuni significativi provvedimenti, tra cui si segnalano, per la particolare rilevanza economica e per il considerevole numero di interessati coinvolti, quelli adottati nei confronti di Facebook Ireland, Facebook Italy e Vincall s.r.l.s.

Con il primo provvedimento (ordinanza-ingiunzione 14 giugno 2019, n. 134, doc. web n. 9121486), il Garante ha applicato a Facebook Ireland e Facebook

19

Italy, in solido, una sanzione di un milione di euro per violazioni emerse nel corso dell'istruttoria relativa al caso Cambridge Analytica. Da tale istruttoria è emerso infatti che 57 utenti italiani avevano "scaricato" l'*app* Thisisyourdigitallife attraverso la funzione "Facebook Login" e che, in base alla possibilità consentita da questa funzione di condividere i dati degli "amici", l'applicazione aveva poi acquisito i dati di ulteriori 214.077 utenti italiani, senza che questi l'avessero "scaricata", fossero stati informati della cessione dei loro dati e avessero espresso il proprio consenso a questa cessione. Riguardo a tali condotte sono state contestate violazioni in tema di informativa e consenso con riferimento ad una banca dati di rilevante dimensioni.

Con il secondo provvedimento (ordinanza-ingiunzione 11 aprile 2019, n. 95, doc. web n. 9116053), il Garante ha comminato una sanzione di oltre due milioni di euro ad una società italiana che aveva svolto, tramite un *call center* operante in Albania, attività di *telemarketing* e *teleselling* per conto di una società del settore energetico senza aver reso alcuna informativa alle persone contattate e senza acquisire il consenso al trattamento dei dati personali per finalità di *marketing*. La società aveva infatti incaricato il *call center* di contattare telefonicamente potenziali clienti utilizzando numerazioni telefoniche raccolte dal *call center* stesso, senza che la lista dei contatti fosse stata fornita o validata dal titolare o dal responsabile del trattamento. Dopo il primo contatto da parte del *call center*, le persone che avevano manifestato la volontà di sottoscrivere un contratto venivano richiamate dalla società italiana. La sanzione è stata definita cumulando ogni violazione contestata per singolo interessato e tenendo conto della gravità della condotta della società, posta in essere in un quadro di disinteresse e unilaterale semplificazione della disciplina nazionale in tema di informativa e consenso nei trattamenti per finalità promozionali.

Il Garante ha altresì affrontato la questione dell'applicazione del principio di legalità di cui all'art. 1, comma 2, l. n. 689/1981 in relazione all'entrata in vigore del RGPD (cfr. ordinanza-ingiunzione 28 marzo 2019, n. 101, doc. web n. 9117126). In questo caso l'Autorità ha ribadito che, al fine della determinazione della norma applicabile sotto il profilo temporale, deve trovare applicazione il principio di legalità di cui all'art. 1, comma 2, l. n. 689/1981. Tale disposizione, nel prevedere che "le leggi che prevedono sanzioni amministrative si applicano soltanto nei casi e nei tempi in esse considerati", asserisce la ricorrenza del principio del *tempus regit actum*. Ne consegue l'obbligo di prendere in considerazione la norma vigente al momento della commessa violazione. Quindi, nel caso in cui la condotta illecita sia stata commessa anteriormente all'applicazione del RGPD (vale a dire prima del 25 maggio 2018), dovrà essere applicata la disposizione vigente al momento in cui la condotta oggetto di contestazione è stata posta in essere.

Con l'ordinanza-ingiunzione del 7 marzo 2019, n. 56 (doc. web n. 9123989) l'Autorità ha comminato una sanzione amministrativa di 10.000 euro nei confronti di un ente pubblico per aver effettuato un illecito trattamento di dati giudiziari, consistente nella comunicazione a terzi di informazioni circa un procedimento penale ancora in corso a carico di uno spedizioniere, in assenza di una norma di legge o di regolamento che espressamente lo prevedesse. La parte si è difesa sostenendo che i dati utilizzati nei verbali di revisione dell'accertamento erano indispensabili rispetto alla finalità del recupero tempestivo nei confronti del doganiere (quale obbligato in solido della società importatrice). Tuttavia è stato accertato che sia la normativa comunitaria (reg. CEE 2913/1992) che la legislazione italiana in materia (l. 25 luglio 2000, n. 213) si limitano a prevedere la responsabilità solidale dello spedizioniere nel caso di dichiarazioni doganali irregolari, di cui è o avrebbe dovuto essere a conoscenza, ma in nessun caso è prevista la possibilità di portare a conoscenza di terze parti i dati giudiziari dello spedizioniere. Anche il regolamento

19

di attuazione degli artt. 20 e 21 del Codice, adottato dall'ente pubblico in data 1° aprile 2009, individua, quali destinatari della comunicazione di dati giudiziari, unicamente le amministrazioni e le autorità doganali italiane ed estere ai fini della mutua assistenza amministrativa, mentre non prevede che rientri tra le operazioni eseguibili la comunicazione di dati giudiziari a soggetti terzi.

Con l'ordinanza-ingiunzione del 14 febbraio 2019, n. 49 (doc. web n. 9106367) l'Autorità ha comminato una sanzione di 16.000 euro ad un medico che aveva utilizzato gli indirizzi di circa 3.500 ex pazienti per inviare lettere a sostegno di un candidato alle elezioni politiche regionali, senza che gli interessati avessero espresso alcuno specifico consenso al riguardo. In particolare, poiché i dati non erano stati raccolti direttamente presso gli interessati (bensì ricevuti tramite l'istituto presso cui il professionista aveva svolto attività lavorativa, al momento della cessazione del rapporto di lavoro), è stata contestata, oltre alla mancata acquisizione del consenso, anche l'omessa informativa, che non era stata resa né al momento della registrazione dei dati dei pazienti né alla prima comunicazione.

Infine nell'ordinanza-ingiunzione del 4 aprile 2019, n. 91 (doc. web n. 9116781) l'Autorità ha ribadito i requisiti necessari per l'accesso alla facoltà di definizione agevolata delle violazioni in materia di protezione dei dati personali di cui all'art. 18, d.lgs. 10 agosto 2018, n. 101. Nel suddetto provvedimento, infatti, è stato evidenziato che il citato articolo, al comma 1, prevedeva che potessero essere oggetto di definizione agevolata i soli procedimenti sanzionatori avviati, con l'adozione del verbale di contestazione, in data antecedente al 25 maggio 2018. Quindi, tutte le violazioni accertate con altrettanti verbali di contestazione elevati in data successiva al 25 maggio 2018, ovvero successivamente a quella di applicazione del RGPD, non potevano essere definibili in via breve.

19.3. *Riscossione coattiva delle sanzioni*

Come accennato, il decreto legislativo n. 101/2018 ha introdotto talune importanti novità anche in relazione alla definizione agevolata delle violazioni in materia di protezione dei dati personali, a decorrere dal 19 settembre 2018. L'art. 18 del citato decreto, in particolare, ha introdotto la possibilità di definire in maniera agevolata taluni procedimenti sanzionatori (riguardanti le violazioni degli artt. 161, 162, 162-*bis*, 162-*ter*, 163, 164, 164-*bis*, comma 2, 33 e 162, comma 2-*bis*, del Codice) non ancora definiti alla data del 25 maggio 2018, mediante l'adozione di ordinanza-ingiunzione.

Alla data di entrata in vigore del predetto decreto, rientravano nell'ambito di applicazione dello stesso circa n. 1.688 procedimenti sanzionatori, per un totale complessivo di importi contestati pari a 26.955.734 euro. In relazione a tali procedimenti sanzionatori era quindi ammesso, come già in precedenza ricordato, il pagamento in misura ridotta, entro novanta giorni dalla data di entrata in vigore del d.lgs. n. 101/2018 (pertanto, entro il 18 dicembre 2018) di una somma pari a due quinti del minimo edittale.

In realtà, la suddetta procedura di definizione agevolata non ha registrato un'elevata adesione da parte dei soggetti coinvolti. Inoltre, un ristretto numero di soggetti ha presentato nuove memorie difensive entro il termine del 16 febbraio 2019, previsto dall'art. 18, d.lgs. n. 101/2018.

Ciò ha comportato che, nel corso del 2019, l'Autorità ha provveduto ad effettuare n. 735 iscrizioni a ruolo relativamente ai procedimenti sanzionatori definiti automaticamente, per effetto delle previsioni di cui al citato art. 18, in seguito al

mancato esercizio della facoltà di definizione agevolata o di presentazione di nuove memorie da parte dei trasgressori. In relazione a tali procedimenti, l'importo complessivamente iscritto a ruolo nel corso del 2019 è stato pari a 12.243.267 euro.

Occorre evidenziare che tale attività ha dato origine ad una mole di richieste di riesame o di annullamento in via di autotutela delle cartelle esattoriali notificate, nonché di richieste di informazioni ed istanze di accesso ai documenti ai sensi della legge n. 241/1990, con conseguente rilevante onere di gestione amministrativa delle suddette istanze.

Oltre alle somme sopra evidenziate, l'Autorità ha provveduto ad avviare la riscossione coattiva delle sanzioni irrogate con i provvedimenti di ordinanza-ingiunzione, adottati nel corso dell'anno, per i quali i trasgressori non hanno proceduto al versamento degli importi dovuti. Tale attività ha consentito l'iscrizione a ruolo di un importo complessivamente pari a 2.940.010 euro.

19.4. *Versamenti relativi alle sanzioni amministrative*

L'ammontare dei pagamenti effettivamente riscossi nell'anno 2019 da parte dei soggetti nei cui confronti sono stati avviati procedimenti sanzionatori amministrativi è risultato complessivamente pari a 2.972.363 euro di cui:

- 112.000 euro, pagati a titolo di definizione in via breve (art. 16, l. n. 689/1981);
- 1.933.786 euro, a seguito di ordinanze-ingiunzione adottate dal Garante;
- 917.717 euro, quali ulteriori entrate derivanti dalla riscossione coattiva di provvedimenti sanzionatori;
- 8.860 euro, a titolo di versamenti spontanei per la definizione agevolata dei procedimenti sanzionatori pendenti alla data del 25 maggio 2018, di cui all'art. 18, d.lgs. n. 101/2018.

Gli importi relativi alle sanzioni applicate dal Garante sono versati sul bilancio dello Stato. Sulla base di quanto previsto dall'art. 166, comma 7, del Codice, tali proventi, nella misura del 50% del totale annuo, sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 8, del Codice, per essere destinati alle specifiche attività di sensibilizzazione ed ispettive- nonché di attuazione del RGPD da parte del Garante.

19.5. *Il quadro sanzionatorio introdotto dal RGPD*

La complessa riforma della normativa in materia di protezione dati si caratterizza per il nuovo assetto delle sanzioni amministrative pecuniarie che rappresentano un elemento centrale con il quale le autorità di controllo possono articolare le misure correttive a fronte di inadempienze da parte del titolare o del responsabile del trattamento.

Se una puntuale ricostruzione del nuovo assetto normativo con riguardo alle sanzioni – profilo qualificante del RGPD, con particolare riferimento alla disposizione contenuta nell'art. 83 – è rinvenibile nella Relazione 2018 (alla quale si fa pertanto rinvio), merita qui rilevare che l'applicazione coerente delle norme in materia di sanzioni amministrative pecuniarie rappresenta un elemento centrale del nuovo regime introdotto dal RGPD per assicurare l'effettività del diritto alla protezione dei dati personali, congiuntamente alle altre misure previste dall'art. 58.

In tale prospettiva, ai sensi dell'art. 70, par. 1, lett. *e*), del RGPD, il Cepd ha la

19

facoltà di pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del RGPD; più precisamente, l'art. 70, par. 1, lett. *k*), specifica che è prevista l'elaborazione di linee guida riguardanti la previsione di sanzioni amministrative pecuniarie.

A tal fine, l'Autorità partecipa attivamente alla *Taskforce fining* istituita ai fini della predisposizione di tali linee guida per un'armonizzata applicazione dei criteri di valutazione fissati dall'art. 83, par. 2, del RGPD.

Per quanto attiene all'esperienza del Garante in relazione all'applicazione del nuovo regime sanzionatorio (significativamente più severo quanto ai massimi edittali previsti dal menzionato art. 83 del RGPD), benché ancora limitata in considerazione della fase di transizione che ha caratterizzato l'anno 2019 (e di rodaggio dell'Autorità con riguardo ai nuovi regolamenti interni), deve tuttavia rilevarsi, laddove se ne sono individuati i presupposti, l'avvenuta irrogazione di sanzioni pecuniarie di particolare rilievo rispetto all'esperienza pregressa, delle quali, come anticipato, si è sinteticamente dato conto nelle pagine della Relazione (cfr., in particolare, parr. 5.1, 5.1.1, 5.2 e 12; ma v. pure parr. 4.5.1, 10.1, 11.1, 11.2 e 11.3).

20 Il contenzioso giurisdizionale

20.1. *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 (art. 152 del Codice e art. 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 notevolmente sul numero delle notifiche effettuate al Garante relative a tale tipologia di giudizi: a fronte dei 14 ricorsi notificati nel 2017 e dei 16 nel 2018, nel 2019 sono stati notificati all'Autorità e da questa trattati 49 ricorsi.

Permane comunque la rilevanza dell'obbligo – purtroppo non sempre puntualmente adempiuto – per le cancellerie di trasmettere al Garante copia dei provvedimenti emessi dall'Autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6, del Codice).

Salvo quanto si dirà al par. 20.4, tale strumento, unitamente alle notifiche dei ricorsi, potrà consentire all'Autorità di avere conoscenza dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e di svolgere il ruolo di segnalazione al Parlamento e al Governo in relazione agli interventi normativi ritenuti necessari.

20.2. *I profili procedurali*

In tema di incompetenza territoriale, il Tribunale di Pisa, con ordinanza del 17 gennaio 2019, n. 1847, ha dichiarato la propria incompetenza in favore del Tribunale di Milano. Nei confronti di un'azione intentata contro una nota multinazionale del digitale con sede legale a Milano, secondo l'adito Tribunale di Pisa, infatti, il giudice competente avrebbe dovuto essere il Tribunale di Milano, ritenendo che l'art. 10, comma 2, d.lgs. n. 150/2011, riprendendo la previsione di cui all'art. 152 del Codice, stabilisce che: "È competente il tribunale del luogo in cui ha la residenza il titolare del trattamento dei dati, come definito dall'articolo 4 del decreto legislativo 30 giugno 2003, n. 196".

20.3. *Le opposizioni ai provvedimenti del Garante*

L'anno 2019 ha registrato un incremento nella proposizione delle opposizioni a provvedimenti dell'Autorità: 109 a fronte dei 101 ricorsi del 2018. Di queste, 50 (di cui 5 cartelle esattoriali emesse ex art. 18, d.lgs. n. 101/2018) si riferiscono a opposizioni a ordinanze-ingiunzioni, in leggero calo rispetto alle 59 del 2018. Di seguito si dà conto delle sentenze di maggior rilievo.

Opposizioni a provvedimenti

Complessivamente l'Autorità ha avuto notizia di 9 decisioni dell'Autorità giudiziaria relative a opposizioni a provvedimenti del Garante, il quale si è sempre costituito tramite l'Avvocatura dello Stato territorialmente competente.

20

Due decisioni, risolte a favore delle tesi del Garante, hanno riguardato l'invio tramite *e-mail* di comunicazioni indesiderate: in un caso, per finalità di natura promozionale e commerciale (Trib. Milano, 28 marzo 2019, n. 2629, su provv. 26 ottobre 2017, n. 437, doc. web n. 7320903); in un altro, con contenuto politico e finalità propagandistica (Trib. Napoli, 15 febbraio 2019, n. 1764, su provv. 25 gennaio 2018, n. 66 (doc. web n. 6240230). Ferma la necessità di un'esatta individuazione, caso per caso, del titolare del trattamento, del responsabile o della presenza di situazioni di contitolarità, l'invio di tali comunicazioni è subordinato al consenso libero e specifico, nonché documentato per iscritto, dell'interessato. Soprattutto, con specifico riferimento al secondo caso, si è ritenuto che tale consenso non potesse essere desunto da precedenti relazioni interpersonali con l'interessato aventi natura e finalità diverse da quella politica sottesa alla comunicazione indesiderata.

In una pronuncia sul provvedimento 2 marzo 2017, n. 89 (doc. web n. 6344006), avente ad oggetto il rapporto tra la tutela del diritto all'immagine e quello di inchiesta, quale sottocategoria del diritto di cronaca, il Tribunale di Roma, con sentenza del 5 marzo 2019, n. 5071, ha ritenuto che la diffusione dell'immagine e del nominativo dell'interessato fossero eccedenti rispetto allo scopo della notizia che mirava solamente a sollecitare l'opinione pubblica e richiamarne l'attenzione su un dato argomento di rilevanza sociale, culturale ed educativa.

Un altro caso ha avuto ad oggetto il trattamento dei dati personali dei lavoratori mediante affissione delle contestazioni disciplinari ricevute su bacheche liberamente accessibili dal personale. Nel confermare il provvedimento del Garante del 13 dicembre 2018, n. 500 (doc. web n. 9068983), il Tribunale di Firenze, con sentenza del 2 agosto 2019, n. 5552, ha rilevato che il consenso espresso al momento dell'assunzione della qualità di socio lavoratore non può ritenersi adeguato per legittimare un trattamento particolarmente invasivo quale la sistematica pubblicazione dei volti dei dipendenti associata a delle "faccine" accompagnate da giudizi sintetici di valutazione (es. "assenteismo", "simulazione malattia", ecc.). Tale trattamento perseguiva un risultato illecito, sproporzionato, privo di giustificazione economica e disfunzionale rispetto allo scopo mutualistico connaturato all'essenza della società cooperativa. Il Tribunale ha concluso quindi che lo scopo di incentivare e organizzare il lavoro avrebbe potuto essere perseguito con comunicazione individuale dei risultati delle valutazioni, senza ostentazione degli stessi.

Con riferimento al perimetro applicativo del diritto di accesso di cui all'oggi abrogato art. 7 del Codice, la Corte di cassazione del 15 novembre 2018, n. 32533, ha ritenuto che lo stesso non potesse essere inteso in senso restrittivo, come mero diritto alla conoscenza di eventuali dati nuovi ed ulteriori rispetto a quelli già entrati nel patrimonio di conoscenza e, quindi, nella disponibilità dell'interessato, né, soprattutto, che il suo esercizio potesse essere sindacato alla luce di una specifica (e non richiesta dalla norma) limitazione in ordine alle concrete finalità per le quali il diritto di accesso può essere esercitato. È stato così confermato l'orientamento del Garante per il quale anche nei confronti dei cd. dati valutativi possono essere esercitati i diritti degli interessati, ad eccezione del diritto alla rettificazione e dell'integrazione, perché anche questi costituiscono dati personali.

In altri tre casi, invece, i ricorsi avverso provvedimenti del Garante sono stati respinti per motivi attinenti al rito o riguardanti aspetti procedurali dell'esercizio dei diritti tramite l'intervento del Garante, quali: il deposito tardivo del ricorso nella sua integralità, oltre i 30 giorni dalla notificazione del provvedimento opposto, ex art. 10, comma 3, d.lgs. n. 150/2011 (Trib. Chieti n. 672/2019, su provv. 13 luglio 2016, n. 303, doc. web n. 5408460); l'aver il Garante dichiarato il "non luogo a procedere" per avere il titolare del trattamento fornito riscontro all'interessato (Trib.

Cagliari n. 334/2019, su provv. 25 febbraio 2016, n. 90, doc. web n. 4885313) e aver quindi compensato le spese nella misura di 150 euro, pari ai soli diritti di segreteria versati dal ricorrente (Cass. civ. n. 15712/2019).

Un'ultima pronuncia riguarda un ricorso al TAR Lazio contro un provvedimento di diniego di accesso agli atti presentato dal Garante ai sensi dell'art. 5, comma 2, d.lgs. n. 33/2013 (cd. accesso civico generalizzato o universale). L'istante aveva chiesto accesso ad alcuni documenti processuali nonchè contabili (concernenti la liquidazione degli onorari dei professionisti); il TAR, dopo aver ricostruito la normativa, ha confermato il provvedimento di diniego del Garante con riferimento ad entrambe le tipologie di atti. In un caso perché alcuni dei documenti richiesti non erano né detenuti né disponibili presso il Garante; nell'altro perché, dopo aver il TAR ricordato che tale forma di accesso è funzionale a un interesse pubblico ravvisabile nel controllo generalizzato e diffuso sull'attività delle pp.aa. e riscontrato invece che le finalità espresse dall'istante riguardavano il controllo dell'attività dei privati o i rapporti tra essi intercorrenti, ha ritenuto quest'ultima finalità alla base della richiesta di accesso ai restanti documenti non rientrante tra gli scopi per i quali la legge riconosce il diritto di accesso civico generalizzato (TAR Lazio, sez. prima *Quater*, 28 marzo 2019, n. 4122).

20

Accesso civico

In un giudizio originato dall'impugnazione di un provvedimento del Garante relativo alla pubblicazione in rete delle situazioni reddituali e patrimoniali di tutti i titolari di incarichi dirigenziali (e loro parenti stretti) è stata sollevata questione di legittimità costituzionale della normativa che prevede tale pubblicità. La Corte costituzionale, con sentenza del 21 febbraio 2019, n. 20, ha quindi analizzato la legittimità costituzionale dell'art. 14, commi 1-*bis* e 1-*ter*, d.lgs. 4 marzo 2013, n. 33 (cd. decreto trasparenza), in riferimento agli artt. 2, 3, 13 e 117, primo comma, della Costituzione – quest'ultimo in relazione agli artt. 7, 8 e 52 della CDFUE, all'art. 5 della Convenzione n. 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, nonché agli artt. 6, par. 1, lett. *c*), 7, lett. *c*) ed *e*), e 8, par. 1 e 4, della direttiva 95/46/CE – , disposizione che aveva di fatto equiparato gli obblighi di trasparenza gravanti sui dirigenti a quelli imposti ai titolari di incarichi politici, di amministrazione, di direzione o di governo di livello statale, regionale e locale. La Corte, se da un lato ha rilevato che la disciplina censurata non superasse il test di proporzionalità, in quanto l'onere di pubblicazione imposto risultava sproporzionato rispetto alla finalità principale perseguita (contrasto alla corruzione nell'ambito della p.a.) e la misura scelta non risultava quella meno restrittiva dei diritti fondamentali in potenziale tensione, dall'altro ha rilevato che una declaratoria d'illegittimità costituzionale che si fosse limitata alla semplice ablazione della disposizione censurata avrebbe lasciato del tutto privi di considerazione principi costituzionali meritevoli di tutela.

Pubblicazione dei dati relativi a redditi e patrimonio dei dirigenti pubblici

Ferma la necessità di un intervento del legislatore, la Corte ha quindi valorizzato la distinzione posta all'art. 19, commi 3 e 4, d.lgs. n. 165/2001, di due particolari categorie di incarichi dirigenziali, quelli di Segretario generale di ministeri e di direzione di strutture articolate al loro interno in uffici dirigenziali generali (comma 3) e quelli di funzione dirigenziale di livello generale (comma 4), per i quali le competenze loro attribuite rendono manifesto lo svolgimento di attività di collegamento con gli organi di decisione politica, con i quali il legislatore presuppone l'esistenza di un rapporto fiduciario, tanto da disporre che i suddetti incarichi siano conferiti su proposta del ministro competente, e quindi di compiti di elevatissimo rilievo. Tale assunto rende non irragionevole, solo per queste figure, il mantenimento in capo ad essi degli obblighi di trasparenza di cui si discute.

In conclusione, la Corte ha dichiarato l'illegittimità costituzionale dell'art. 14,

20

comma 1-*bis*, d.lgs. n. 33/2013, nella parte in cui prevede che le pp.aa. pubblicano i dati di tutti i titolari di incarichi dirigenziali, a qualsiasi titolo conferiti, ivi inclusi quelli conferiti discrezionalmente dall'organo di indirizzo politico senza procedure pubbliche di selezione, anziché solo per i titolari degli incarichi dirigenziali previsti dall'art. 19, commi 3 e 4, d.lgs. 30 marzo 2001, n. 165, con riferimento alla lett. *f*) dello stesso articolo, mentre ha dichiarato non fondate le questioni di legittimità costituzionale con riferimento alla lett. *c*) dello stesso.

Inammissibile è stata invece dichiarata le questioni di legittimità costituzionale dell'art. 14, comma 1-*ter*, d.lgs. n. 33/2013.

Opposizioni alle ordinanze-ingiunzione

Il Garante, avuta notizia di 40 decisioni dell'Autorità giudiziaria relative a opposizioni ad ordinanze-ingiunzioni (delle quali 2 hanno avuto ad oggetto cartelle esattoriali), si è sempre costituito tramite l'Avvocatura dello Stato territorialmente competente.

Cartelle esattoriali

Nelle opposizioni promosse contro le cartelle di pagamento inviate per conto del Garante sulla base del credito da questo vantato, le questioni affrontate sono state di natura prettamente procedurale. In un caso, infatti, in seguito all'annullamento dell'ordinanza-ingiunzione che costituiva il presupposto di una cartella di pagamento, anche questa è stata annullata perché rimasta priva di titolo esecutivo (Trib. Catania, 27 marzo 2018, n. 1355). In un secondo caso, invece, su concorde richiesta delle parti, il Giudice ha dichiarato la cessazione della materia del contendere (Trib. Cagliari, 25 ottobre 2019, n. 2398).

Informativa e consenso

La maggior parte delle opposizioni a ordinanza-ingiunzione erano dirette a negare l'applicazione di istituti importanti della protezione dei dati personali, quale l'obbligo di fornire l'informativa ex art. 13, d.lgs. n. 196/2003 (nella sua versione antecedente alle modifiche apportate dal d.lgs. n. 101/2018) e la conseguente acquisizione del consenso ex art. 23 del medesimo Codice. Innanzitutto, con riferimento all'ambito di applicazione delle norme contenute nel Codice, l'art. 5, comma 3, dello stesso ne escludeva l'applicazione ai trattamenti effettuati da persone fisiche per fini esclusivamente personali e che non prevedano la comunicazione sistematica o diffusione dei dati. Diversamente, se il trattamento risponde ad una finalità di natura professionale, istituzionale o similare, lo stesso dovrà essere svolto nel rispetto delle norme del Codice a partire dalla richiesta di consenso sulla base di idonea informativa (Trib. Ivrea, 26 settembre 2018, n. 937) che potrà essere rilasciata anche in forma orale (Trib. Alessandra, 17 aprile 2019, n. 150). L'importanza di rilasciare l'informativa e ottenere il consenso al trattamento da parte degli interessati è stata evidenziata anche con riferimento all'attività di *marketing* da parte degli operatori telefonici (Trib. Milano, 12 novembre 2018, n. 11373), all'interno di *form online* dove il consenso deve essere libero e specifico, ossia richiesto per ogni singola finalità distinguendo soprattutto quella pubblicitaria (Trib. Torino, 12 dicembre 2018, n. 5748) o per la creazione di *mailing list* e l'invio di *newsletter* ai propri utenti (Trib. Roma, 25 febbraio 2019, n. 4332 e Trib. Cagliari, 22 ottobre 2019, n. 2351). Con specifico riferimento alle comunicazioni commerciali indesiderate tramite sistemi automatizzati, la richiesta di consenso è prevista dall'art. 130 del Codice, né in ogni caso può considerarsi lecito l'utilizzo a tal fine dei dati personali reperibili su siti web senza il consenso dell'interessato ove questi siano liberamente accessibili per fini diversi da quelli promozionali (Trib. Torino, 22 luglio 2019, n. 2738). Infine, la richiesta di consenso è ancor più importante con riferimento al trattamento di "dati sensibili" (Trib. Treviso, 15 febbraio 2019, n. 366).

Trasparenza amministrativa

Altra parte delle opposizioni ha riguardato il tema della trasparenza amministrativa e quindi la ricerca del giusto bilanciamento tra la trasparenza e la riservatezza del singolo con riferimento agli atti pubblicati da enti pubblici in senso lato.

20

Due opposizioni hanno avuto ad oggetto la pubblicazione di dati personali comuni. La prima riguardava la diffusione di dati personali da parte di un comune oltre il periodo di legge di 15 giorni, sanzionato dal Garante con provvedimento 14 dicembre 2017, n. 534 (doc. web n. 8052263), poi annullato dal Tribunale di Udine, con sentenza del 24 ottobre 2019, n. 586, per il quale la pubblicazione dell'atto era resa obbligatoria da norme di legge; inoltre, la pubblicazione dei dati in esso contenuti non violava i principi di necessità, pertinenza e non eccedenza rispetto allo scopo della pubblicazione e la visibilità di tali documenti oltre il periodo previsto dalla legge era dovuto all'utilizzo di un meccanismo informativo (la memorizzazione e l'utilizzo reiterato dell'URL inerente la pagina pubblicata) utilizzato non da chiunque ma dal diretto interessato per controllare il persistere della pubblicazione. La seconda opposizione riguardava la pubblicazione, da parte di un ente pubblico, di una graduatoria contenente sia i dati dei soggetti ammessi che di quelli non ammessi a un beneficio economico, in numero e tipologia non necessaria per fini di trasparenza. L'ordinanza-ingiunzione del 24 novembre 2016, n. 494 (doc. web n. 6018315) è stata però annullata dal Tribunale di Firenze, con sentenza del 19 marzo 2019, n. 885, il quale ha ritenuto la pubblicazione di tali dati come "assolutamente indispensabile", negando quindi la sussistenza di una diffusione non giustificata, non necessitata e non pertinente. Il Garante ha quindi presentato ricorso per Cassazione.

Diversamente, con riferimento al caso di un comune che aveva pubblicato sul suo sito web i dati personali dei candidati non ammessi al concorso per il reclutamento del posto di comandante della polizia locale, la Corte di cassazione 7 agosto 2019, n. 21148, ha accolto il ricorso del Garante perché sul punto non vi era stata impugnazione della parte ma una pronuncia d'ufficio, cassando così la sentenza di primo grado che aveva annullato l'ordinanza del Garante per la asseritamente tardiva notifica della contestazione ex art. 14, l. n. 689/1981.

Molte altre decisioni, invece, riguardano la diffusione di dati personali idonei a rivelare lo stato di salute dell'interessato: è il caso della pubblicazione di alcune ordinanze di TSO da parte di un comune (Trib. Grosseto, 20 giugno 2019, n. 484), o della pubblicazione dei dati dei dipendenti comunali beneficiari dei permessi di astensione obbligatoria dal lavoro e congedo retribuito per lo stato di grave disabilità del padre convivente (Trib. Verona, 12 settembre 2019, n. 1947), oppure eccedenti o non pertinenti rispetto alle finalità perseguite, come la pubblicazione della qualifica di "invalido civile" di fianco ai nomi e agli altri dati personali degli aventi diritto all'interno di una graduatoria (Trib. Benevento, 15 luglio 2019, n. 1307). Infine, sul rapporto tra tutela dei dati personali e trasparenza, nell'esame di un caso in cui una provincia aveva diffuso dati sullo stato di salute dei suoi dipendenti, la Corte di cassazione 4 aprile 2019, n. 9382, ha affermato che "la tutela del dato sensibile prevale su una generica esigenza di trasparenza amministrativa sia sotto il profilo costituzionalmente rilevante della valutazione degli interessi in discussione sia sotto quello della sostanziale elusione della normativa sulla protezione dei dati personali, accentuata nel caso dei dati sensibili, ove si dovesse far prevalere una generica esigenza di trasparenza amministrativa nemmeno concretamente argomentata e provata. […] È consolidato il principio che i dati sensibili idonei a rilevare lo stato di salute possono essere trattati dai soggetti pubblici soltanto mediante modalità organizzative che rendano non identificabile l'interessato".

Notificazione

Altre pronunce hanno interessato il mancato rispetto dell'obbligo di notificazione del trattamento al Garante di cui agli artt. 37 e ss. del Codice. La maggior parte di esse riguardano l'utilizzo di sistemi di geolocalizzazione di veicoli aziendali o adibiti a noleggio nei quali il Garante ha sanzionato il mancato rispetto dell'ob-

20

bligo di notifica che, come rilevato anche dalla giurisprudenza, "è ben lungi dal costituire una violazione di natura esclusivamente formale" ma, poiché impedisce al Garante di acquisire informazioni relative ai trattamenti "più delicati" e valutare le iniziative più opportune, al contrario integra una violazione di particolare gravità (Trib. Milano, 11 gennaio 2019, n. 298). In un caso l'opposizione all'ordinanza-ingiunzione è stata rigettata, sebbene sia stata rideterminata la sanzione (Trib. Alessandria, 17 dicembre 2019, n. 932); nell'altro invece è stata accolta, con conseguente annullamento della sanzione del Garante, perché il Giudice, dopo aver rilevato che il sistema di geolocalizzazione dei veicoli adibiti al *car sharing* fosse attivo solo al di fuori degli orari di noleggio, al solo fine di verificare il corretto rilascio del mezzo negli stalli dedicati e che l'attivazione del GPS su un veicolo in uso dall'utente potesse essere effettuato solo su richiesta dell'Autorità giudiziaria, dell'utente stesso o del manutentore in caso di incidente, ha ritenuto che tali modalità non permettessero né una localizzazione continua né l'identificazione dell'utente e, quindi, non si integrasse un trattamento di dati soggetto all'obbligo di notifica (Trib. Parma, 23 gennaio 2019, n. 128). In un altro caso, infine, in cui la sanzione del Garante per omessa notificazione è stata confermata dal Giudice, il titolare aveva anche previsto un sistema di profilazione automatizzato che realizzava offerte personalizzate in base alla frequenza con cui l'utente usufruiva del servizio di *car sharing* (Trib. Livorno, 22 novembre 2018, n. 1202).

In altri due casi, invece, è stata sanzionata da parte del Garante la mancata notificazione con riferimento al trattamento di dati genetici e biometrici. Nel primo caso, l'ordinanza-ingiunzione è stata annullata per meri motivi processuali, non essendosi il Garante costituito nel rispetto dei termini di cui all'art. 416 c.p.c. (Trib. Firenze, 9 maggio 2019, n. 1451); il Garante ha presentato ricorso in Cassazione. Nel secondo il Giudice ha confermato la sanzione del Garante per mancata informativa e notificazione con riferimento al trattamento posto in essere da un istituto scolastico che, per due mesi e a titolo di sperimentazione, aveva installato un sistema biometrico di riconoscimento dei propri dipendenti, basato su impronte digitali, al fine di accertarne la presenza a lavoro (Trib. Taranto, 25 luglio 2019, n. 2553).

Videosorveglianza

Quattro opposizioni, tutte sostanzialmente respinte dai giudici aditi, hanno avuto ad oggetto il tema della videosorveglianza e, in particolare, la conservazione delle immagini per un periodo eccedente rispetto a quello suggerito all'interno del provvedimento generale del Garante dell'8 aprile 2010 (doc. web n. 1712680). In un primo caso il sistema di videosorveglianza era stato adottato da un comune (Trib. Bologna, 24 gennaio 2019, n. 20104), in due da una società privata (Trib. Nola, 28 marzo 2019, n. 533) e da un esercizio commerciale bar/birreria (Trib. Verona, 22 novembre 2019, n. 2592). In un ultimo caso, in un centro raccolta di scommesse sportive in un piano interrato ove erano collocate anche apparecchiature da gioco con vincite in denaro sulle quali puntava una videocamera ad infrarossi e il cui impianto di registrazione con relativo monitor era posto nel locale al piano terra ove avveniva l'esercizio di somministrazione di alimenti e bevande; rispetto a tale fattispecie, oltre al mancato rispetto dei termini di conservazione dei dati, sono stati contestati la mancata adozione di misure di sicurezza e l'informativa nella forma della cartellonistica che dà evidenza della presenza di un sistema di videosorveglianza (Trib. Novara, 28 novembre 2019, n. 880).

Attivazione non autorizzata di utenze telefoniche

Un altro gruppo di pronunce, tutte decise a favore del Garante, hanno riguardato l'attivazione di abbonamenti telefonici all'insaputa degli interessati, che si erano ritrovati schede sim a loro intestate senza autorizzazione, con i relativi costi che si accumulavano nel tempo. In un caso, in cui un interessato lamentava l'ingiustificata attivazione a proprio nome e a propria insaputa di 856 utenze telefoniche,

è stato respinto il ricorso contro l'ordinanza-ingiunzione del 16 maggio 2018, n. 297 (doc. web n. 9370122) che aveva inflitto una sanzione amministrativa pari ad 800.000 euro alla società di telecomunicazioni un trattamento di dati personali in assenza di fondamento di liceità, nonché l'illecita comunicazione dei dati di clienti a terzi (Trib. Milano, 4 aprile 2019, n. 3371).

Analogamente, un negozio di telefonia ha attivato utenze telefoniche non richieste a clienti che, invece, avevano richiesto l'esecuzione di altre operazioni, come il passaggio a un altro operatore con portabilità del numero (Trib. Roma, 26 novembre 2018, n. 22764). Infine, in due casi la Corte di cassazione ha accolto i ricorsi del Garante, confermandone così i provvedimenti sanzionatori, rinvenendo, nel primo, nell'attivazione non autorizzata di centinaia di schede sim un trattamento illecito di dati personali in assenza della previa informativa e l'acquisizione del consenso degli interessati (Cass. civ., 17 aprile 2019, n. 10740) e specificando, nel secondo, che "la contestazione dell'indebito utilizzo dei dati personali ha per presupposto, non solo logico ma anche effettivo e oggetto di specifica contestazione, l'accertamento dell'avvenuta acquisizione di quei dati in difetto della obbligatoria informazione da parte del responsabile del trattamento (non è consentito, infatti, che le schede siano state intestate a persone ignare di tale intestazione); informazione che, ovviamente, era onere del responsabile dimostrare di avere fornito ai soggetti i cui dati sono stati acquisiti e poi utilizzati a loro insaputa. […] In sostanza, la contestazione della mancata informativa di cui all'art. 13 (art. 161, applicato nel caso di specie), non può ritenersi esclusa per il fatto che il dato sia stato utilizzato, posto che l'utilizzazione presuppone la raccolta dello stesso nelle dovute forme stabilite dall'art. 13, e quindi nel rispetto dell'obbligo della necessaria informativa. […] Deve, quindi, escludersi che il Garante abbia fatto applicazione analogica dell'art. 13 del d.lgs. 196 del 2003 […]" (Cass. civ., 17 aprile 2019, n. 10741).

Comunicazione e diffusione

Altre opposizioni hanno avuto ad oggetto fattispecie illecite di comunicazione e diffusione di dati personali. In particolare, il testo previgente dell'art. 19 del Codice disciplinava la comunicazione di dati da parte di soggetti pubblici ammettendola solo in presenza di una norma di legge o regolamento. In mancanza di tale base normativa, la comunicazione era ammessa quando necessaria per lo svolgimento di funzioni istituzionali dell'ente titolare del trattamento. In un caso, il Tribunale di Roma, con sentenza del 4 aprile 2019, n. 2441, ha confermato l'ordinanza-ingiunzione del Garante del 18 luglio 2013, n. 358 (doc. web n. 2578201) nei confronti del Ministero della giustizia che aveva pubblicato sui luoghi di lavoro elenchi nominativi relativi al personale che aveva effettuato lavoro straordinario in luogo di dati numerici o aggregati. È stata ritenuta eccedente anche la pubblicazione oltre i limiti temporali previsti dalla legge, da parte di una regione, di dati riferiti a un dipendente messo in mobilità (Trib. Aosta, 3 maggio 2018, n. 127). Anche nei confronti di grandi società private il Garante ha rinvenuto fenomeni di comunicazione non autorizzata di dati, realizzatesi tramite malfunzionamenti di sistemi che hanno consentito a terzi di accedere ai dati personali degli interessati (Trib. Milano, 16 maggio 2019, n. 4428); così pure nel caso della comunicazione di dati da parte di un comune a una società, in assenza di norma di legge ma sul presupposto che quest'ultima perseguisse fini di interesse pubblico e pertanto potesse essere considerata quale incaricato di pubblico servizio, con parificazione ai soggetti pubblici per finalità di formazione ed inserimento nel mondo del lavoro. Tale qualificazione è stata contestata dapprima dal Garante, che ha conseguentemente emesso l'ordinanza-ingiunzione 26 aprile 2018, n. 251 (doc. web n. 9022020), e poi dal Tribunale di Spoleto che, con sentenza del 29 maggio 2019, n. 416, ha respinto l'impugnazione affermando che "la funzione di interesse pubblico non può comportare, *sic*

20

Varie

et simpliciter, la qualificazione della stessa come ente pubblico o come incaricato di un pubblico servizio, equiparato ai primi, nella materia dei dati personali, e ciò in considerazione della finalità cui la stessa è preordinata, ossia a tutelare la riservatezza di dati personali di soggetti privati. Ciò comporta che la nozione di ente pubblico, nella presente materia, debba essere interpretata in modo stringente, proprio perché la mancanza di una norma o di un regolamento che autorizzi la trasmissione, elemento negativo previsto *a contrario* dall'art. 19, comma 3 per i soggetti non privati o non qualificabili quali enti pubblici economici, si appalesa come previsione che affievolisce la tutela dei soggetti cui si riferiscono i dati trasmessi, facendo venire meno il penetrante controllo esercitato dal Garante e, quindi, la penetrante tutela al bene giuridico che la normativa tende a tutelare".

In due casi sono state confermate le ordinanze-ingiunzione nei confronti di soggetti che non avevano dato seguito alla richiesta di informazioni ricevuta dal Garante (Trib. Cosenza, 14 gennaio 2019, n. 57 e Trib. Torino, 5 febbraio 2019, n. 550).

In un altro, il Garante ha sanzionato un medico ex art. 169, comma 2, del Codice per non aver adottato le misure minime di protezione di cui all'art. 33 del medesimo Codice, avendo lo stesso consegnato alla moglie una chiavetta USB contenente dati sensibili riferiti ai suoi pazienti. Il Tribunale di Roma, con sentenza del 2 novembre 2018, n. 20990, ha affermato che "il primo comma della disposizione [art. 169 Codice] disciplina un reato contravvenzionale, sanzionato con la pena detentiva fino a due anni. Il secondo comma, invece, descrive un procedimento prescrizionale demandato all'attività amministrativa volto, da un lato, a conseguire la regolarizzazione delle attività dell'autore del fatto e, dall'altro, l'estinzione del reato: tale procedimento si articola nell'intimazione di un provvedimento recante le misure da adottare e, ove consti l'adozione delle stesse, in un atto del Garante che ammetta l'autore del reato a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa corrispondente. L'adempimento alle prescrizioni impartite e il pagamento della somma estinguono il reato. Si tratta, in altri termini, di un procedimento che integra una speciale causa di estinzione del reato". Ciò considerato, il Tribunale adito, nel condividere le tesi difensive del Garante, ha concluso per l'inammissibilità del ricorso in quanto "l'atto impugnato […] si iscrive nell'alveo di un procedimento penale e non costituisce espressione di un potere sanzionatorio amministrativo; il ricorrente dovrà quindi tutelare le proprie ragioni, ove lo ritenga, nella competente sede penale dove il procedimento, in assenza del pagamento e secondo le determinazioni del Pubblico Ministero, eventualmente proseguirà per l'accertamento dei fatti".

In un altro caso, il Tribunale di Napoli Nord, con sentenza dell'8 ottobre 2019, n. 2613, ha rigettato il ricorso avverso l'ordinanza-ingiunzione del 21 marzo 2018, n. 169 (doc. web n. 9004722) con la quale il Garante aveva sanzionato, ex artt. 162, comma 2-*bis*, in relazione agli artt. 169 e 19 del Codice, il fatto che un'azienda sanitaria rendesse possibile effettuare, attraverso l'*home page* del proprio sito web, una ricerca per campi all'esito della quale risultavano accessibili e modificabili da chiunque i dati personali forniti da coloro che usufruivano dei servizi *online* della stessa.

In un ultimo caso, con l'ordinanza-ingiunzione 31 marzo 2016, n. 148 (doc. web n. 4858951) il Garante ha sanzionato un consulente tecnico di un ufficio giudiziario per avere questo detenuto e continuato a trattare dati personali al di là dei termini fissati per i singoli incarichi, integrando così diverse violazioni alla normativa in materia di protezione dei dati personali (cfr. le linee guida in materia di trattamento dei dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero: provv. 26 giugno 2008, doc. web n. 1534086).

Il Tribunale di Palermo, con sentenza del 18 luglio 2019, n. 3563, ha annullato il provvedimento del Garante ritenendo che, nel caso di specie, "tutta la strumentazione informatica, i reperti e la banca dati oggetto di sequestro, era preordinata, perlomeno in parte, alla definizione di incarichi ancora pendenti […] e dunque, la relativa attività di trattamento dei dati personali ivi contenuti era legittimamente esercitata "nell'ambito giudiziario" e come tale annoverabile nella cornice derogatoria di cui al predetto art. 166 [del Codice]". Avverso la pronuncia pende ricorso in Cassazione.

20.4. *L'intervento del Garante nei giudizi relativi all'applicazione del Codice*

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.

In questo quadro, l'Autorità ha comunque seguito con attenzione tutti i contenziosi nei quali non ha ritenuto opportuno intervenire, chiedendo all'Avvocatura 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 RGPD, 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 ora 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". Il menzionato art. 154-*ter* del Codice, 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.

Occorre ancora considerare che in base al Codice l'Autorità giudiziaria deve comunicare al Garante la pendenza di una controversia, trasmettendo copia degli atti introduttivi (art. 10, comma 9, d.lgs. 1° settembre 2011, n. 150, 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". In tal senso osservazioni sono state presentate in due casi: uno concernente l'accesso della madre, per valutare il rischio procreativo, ai dati del neonato non riconosciuto affetto da gravi patologie; l'altro, la *class action* intentata da un'associazione di consumatori nei confronti di un importante *social network* per il risarcimento del danno derivante dall'illegittimo trattamento di dati personali.

21 Le relazioni comunitarie e internazionali

21.1. *La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dati*

Il Comitato europeo per la protezione dei dati (Cepd o Comitato) – che dal 2018 riunisce le autorità nazionali di controllo dei singoli Stati membri e dei tre Paesi che sono parti dell'Accordo sullo Spazio economico europeo (See) e il Garante europeo per la protezione dei dati (Gepd), con l'intervento, senza diritto di voto, della Commissione europea – ha proseguito la sua intensa attività volta a favorire il processo di adeguamento al RGPD e a dare piena attuazione allo stesso.

Nel corso dell'anno il Comitato, presieduto da Andrea Jelinek, si è riunito 11 volte nella sua composizione plenaria e ha continuato ad avvalersi dei suoi diversi sottogruppi (suddivisi per aree di competenza). Il lavoro del Cepd si è basato in massima parte sul programma di lavoro biennale (2019/2020) adottato il 12 febbraio 2019 oltre che sulle questioni via via emerse anche alla luce delle sollecitazioni da parte di soggetti esterni (le notizie relative alle attività del Comitato, le linee guida e tutti i documenti sono rinvenibili al sito internet: https://edpb.europa.eu).

Il 2019 è stato un anno importante per il Comitato: ha rappresentato l'occasione per un primo bilancio degli effetti del RGPD a distanza di un anno dalla sua piena applicazione e dalla costituzione del Cepd (risalente al 25 maggio 2018), le cui regole procedurali sono state peraltro oggetto di alcuni aggiustamenti dettati dall'esperienza maturata; nel corso dell'anno si è dato inizio al riesame del RGPD, come previsto dall'art. 97; è stato infine l'anno dominato dalle negoziazioni per l'uscita del Regno Unito dall'UE che, di riflesso, hanno impegnato la plenaria con riferimento sia alle sue ripercussioni sulle attività del Comitato, sia agli effetti sui trasferimenti di dati personali tra Regno Unito e See (v. *infra*).

Regole procedurali del Comitato

Il regolamento interno del Comitato è stato adottato all'atto del suo insediamento e ne disciplina le principali modalità operative, l'organizzazione, le modalità in cui è strutturata la collaborazione tra i suoi membri, l'elezione del presidente e del vicepresidente nonché le procedure di lavoro.

Come detto, il regolamento è stato più volte rivisitato nel corso del 2019 al fine di chiarirne o integrarne alcuni aspetti; in particolare, sono stati modificati gli artt. 8, 10 e 24. Alla luce della modifica introdotta all'art. 8, sarà possibile attribuire lo *status* di osservatore in seno al Comitato alle autorità di Paesi terzi che ne facciano richiesta, agiscano in completa indipendenza e siano stabilite in un Paese terzo che, in vista della sua accessione all'UE, abbia assunto l'obbligo vincolante sul piano internazionale di allineare le proprie norme sulla protezione dei dati a quelle dell'UE. L'art. 10, relativo alla procedura per l'adozione dei pareri ai sensi dell'art. 64 del RGPD, cioè quelli finalizzati ad assicurare la coerenza nelle attività delle autorità nazionali di controllo, è stato modificato al fine di chiarire i passi successivi all'adozione, da parte del Comitato, degli stessi; le modifiche mirano ad assicurare che tutti i membri del Comitato siano informati dell'intenzione o meno di un'autorità di protezione dei dati di mantenere o emendare la propria decisione alla luce del parere del Comitato e prevedono che, laddove un'autorità dichiari di volersi conformare ad esso (e conseguentemente emendare la propria bozza di decisione),

i *rapporteur* che lo hanno elaborato, i membri del sottogruppo competente sulla materia oggetto dello stesso e il segretariato siano tenuti a valutare le modifiche in questione e ad informarne il Comitato. La *ratio* della norma è fornire un riscontro tempestivo all'autorità che intende adottare la bozza di decisione modificata senza giungere a una nuova presa di posizione formale da parte del Comitato. Infine, le modifiche apportate all'art. 24 sono finalizzate a circoscrivere la possibilità di sospendere le votazioni in procedura scritta. Secondo il nuovo testo, con riferimento alle procedure scritte lanciate dal Comitato, tale sospensione può ora avvenire solo in presenza di sopravvenute circostanze che alterino in misura sostanziale il quadro della decisione messa al voto. Con riferimento alle procedure scritte volute dalla Presidenza, la richiesta di sospensione deve provenire da almeno 3 membri con diritto di voto (e non più da uno solo).

Riesame del RGPD

In base all'art. 97 del RGPD, la Commissione europea è chiamata entro il 25 maggio 2020, e successivamente ogni quattro anni, a trasmettere al Parlamento europeo e al Consiglio le relazioni di valutazione e riesame del RGPD, potendo a tal fine richiedere informazioni agli Stati membri e alle autorità di controllo nazionali. In tale procedura di riesame, che in questa occasione ha riguardato l'applicazione e il funzionamento del Capo V sul trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali e del Capo VII in materia di cooperazione e coerenza, il Garante, come le altre autorità che compongono il Comitato, ha fornito il proprio contributo rispondendo ad un questionario della Commissione relativo all'esperienza maturata sui profili applicativi del RGPD.

Il Comitato, sulla base dei riscontri forniti dalle autorità di controllo, ha lavorato alla predisposizione di un proprio documento, poi adottato il 18 febbraio 2020, che, oltre a sintetizzare i contributi nazionali, offre alcune valutazioni di carattere generale sull'implementazione del RGPD. In tale documento il Cepd valuta positivamente la prima fase di applicazione del RGPD, che ha rafforzato i diritti degli interessati, incrementandone la consapevolezza, fornito un quadro normativo armonizzato a titolari e responsabili del trattamento – nonché la possibilità, per questi ultimi, laddove il trattamento abbia carattere transfrontaliero, di avere un'unica autorità con cui interagire in base al meccanismo dello sportello unico – e incrementato i poteri correttivi e investigativi delle autorità, fornendo in via generale una visibilità accresciuta al modello europeo di protezione dei dati anche fuori dall'UE.

Nel proprio contributo, il Comitato prende atto delle sfide, soprattutto per piccole e medie imprese, determinate dall'applicazione del RGPD e ricorda gli sforzi compiuti dalle autorità nazionali per sviluppare strumenti di supporto a tali operatori nonché, più in generale, il lavoro svolto dal Comitato stesso per chiarire, attraverso linee guida e altri documenti, le previsioni del RGPD di maggiore rilevanza al fine di garantirne l'applicazione coerente nell'Unione.

Consapevole anche delle difficoltà incontrate dalle autorità nella prima fase di applicazione del meccanismo di coerenza, spesso causate dalle diverse procedure nazionali – ad esempio nella gestione dei reclami (v. *infra*) – il Comitato ritiene comunque che la cooperazione tra autorità sia un tratto essenziale del nuovo quadro normativo e che sia necessario continuare a ricercare soluzioni volte ad assicurare un'applicazione comune dei concetti chiave e delle procedure di cooperazione.

Nel contributo si sottolinea inoltre la necessità di garantire risorse adeguate alle diverse autorità europee per far fronte ai compiti ad esse attribuiti. Inoltre, il Comitato ricorda l'importanza dei trasferimenti dei dati a Paesi terzi e organizzazioni internazionali come parte integrante dell'ambiente digitale e a tal proposito sottolinea il proprio impegno volto a garantire una valutazione indipendente degli

21

strumenti di trasferimento predisposti dalla Commissione, in particolare le decisioni di adeguatezza.

Il Comitato valuta nel complesso positivamente l'attuazione del RGPD e ne considera allo stato prematura una revisione: al contrario, reputa necessario intensificare gli sforzi affinché si addivenga ad una tempestiva adozione del regolamento *e-Privacy*, per completare il quadro normativo UE sulla protezione dei dati.

Il RGPD detta regole dettagliate volte ad assicurarne l'applicazione coerente. In particolare, gli articoli 60 e ss. disciplinano da un lato gli obblighi di cooperazione in capo alle autorità di protezione dei dati dell'UE (e del See), specie quando il trattamento abbia carattere transfrontaliero, e, dall'altro, il meccanismo che, attraverso l'intervento del Cepd, deve garantire la coerenza delle azioni dalle stesse poste in essere. Il 2019 è stato un anno cruciale per avviare e consolidare gli strumenti attraverso cui tale cooperazione deve realizzarsi.

Sistema IMI

Dal 25 maggio 2018 le autorità di protezione dei dati dell'UE utilizzano la piattaforma IMI (*Internal Market Information System*): tale sistema multilingue, inizialmente sviluppato dalla Commissione europea per consentire alle autorità pubbliche di adempiere i propri obblighi di cooperazione amministrativa transfrontaliera, è stato successivamente adattato per supportare i meccanismi di cooperazione e coerenza previsti dal RGPD. Come già sottolineato (v. Relazione 2018, p. 144 e, in relazione all'esperienza finora maturata: v., in particolare, i parr. 11.4 e 14.6), attraverso IMI le autorità di controllo possono ora contare su uno strumento trasparente, flessibile e sicuro per diverse finalità, quali ad esempio identificare l'autorità di controllo capofila ai sensi dell'art. 56, par. 1, del RGPD e le autorità di controllo "interessate" ai sensi dell'art. 4, par. 1, n. 22, del RGPD, e quindi contribuire al processo di co-decisione dello sportello unico (cd. *One Stop Shop*); oppure possono fornire assistenza reciproca attraverso lo scambio di informazioni ai sensi dell'art. 61 del RGPD; o, ancora, condurre indagini e porre in essere misure di contrasto congiunte ai sensi dell'art. 62 del RGPD. Infine, allo scopo di favorire un'applicazione coerente del RGPD in tutta l'Unione, è previsto che la piattaforma venga utilizzata anche per consentire alle autorità di controllo di consultare il Cepd al fine di raccoglierne il parere di cui all'art. 64 del RGPD, ad esempio per questioni di applicazione generale o che producono effetti in più di uno Stato membro o in merito ai criteri nazionali per l'accreditamento degli organismi di monitoraggio dei codici di condotta ai sensi dell'art. 41, par. 3, del RGPD o degli organismi di certificazione ai sensi dell'art. 43, par. 3, o, ancora, per ottenere una decisione vincolante che componga eventuali conflitti fra le stesse autorità di controllo (come previsto dall'art. 65 del RGPD).

Al fine di sostenere la cooperazione e il meccanismo di coerenza tra le autorità di protezione dei dati, la DG GROW della Commissione europea, insieme alla segreteria del Comitato e ai membri dello stesso, hanno modificato tale sistema informatico, già esistente, adattandolo alle esigenze dettate dal RGPD. Il sistema è operativo sin dal primo giorno dell'entrata in vigore del RGPD e fornisce un meccanismo strutturato e sicuro per condividere le informazioni tra le autorità oltre che per adottare le decisioni soggette al meccanismo di sportello unico. Come ha fatto notare il Comitato nella relazione presentata al Parlamento europeo il 26 febbraio 2019 (il cui allegato fornisce una panoramica del funzionamento del sistema) e ribadito nel contributo per la revisione del RGPD adottato il 18 febbraio 2020 (v. *supra*), la gestione dei casi transfrontalieri richiede tempo, tenuto conto della necessità di aggiungere all'ordinaria attività istruttoria e di indagine, i tempi propri per garantire un'effettiva cooperazione tra le autorità interessate, nel rispetto delle (spesso) diverse norme procedurali nazionali.

21

L'attività di cooperazione attraverso il sistema ha registrato un costante aumento. Se nel febbraio del 2019 erano solo sei i casi definiti di *One Stop Shop* (dato fornito dal Comitato al Parlamento europeo), al 31 dicembre dello stesso anno sono stati 141 i progetti di decisione presentati ai sensi dell'art. 60, par. 3, di cui 79 già adottati a norma dell'art. 60, par. 6. Tuttavia, come ha notato il Comitato, da ultimo nel suo contributo alla revisione del RGPD, lo sportello unico e il meccanismo di cooperazione sono ancora procedure relativamente nuove rispetto alle quali il Comitato stesso si è impegnato a chiarire fasi procedurali, discipline nazionali applicabili e concetti chiave (quali, ad es, la nozione di "reclamo" o di "decisione") in modo da garantire (per quanto possibile) un'interpretazione comune degli stessi e favorire un più agile funzionamento del sistema.

Competenza di un'autorità di controllo in caso di cambiamento dello stabilimento principale

Proprio allo scopo di fornire alcuni chiarimenti circa il funzionamento del meccanismo di sportello unico, il Comitato ha adottato un parere (8/2019), sollecitato dalle autorità francese e svedese, in merito alla definizione dei criteri che disciplinano la competenza dell'autorità capofila al mutare delle condizioni che ne avevano inizialmente definito l'intervento (mutamento della sede dello stabilimento principale o unico del titolare nell'UE intervenuto in corso di procedimento). Il parere chiarisce che la competenza ad agire in qualità di autorità capofila cambia al mutare delle condizioni relative allo stabilimento principale (che il titolare o responsabile dovrà dimostrare essere effettivamente tale) fino al momento in cui l'autorità capofila competente emana la decisione finale all'esito del procedimento di cooperazione ai sensi dell'art. 60, RGPD. L'autorità che ha svolto il ruolo di capofila precedentemente all'assunzione di tale decisione finale sarà quindi tenuta a condividere ogni informazione con la nuova autorità capofila in modo da consentire la più celere definizione del procedimento.

Il Comitato ha continuato a lavorare sulla predisposizione di linee guida e documenti finalizzati a chiarire i concetti chiave del nuovo quadro normativo.

Linee guida sul trattamento dei dati ex art. 6.1.b RGPD nell'ambito dei servizi *online*

Le linee guida sul trattamento dei dati ai sensi dell'art. 6, par. 1, lett. *b*), del RGPD nell'ambito dei servizi *online*, adottate nella prima versione il 9 aprile 2019, sottoposta a consultazione pubblica e quindi in quella finale l'8 ottobre 2019 (linee guida 2/2019), si soffermano sull'interpretazione della norma del RGPD che prevede la liceità del trattamento ove esso sia necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Le linee guida, che si concentrano sui trattamenti effettuati *online*, sottolineano che la disposizione richiamata costituisce una valida base giuridica solo quando il trattamento è oggettivamente necessario all'esecuzione del contratto (ad es. il numero di carta di credito per effettuare il pagamento o l'indirizzo per effettuare la spedizione, ma non, rispettivamente, se non si paga con carta, o si predilige la spedizione del prodotto ad un punto di raccolta) e che nella valutazione della necessità occorre tenere conto, in base al principio di correttezza del trattamento, anche delle "ragionevoli aspettative dell'interessato", considerato, peraltro, che spesso si tratta di contratti per adesione unilateralmente determinati dal fornitore del servizio *online*.

Il documento esamina anche il caso dei trattamenti necessari al miglioramento del servizio, alla prevenzione delle frodi e alla pubblicità comportamentale (*behavioural advertising*), ed esclude, in linea generale, che tali trattamenti possano fondarsi sull'art. 6, par. 1, lett. *b*) (non escludendosi invece altre basi giuridiche).

Linee guida sull'ambito di applicazione territoriale del RGPD

Tra le norme chiave del RGPD, il Comitato ha ritenuto importante fornire chiarimenti anche sull'art. 3, relativo all'ambito di applicazione territoriale del RGPD (linee guida 3/2018), che rappresenta una novità significativa rispetto al quadro normativo preesistente (direttiva 95/46/CE).

21

L'art. 3 riflette l'intenzione del legislatore di assicurare un'ampia protezione dei diritti degli interessati nell'UE a fronte di di trattamenti sempre più globalizzati e definisce l'ambito di applicazione del RGPD sulla base di specifici criteri.

Le linee guida – adottate il 12 novembre 2019 nella loro versione finale all'esito della consultazione pubblica cui era stata sottoposta la prima versione – si soffermano pertanto sull'interpretazione dei criteri previsti dall'art. 3; forniscono chiarimenti sul criterio dello stabilimento di cui all'art. 3. par. 1, in base al quale il RGPD si applica al trattamento dei dati effettuati nell'ambito delle attività di uno stabilimento da parte di un titolare o di un responsabile del trattamento nell'UE, indipendentemente dal fatto che esso avvenga nell'UE, nonché del criterio del *targeting* (art. 3, par. 2), che rende invece applicabile il RGPD ai trattamenti di dati che, pur essendo effettuati da soggetti non stabiliti nell'UE, sono relativi ad interessati che si trovano nell'Unione e riguardano l'offerta di beni o la prestazione di servizi agli stessi rivolti, o il monitoraggio del loro comportamento che abbia luogo nel territorio UE.

Le linee guida forniscono chiarimenti anche sull'art. 3, par. 3, in base al quale il RGPD si applica al trattamento di dati effettuato da un titolare che è stabilito in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico (ad es. in ambasciate e consolati).

Inoltre, poiché i titolari e i responsabili stabiliti fuori dall'UE i cui trattamenti rientrino nell'ambito di applicazione del RGPD sulla base del criterio del *targeting* sono tenuti a designare un rappresentante nell'Unione, le linee guida si soffermano anche sulla procedura di tale designazione e sulle responsabilità che da essa derivano, nonché sulle deroghe a tale obbligo previste dall'art. 27, par. 2, del RGPD.

Aggiornamento del parere sulla nozione di titolare e responsabile del trattamento

Il Comitato ha avviato la predisposizione di linee guida sulle nozioni di titolare e responsabile del trattamento volte ad attualizzare il parere 1/2010 del Gruppo Art. 29. Se da una parte le nozioni di titolare e responsabile non hanno subito sostanziali modifiche rispetto alla direttiva 95/46/CE, il suo aggiornamento è particolarmente utile alla luce delle novità previste dal RGPD, specie con riferimento alla necessità che i trattamenti da parte di un responsabile siano disciplinati da un contratto o altro atto giuridico che lo vincoli al titolare (art. 28, par. 3), nonché in relazione alle questioni della contitolarità (art. 26) e dell'accordo interno che deve adeguatamente riflettere i ruoli e rapporti dei contitolari con gli interessati.

Il lavoro del Comitato, che dovrebbe portare all'adozione delle linee guida nel corso del 2020, è stato svolto anche sulla base delle riflessioni emerse in seno ad uno specifico *workshop*, tenutosi a Bruxelles il 25 marzo 2019, al quale hanno potuto partecipare diversi attori, ivi comprese le associazioni di titolari del trattamento europei.

Clausole contrattuali standard tra titolare e responsabile dell'Autorità danese

Con riferimento alla definizione dei ruoli di titolare e responsabile, è da segnalare anche l'adozione da parte del Comitato del parere sulle clausole contrattuali standard tra titolare e responsabile del trattamento, sottoposte dall'Autorità di controllo danese al meccanismo di coerenza ai sensi dell'art. 28, par. 8, del RGPD (parere 14/2019).

Tali clausole costituiscono un modello contrattuale di cui i titolari possono avvalersi per regolare il rapporto con i rispettivi responsabili del trattamento, dando così adeguata attuazione ai requisiti previsti dall'art. 28, parr. 3 e 4, del RGPD. Le clausole contrattuali standard ripercorrono sostanzialmente gli elementi che il contratto o altro atto giuridico di nomina a responsabile del trattamento deve avere, ai sensi del richiamato art. 28. La prima parte delle stesse deve stabilire il perimetro di azione in cui opererà il responsabile del trattamento e dovranno altresì essere indicati: i diritti e gli obblighi del titolare; gli obblighi del responsabile; la garanzia che le persone autorizzate al trattamento dei dati si siano impegnate a garantire la

riservatezza delle informazioni trattate o siano tenute ad un adeguato obbligo legale di riservatezza; l'obbligo di adottare le misure di sicurezza richieste dall'art. 32; l'impiego di sub-responsabili; l'eventuale trasferimento dei dati verso Paesi terzi o organizzazioni internazionali; l'obbligo di assistere il titolare del trattamento nell'adempimento delle richieste presentate dall'interessato per l'esercizio dei diritti previsti dal Capo III del RGPD; l'obbligo di informare il titolare del trattamento, senza ingiustificato ritardo, di una violazione di dati personali; la possibilità di svolgere *audit* o ispezioni da parte del titolare per verificare il rispetto delle norme del RGPD da parte del responsabile. La possibilità di ricorrere a tali clausole adottate da un'autorità di protezione dati non impedisce alle parti di aggiungere ulteriori garanzie purché esse non siano in contrasto con le clausole adottate o pregiudichino i diritti fondamentali degli interessati. In ogni caso le clausole in questione devono essere adoperate "così come sono" e ove le parti decidano di modificarle, non potranno rivendicare di essersene avvalsi.

A seguito del parere del Comitato, il testo finale delle clausole danesi è stato pubblicato nel registro del Comitato che contiene le decisioni adottate dalle autorità in base al meccanismo di coerenza.

Elenchi delle tipologie di trattamento soggette DPIA

Il Comitato ha espresso cinque pareri in merito alle liste con cui le autorità di protezione dati di Liechtenstein (pareri 1/2019), Norvegia (parere 2/2019), Spagna (parere 6/2019), Islanda (parere 7/2019) e Cipro (parere 10/2019) hanno individuato i trattamenti che, presentando un rischio elevato per i diritti e le libertà delle persone fisiche e avendo riflessi in più di uno Stato membro, devono essere sottoposti a valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD. I pareri vanno ad aggiungersi ai ventisei adottati dal Comitato nel corso del 2018 in relazione alle analoghe liste già predisposte dalle altre autorità di protezione dei dati del See (v. Relazione 2018, p. 188 s.); come i precedenti, sottolineano la necessità che le liste facciano riferimento ad almeno due criteri di rischio per ciascuna tipologia di trattamento e contengano un nucleo comune obbligatorio di tipologie di trattamenti, tra i quali quelli aventi ad oggetto dati genetici, biometrici e di localizzazione. Al fine di individuare i criteri di rischio da tenere in considerazione il Comitato ha fatto riferimento, oltre a quelli contenuti nello stesso art. 35, par. 3, del RGPD, alle indicazioni fornite nelle linee guida in materia di valutazione d'impatto sulla protezione dei dati (WP 248, rev. 01, adottato nell'ottobre 2017, v. Relazione 2017, pp. 158 e 159).

Sempre in tema di valutazione d'impatto, il Comitato ha adottato la raccomandazione 1/2019 concernente il progetto di elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto sulla protezione dei dati redatto dal Garante europeo della protezione dei dati ai sensi dell'art. 39, par. 4, del regolamento (UE) 2018/1725 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione. Il Comitato ha reso il parere poiché l'elenco si riferisce a operazioni di trattamento effettuate da Istituzioni e organi dell'Unione congiuntamente con uno o più titolari del trattamento stabiliti in uno degli Stati membri (e quindi soggetti al RGPD). Al fine di garantire un approccio coerente, il Comitato ha fornito, anche in questo caso, indicazioni volte ad armonizzare le definizioni e gli esempi contenuti nell'elenco alla luce delle già citate linee guida in materia di valutazione d'impatto sulla protezione dei dati (WP 248, rev. 01).

Il RGPD prevede che le autorità di protezione dei dati possano adottare anche l'elenco delle tipologie di trattamenti che non necessitano di una valutazione di impatto sulla protezione dei dati. Nel corso del 2019, tre autorità (ceca, francese e spagnola) hanno ritenuto di predisporre tali elenchi ai sensi dell'art. 35, par. 5, del

21

RGPD e li hanno sottoposti per il dovuto parere al Comitato. I tre pareri (11/2019, 12/2019 e 13/2019) chiariscono che tali elenchi sono per loro natura non esaustivi e indicano le tipologie di trattamento per le quali le autorità di controllo nazionali sono certe che in nessun caso comporteranno un rischio elevato per i diritti e la libertà delle persone fisiche e quelle per cui le stesse ritengono improbabile che vi sia un rischio elevato alla luce dei criteri indicati nelle linee guida in materia di valutazione d'impatto sulla protezione dei dati (WP 248, rev. 01, adottato nell'ottobre 2017: v. Relazione 2017, pp. 158 e 159). In ogni caso, i pareri ribadiscono che rimane fermo l'obbligo del titolare o del responsabile del trattamento di valutare il rischio del trattamento e rispettare i restanti obblighi imposti dal RGPD.

Codici di condotta

Dopo un complesso lavoro di approfondimento e muovendo anche dall'esperienza acquisita nella valutazione dei progetti sottoposti alla sua attenzione nel corso del 2018, il Comitato è intervenuto in materia di codici di condotta e organismi di monitoraggio (linee guida 1/2019) fornendo chiarimenti interpretativi e orientamenti pratici in merito all'applicazione degli artt. 40 e 41 del RGPD. I codici di condotta sono, insieme a certificazioni e valutazione d'impatto, uno degli strumenti di natura volontaria utili per i titolari e responsabili del trattamento al fine di dimostrare la propria conformità al RGPD e per conquistare la fiducia degli interessati. Tra gli obiettivi delle linee guida, quello di chiarire le procedure e le norme relative alla presentazione, all'approvazione e alla pubblicazione dei codici di condotta a livello sia nazionale che europeo, nonché quello di fornire un quadro di riferimento utile alle autorità di controllo, al Comitato e alla Commissione affinché la valutazione degli stessi codici sia effettuata in modo coerente.

Le linee guida chiariscono che le associazioni o le organizzazioni rappresentative di un settore possono proporre codici per aiutare il rispettivo settore a conformarsi al RGPD in modo efficiente e potenzialmente economico, tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in ciascuno di essi e delle esigenze specifiche delle microimprese e delle Pmi. Affinché un progetto di codice di condotta possa essere valutato, è necessario che lo stesso contenga una motivazione chiara e concisa in cui siano specificati lo scopo, l'oggetto e il contributo che lo stesso intende fornire in termini di più efficace applicazione del RGPD; deve essere chiaramente indicato l'ambito di applicazione territoriale dello stesso (i codici possono infatti essere nazionali o transnazionali) e deve prevedere meccanismi attraverso i quali sia possibile vigilare sull'osservanza delle relative disposizioni. In particolare, i progetti di codice che contemplano attività di trattamento di enti non pubblici devono identificare un organismo di monitoraggio, esterno o interno, e descrivere i meccanismi attraverso i quali tale organismo potrà svolgere le sue funzioni di controllo sull'osservanza del codice da parte dei soggetti aderenti. Tale organismo potrà operare solo dopo essere stato accreditato dall'autorità di controllo competente ai sensi dell'art. 41, par. 1, del RGPD sulla base dei requisiti di accreditamento che dovranno essere prestabiliti dalla medesima autorità e approvati dal Comitato nell'ambito del meccanismo di coerenza di cui all'art. 63 del RGPD. Tra tali requisiti si annoverano: l'indipendenza rispetto agli aderenti al codice e al settore, professione o attività cui questo si applica; l'assenza di conflitto di interessi; il livello necessario di competenze e l'esistenza di appropriate procedure per svolgere la propria funzione di controllo in modo efficace, per gestire i reclami in modo trasparente e imparziale e per l'adozione di eventuali misure correttive, nei confronti degli aderenti al codice che ne abbiano violato le diposizioni, volte a porre termine a tali violazioni e ad evitare che queste si ripetano in futuro. Nelle linee guida il Comitato ha anche chiarito che, benché l'accreditamento di un organismo di monitoraggio valga solo per un determinato codice, uno stesso organismo può essere accreditato

21

Pareri sui requisiti per l'accreditamento degli organismi di monitoraggio

per esercitare il monitoraggio su più di un codice a condizione che soddisfi i requisiti di accreditamento con riferimento a ciascuno di essi. Da notare infine che, ai sensi dell'art. 41, par. 5, del RGPD, quando un organismo di monitoraggio non rispetta le disposizioni del RGPD, l'autorità di controllo competente potrà revocarne l'accreditamento.

Le linee guida in materia di codici di condotta hanno trovato la loro prima applicazione a luglio 2019 in occasione del parere reso dal Comitato in ordine ai requisiti di accreditamento degli organismi di monitoraggio di codici di condotta, ai sensi dell'art. 41 del RGPD, predisposti dall'autorità austriaca (parere 9/2019). Allo scopo di garantire un approccio uniforme da parte di tutte le autorità di protezione dei dati, il parere sottolinea l'importanza che ciascuna autorità fissi i propri requisiti di accreditamento dell'organismo di monitoraggio tenendo in considerazione gli otto indicati nella sezione 12 delle linee guida 1/2019. Il parere, traendo spunto dai requisiti proposti dall'Autorità austriaca, fornisce alcune utili precisazioni in merito. In particolare, secondo il Comitato, i requisiti di accreditamento dovrebbero anzitutto indicare gli elementi essenziali sulla base dei quali dovrà essere valutata l'indipendenza dell'organismo, soffermandosi su quattro profili principali: l'indipendenza decisionale e giuridica (a tale proposito, la durata e la scadenza del mandato dell'organismo di monitoraggio dovrebbero essere fissate in modo tale da impedire un'eccessiva dipendenza dal rinnovo oppure da scongiurare il timore di perdere l'incarico); l'indipendenza finanziaria, per cui gli organismi di monitoraggio dovrebbero disporre delle risorse e della stabilità finanziaria necessarie per lo svolgimento efficace dei propri compiti e gestire in modo indipendente il proprio bilancio; l'indipendenza organizzativa, alla luce della quale gli organismi di monitoraggio dovrebbero disporre delle risorse umane e tecniche necessarie per assolvere con efficacia alle proprie funzioni; infine, l'indipendenza attraverso la responsabilizzazione, ovvero, per essere considerato indipendente, l'organismo di monitoraggio deve essere in grado di dimostrare un approccio "responsabilizzante" rispetto alle proprie decisioni e azioni.

Il parere precisa inoltre che un organismo di monitoraggio deve essere stabilito nel territorio dello See per essere in grado di tutelare efficacemente i diritti degli interessati e trattarne utilmente i reclami, oltre che per garantire la piena applicazione del RGPD e il controllo da parte delle autorità di protezione dei dati. Sotto altro profilo, il parere chiarisce che laddove sia consentito all'organismo di subappaltare le proprie attività, debbano essere indicate le condizioni alle quali ciò sia possibile, prevedendo che gli obblighi riferiti all'organismo di monitoraggio debbano trovare identica applicazione anche nei riguardi dei subappaltatori.

In merito alla composizione dell'organismo, il parere ammette la possibilità di accreditare come organismo di monitoraggio anche persone fisiche; in questo caso però richiede il rispetto di requisiti supplementari per l'accreditamento, quali la dimostrata disponibilità di risorse sufficienti per fare fronte ad eventuali responsabilità e obblighi, nonché per garantire la piena operatività nel tempo del meccanismo di monitoraggio.

In ordine al livello di competenza richiesto all'organismo, il parere evidenzia come ciascun codice dotato di un organismo di monitoraggio dovrà individuare il livello di competenza appropriato al proprio organismo, al fine di svolgere in maniera efficace le proprie attività di controllo. In questa prospettiva l'autorità di protezione dei dati è chiamata a operare una valutazione in funzione di ciascun codice, che tenga conto delle dimensioni del settore interessato, dei diversi interessi coinvolti e dei rischi delle attività di trattamento.

Un ulteriore parere reso dal Comitato sui requisiti di accreditamento degli orga-

nismi di monitoraggio dei codici di condotta, ai sensi dell'art. 41 del RGPD, ha riguardato il progetto presentato dall'autorità di controllo della protezione dei dati del Regno Unito (parere 17/2019). Anche in questo caso, il parere ricorda l'importanza di prendere in considerazione i requisiti indicati nella sezione 12 delle linee guida e chiede di fornire ulteriori specificazioni, ad esempio, in tema di indipendenza finanziaria: al riguardo, il parere chiede di introdurre esempi che chiariscano i casi in cui tale indipendenza non si possa configurare in capo all'organismo che richiede l'accreditamento (ad es, se è consentito ad un soggetto aderente al codice di condotta su cui l'organismo di monitoraggio sta investigando, di non contribuire più al suo finanziamento), invitando ad introdurre alcuni esempi di strumenti di sostegno finanziario compatibili con tale requisito. In ordine alla dotazione organica, il parere ribadisce che la stessa deve essere adeguata allo svolgimento delle funzioni di controllo, tenendo conto del settore specifico e dei rischi delle attività di trattamento previste dal codice di condotta. Con riferimento al termine di validità dell'accreditamento – che l'Autorità del Regno Unito aveva originariamente fissato in cinque anni – il parere considera che l'art. 41 del RGPD non fa riferimento alla durata dell'accreditamento dell'organismo di monitoraggio e lascia pertanto un certo margine di manovra alle autorità nazionali di controllo, pur sottolineando che i requisiti di accreditamento dovrebbero essere rivalutati periodicamente, al fine di garantire il pieno rispetto del RGPD; al riguardo, il parere rileva che dovrebbe essere chiarito cosa avvenga al termine del periodo di validità dell'accreditamento e le relative procedure.

Trasferimento dati all'estero

In materia di trasferimento di dati all'estero, il Comitato ha adottato il suo primo parere relativo ad un accordo amministrativo per il trasferimento di dati personali tra soggetti pubblici. A norma dell'art. 46, par. 1, del RGPD, in mancanza di una decisione di adeguatezza da parte della Commissione europea, il titolare o il responsabile del trattamento può trasferire dati personali verso un Paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Nel caso di trasferimenti effettuati da parte di soggetti pubblici, tali garanzie possono essere contenute o in strumenti giuridicamente vincolanti e aventi efficacia esecutiva tra autorità pubbliche o organismi pubblici, quali i trattati internazionali, o in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendano diritti effettivi e azionabili per gli interessati e che siano autorizzati dalla competente autorità nazionale di protezione dei dati, tenuta, a norma dell'art. 46, par. 4, del RGPD, ad applicare il meccanismo di coerenza ai sensi dell'art. 63 del RGPD.

Alla luce di ciò, facendo seguito a vari cicli di discussioni, l'Autorità europea degli strumenti finanziari e dei mercati (Esma) insieme all'Organizzazione internazionale delle commissioni sui valori mobiliari (Iosco) hanno presentato un progetto di accordo amministrativo conformemente all'art. 46, par. 3, lett. *b*), del RGPD, per definire il quadro dei trasferimenti di dati personali dalle autorità di vigilanza finanziaria del See (e dall'Esma stessa) verso le loro omologhe al di fuori del See. Il Comitato ha espresso il proprio parere favorevole (parere 4/2019: v. anche Relazione 2018, pp. 191 e 192) e ha consentito così a diverse autorità di protezione dei dati di autorizzare gli accordi siglati dalle rispettive autorità nazionali: entro questa cornice il Garante ha autorizzato la Consob a siglare l'Accordo con provvedimento 23 maggio 2019 (cfr. par. 4.8).

L'Accordo contiene definizioni in linea con il RGPD e prevede il rispetto dei principi di trasparenza, proporzionalità e qualità dei dati, l'adozione di adeguate misure di sicurezza e l'esistenza di meccanismi di tutela per gli interessati. Specifiche cautele inoltre sono previste nel caso di trasferimenti successivi di dati verso

un soggetto che non sia parte dell'Accordo o sia stabilito in Paese terzo che non assicuri un livello adeguato di tutela.

21

Trasferimento di dati tra soggetti pubblici

Anche alla luce dell'esperienza acquisita con la revisione dell'Accordo, il Comitato ha lavorato nel corso del 2019 alla predisposizione di apposite linee guida per il trasferimento di dati tra soggetti pubblici poi adottate nel febbraio 2020 (linee guida 2/2020). Sottoposte a consultazione pubblica, esse recano indicazioni in ordine alle garanzie adeguate che dovranno essere contenute sia negli accordi internazionali vincolanti per gli Stati (per i quali, ai sensi dell'art. 46, par. 2, lett. *a*), del RGPD, non c'è bisogno di autorizzazione da parte dell'autorità di protezione dei dati) sia negli accordi amministrativi tra autorità pubbliche o organismi pubblici che dovranno essere autorizzati dalle autorità di protezione dei dati dopo aver ottenuto il parere del Comitato ex art. 64, par. 2, del RGPD. Tra gli elementi essenziali si annoverano: definizioni in linea con quelle contenute nel RGPD; disposizioni in materia di trasparenza per gli interessati; espressa previsione dei principi di protezione dei dati e dei diritti degli interessati (compreso il diritto ad una tutela effettiva); disposizioni in materia di trasferimenti ulteriori e misure di sicurezza; la previsione di un meccanismo di supervisione dell'accordo che abbia carattere di indipendenza. Le linee guida chiariscono che ciascun accordo verrà valutato caso per caso e ciò consentirà anche di individuare, ove necessario, garanzie specifiche per assicurare la tutela effettiva agli interessati.

Bcr e RGPD

Nel 2019 hanno anche visto la luce le prime due norme vincolanti di impresa per titolari del trattamento (*Binding corporate rules*, di seguito Bcr) approvate dopo l'applicazione del RGPD (pareri 15/2019 e 16/2019). L'Autorità del Regno Unito e l'Autorità belga hanno infatti presentato, in qualità di autorità competenti per l'approvazione delle norme vincolanti d'impresa (cd. *Bcr Lead*), due progetti di decisione sui quali il Comitato ha reso il proprio parere ai sensi dell'art. 64, par. 1, lett. *f*), del RGPD. I due pareri, richiamando la procedura di approvazione delle Bcr (WP 263 rev. 01: v. Relazione 2018, p. 190) che ha consentito alle autorità di protezione dei dati la valutazione congiunta delle medesime, hanno confermato che le stesse offrono un livello adeguato di tutela dal momento che presentano tutti gli elementi richiesti dall'art. 47 del RGPD e dal documento di lavoro relativo alle Bcr per titolari (WP 256, rev. 01: cfr. Relazione 2017, p. 167). Una volta ottenuto il parere, le due *Bcr Lead* coinvolte hanno potuto approvare le regole vincolanti di impresa che saranno considerate come "garanzie adeguate" anche negli altri Paesi See e potranno essere utilizzate per il trasferimento dei dati da parte delle società del gruppo ivi stabilite senza ulteriori autorizzazioni (art. 46, par. 2, lett. *b*), del RGPD). Nel corso dell'anno numerose altre Bcr sono state oggetto di valutazione nell'ambito della procedura di approvazione che prevede che la *Bcr Lead* (nella sua qualità di punto di contatto), consultate le altre autorità, possa indicare al gruppo imprenditoriale richiedente le modifiche da apportare al testo originariamente proposto al fine di renderlo conforme al RGPD. Non appena le stesse saranno modificate e ritenute in linea con le indicazioni ricevute dalle autorità, la *Bcr Lead* le presenterà al Comitato per il necessario parere.

Terza revisione periodica del *Privacy Shield*

Il Comitato ha partecipato nel 2019 alla terza revisione annuale del *Privacy Shield* che ha portato all'adozione della terza relazione sul funzionamento dell'Accordo negoziato nel 2016 fra Unione europea e Stati Uniti per il trasferimento dati personali verso le società certificate nel quadro dello stesso (Relazione 2016, p. 153). Come negli anni precedenti, nel dare atto di alcuni ulteriori sforzi posti in essere da parte statunitense per dare attuazione completa all'Accordo – tra i quali, un incremento dell'attività di controllo *ex officio*, la nomina degli ultimi membri dell'Autorità per la tutela della vita privata e delle libertà civili (PCLOB) e la nomina di un

21

ombudsperson permanente –, il rapporto si sofferma anche su alcuni aspetti sui quali permangono aspetti da risolvere. Per la parte commerciale rimangono infatti ancora da chiarire alcuni profili relativi ai trasferimenti ulteriori, al trattamento dei dati relativi alle risorse umane, agli obblighi propri dei soggetti che agiscono in qualità di responsabile del trattamento e al processo di rinnovo della certificazione. Per quanto riguarda la raccolta di dati da parte delle autorità pubbliche, il Comitato incoraggia il PCLOB a pubblicare ed adottare le proprie relazioni al fine di assicurare una valutazione indipendente dei programmi di sorveglianza condotti al di fuori del territorio statunitense e ribadisce che i propri esperti in possesso del nulla osta di sicurezza sono pronti ad esaminare ulteriori documenti (anche classificati). Rispetto alla figura del mediatore, il Comitato rappresenta di non essere ancora in grado di concludere che lo stesso sia dotato di poteri sufficienti per accedere a tutte le informazioni necessarie e porre rimedio alle eventuali inadempienze, ricordando inoltre che la questione pende davanti alla CGUE nell'ambito del procedimento C-311/18 (Facebook Ireland e Schrems) relativo alla validità delle clausole contrattuali standard nel caso in cui le stesse siano utilizzate per trasferire dati personali verso gli Stati Uniti.

Clausole contrattuali standard

Ed è proprio il procedimento avviato davanti alla CGUE nel cd. caso "Schrems 2" ad aver dato al Comitato l'occasione per riflettere sul ruolo e l'utilizzo delle clausole contrattuali standard adottate dalla Commissione in base all'art. 26, par. 4, direttiva 95/46/CE e ancora in vigore ai sensi dell'art. 46, par. 5, del RGPD. Nel corso della discussione orale della causa davanti alla Corte e su richiesta della stessa, il Comitato ha infatti presentato alcune osservazioni relative alle diverse questioni pregiudiziali sollevate precisando, tra l'altro, che le clausole contrattuali standard sono strumenti di trasferimento dei dati che hanno carattere generale e che possono essere utilizzate per il trasferimento dei dati in diversi Paesi terzi a prescindere dal livello di protezione esistente in ciascuno di essi. Il Comitato ha chiarito che spetta all'esportatore e all'importatore fare una valutazione circa la possibilità di utilizzare e rispettare tali clausole e alle autorità di protezione dei dati valutare, laddove necessario, il loro effettivo rispetto nei singoli casi. Tale valutazione sembra essere stata condivisa dall'Avvocato generale nelle sue Conclusioni, rese il 19 dicembre 2019, secondo il quale l'analisi delle questioni non ha evidenziato elementi atti ad inficiare la validità della decisione relativa all'adeguatezza delle clausole contrattuali utilizzate nel caso di specie (ovvero la decisione 2010/87). Sul punto, si attende ora la sentenza della CGUE.

Brexit e trasferimento dei dati all'estero

Il 2019 è stato anche l'anno nel quale grande è stata l'incertezza in merito alle modalità attraverso le quali il Regno Unito avrebbe lasciato l'UE. Il tema è ovviamente di rilievo con riferimento ai trasferimenti di dati all'estero dal momento che, una volta lasciata l'Unione, il Regno Unito sarà considerato a tutti gli effetti un Paese terzo verso il quale, in assenza di un'eventuale decisione di adeguatezza della Commissione, ogni trasferimento di dati personali sarà possibile solo attraverso l'utilizzo di uno degli strumenti previsti dal Cap. V del RGPD. Ed è proprio per chiarire questo aspetto e il ruolo dell'Autorità del Regno Unito nelle procedure di approvazione delle Bcr per le quali la stessa è *Bcr Lead* che sono stati adottati dal Comitato, il 12 febbraio 2019, due documenti contenenti indicazioni pratiche sull'utilizzo dei meccanismi per i trasferimenti di dati previsti dal RGPD nel caso di "*no deal*" e sui passi che i gruppi di imprese stabiliti nel Regno Unito avrebbero dovuto seguire per ottenere l'approvazione delle proprie Bcr. I documenti sono stati di fatto superati dal momento che, dopo una serie di proroghe, l'accordo raggiunto tra UE e Regno Unito ha previsto che i trasferimenti di dati personali tra le due aree geografiche potranno ancora essere effettuati liberamente fino al 31 dicembre 2020.

21

Il Garante ha continuato a coordinare il sottogruppo "*Financial matters*" che nell'ambito del Comitato è incaricato di approfondire le diverse questioni legate all'applicazione della disciplina sulla protezione dei dati nel settore finanziario.

PSD2 e RGPD

Una delle questioni che ha maggiormente impegnato il sottogruppo è stato il rapporto tra il RGPD e la direttiva (UE) 2015/2366 sui servizi di pagamento (cd. PSD2), due normative chiave della legislazione europea degli ultimi anni. La direttiva PSD2 presenta novità importanti nel sistema dei pagamenti consentendo a nuovi soggetti di attuare servizi che un tempo erano prerogativa pressoché esclusiva delle banche, consentendo ad essi di accedere ad una mole considerevole di dati finanziari non solo dei clienti, ma anche di soggetti terzi, ad esempio dei beneficiari di ordini di pagamenti. Il Comitato, che si era già occupato di alcune questioni legate alla PSD2 con la risposta a una lettera dell'europarlamentare Sophie in't Veld, fornendo prime indicazioni su alcuni punti controversi del rapporto tra tale direttiva e RGPD, ha ritenuto necessario avviare una riflessione più approfondita sul tema anche alla luce degli esiti di un *workshop*, organizzato dal segretariato e tenutosi a Bruxelles il 27 febbraio 2019, nel corso del quale i diversi *stakeholders* si sono confrontati sulle parti più complesse dell'interazione tra PSD2 e RGPD, in particolare sull'individuazione della corretta base giuridica per il trattamento dei dati relativi ai terzi effettuato dai nuovi operatori nei servizi di pagamento e delle deroghe al divieto di trattare speciali categorie di dati ai sensi dell'art. 9 del RGPD da essi utilizzabili.

Scambi di informazioni tra autorità di controllo dei mercati finanziari ai fini di cooperazione

È stato concluso il lavoro del Comitato sullo scambio di informazioni tra autorità di controllo dei mercati finanziari nell'ambito della loro attività di cooperazione. In tale attività di scambio occorre che i trasferimenti di dati dalle autorità finanziarie europee alle loro omologhe extra-UE siano effettuati nel rispetto dei principi di protezione dati. In particolare, in base all'art. 46, par. 3, lett. *b*), del RGPD, le autorità pubbliche o organismi pubblici possono stipulare accordi amministrativi, che includano diritti effettivi e azionabili per gli interessati, per assicurare le garanzie necessarie a legittimare i trasferimenti di dati verso Paesi sforniti di adeguatezza. Come anticipato (cfr. par. 4.8), il Comitato ha esaminato il modello di accordo di cui potranno avvalersi le autorità finanziarie per i trasferimenti dei dati extraeuropei predisposto da Esma unitamente a Iosco. Con il parere 4/2019 adottato il 12 febbraio 2019 (ai sensi dell'art 64, par. 2, del RGPD) il Cepd ha concluso che la versione finale di tale accordo assicura le garanzie adeguate necessarie a trasferire i dati, ed ha comunque fornito alcune ulteriori indicazioni riguardo all'implementazione dei meccanismi di tutela posti in essere dall'accordo stesso.

FATCA

In ambito finanziario è altresì proseguita l'attività del Comitato relativa all'analisi delle implicazioni della normativa statunitense FATCA (*Foreign Account Tax Compliance Act*) sulla tutela della vita privata e sul principio di non discriminazione, previsti dagli artt. 8 e 14 della CEDU. L'8 febbraio 2019 il Comitato ha adottato una dichiarazione (*Statement* 1/2019) in risposta alla risoluzione del 5 luglio 2019 del Parlamento europeo e alle richieste dell'associazione dei cd. *Accidental Americans*, che hanno sollecitato un intervento del Comitato sulle implicazioni di FATCA. La dichiarazione, richiamando i diversi interventi dell'allora Gruppo Art. 29 sul tema, annuncia l'avvio da parte del Comitato della predisposizione di linee guida sugli strumenti per il trasferimento dei dati ai sensi dell'art. 46 del RGPD, che offriranno indicazioni anche per il caso FATCA, in particolare con riferimento alla garanzie minime che dovranno essere inserite, per i trasferimenti di dati all'estero, negli strumenti giuridicamente vincolanti tra autorità pubbliche ai sensi dell'art. 46, par. 2, lett. *a*), del RGPD o negli accordi amministrativi tra le stesse ai sensi dell'art. 46, par. 3, lett. *b*), del RGPD. Tali linee guida costituiranno uno strumento utile anche

21

ai fini della valutazione degli accordi intergovernativi firmati tra gli Stati membri e il governo statunitense per far sì che l'applicazione di FATCA sia conforme ai principi di protezione dati previsti dal RGPD.

È stata inoltre avviata la discussione sulla base giuridica della conservazione dei dati relativi a carte di credito, effettuata dalle piattaforme di *e-commerce*, al fine di facilitare gli acquisti successivi da parte dei loro clienti, nonché sul tema delle criptovalute nell'ambito della più ampia riflessione in materia di *blockchain* avviata dagli specifici sottogruppi cui il Comitato ha dato mandato.

Il tema delle criptovalute è stato altresì discusso dal Comitato con riferimento all'iniziativa lanciata da Facebook in collaborazione con l'associazione svizzera "Libra" sulla creazione di una nuova criptovaluta. La questione è stata già oggetto di una dichiarazione congiunta di diverse autorità per la protezione dei dati (di Albania, Australia, Burkina Fasu, Canada, Regno Unito, insieme all'EDPS e alla *Federal Trade Commission*) e di una lettera del *Commissioner* svizzero rivolta alla Presidente del Comitato affinché sia aperto un dialogo sui profili di protezione dei dati implicati in tale iniziativa.

Protezione dei dati e *law enforcement*

Il Comitato ha proseguito la sua attività relativa alla protezione dei dati nell'ambito delle attività di indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, oggetto della direttiva (UE) 2016/680.

CLOUD Act

È stata adottata la risposta congiunta del Comitato e del GCPD del 10 luglio 2019 sull'impatto della normativa statunitense "*CLOUD Act*" – che prevede la possibilità per le autorità statunitensi di richiedere ai fornitori di servizi i dati detenuti anche nel caso in cui siano conservati sul territorio extra-USA – sull'ordinamento UE. La lettera sottolinea che un accordo UE-USA riguardo all'accesso transfrontaliero dei dati che contenga efficaci garanzie a tutela dei diritti della persona rappresenta lo strumento più appropriato per assicurare un livello di protezione adeguato e la certezza giuridica per le imprese.

Sistemi ETIAS e ECRIS-TCN

È stata adottata la lettera del 13 novembre 2019 di risposta alla LIBE che nell'aprile 2019 aveva chiesto al Comitato di valutare due proposte di regolamento presentate dalla Commissione europea nel gennaio 2019 al fine di introdurre le modifiche tecniche necessarie a rendere pienamente operativo il sistema ETIAS e quello ECRIS-TCN, modificando gli atti giuridici riguardanti i sistemi informatici dell'UE (quali SIS, VIS, Eurodac, ecc.). Nella lettera adottata dal Comitato si chiarisce che i documenti in questione contengono in realtà solo modifiche volte a rendere applicabile il nuovo quadro per l'interoperabilità dei sistemi informativi sul quale il Gruppo Art. 29 aveva già manifestato grosse perplessità con il parere WP 266 dell'aprile 2018 e si sottolinea che le modifiche introdotte a sistemi informativi non ancora realizzati rischiano di ledere la trasparenza, il principio per cui i trattamenti devono essere fondati su regole chiare e certe nonché quelli di *privacy by design* e *by default*. La lettera ribadisce infine che il previsto sistema di interoperabilità solleva seri dubbi circa il rispetto del principio di finalità e dei diritti degli interessati.

Il secondo Protocollo addizionale alla Convenzione di Budapest

Il Comitato ha inoltre fornito il proprio contributo alla consultazione pubblica lanciata dal Comitato *cybercrime* (T-CY) del Consiglio d'Europa sulla bozza di secondo Protocollo addizionale alla Convenzione di Budapest, in particolare sui temi della cd. *direct disclosure*, ovvero la procedura che permette una diretta cooperazione tra le autorità di una Parte e un fornitore di servizi di comunicazione elettronica situato nel territorio di un'altra Parte al fine di ottenere informazioni relative al *subscriber*, e della procedura che permette ad una Parte di dare mandato ad un'altra al fine di obbligare un fornitore di servizi situato nel territorio di quest'ultima a esibire specifiche informazioni sul *subscriber* e i dati di traffico ad esso relativi. Il contributo del Cepd richiama le posizioni già assunte dal Gruppo Art. 29, dal Comitato

medesimo e dal Gepd in materia; sottolinea la necessità che la protezione dei dati sia inclusa nelle norme del Protocollo, rendendo l'accessibilità dei dati pienamente compatibile con i trattati UE e la CDFUE; ricorda che il Comitato rimane a disposizione per ulteriori contributi ai fini della preparazione delle specifiche previsioni normative in materia di protezione dati su cui il T-CY sta lavorando, auspicando il coinvolgimento tempestivo delle autorità di protezione dati nel processo di elaborazione del Protocollo. Con riferimento a specifiche previsioni normative in materia di protezione dei dati, il contributo sottolinea la necessità che il testo sia arricchito da tali previsioni, che riflettono i principi cardine UE ma anche quelli previsti dalla Convenzione 108+; richiama a tal proposito i principi sostanziali e procedurali che devono regolare l'accesso ai dati da parte delle autorità di *law enforcement* (accesso previsto da una chiara base legale; accesso individuale solo in relazione a individui sospettati di voler commettere o di aver commesso crimini gravi; autorizzazione da parte di autorità giurisdizionali; proporzionalità e qualità dei dati raccolti; speciali garanzie per dati sensibili; informativa agli interessati non appena possibile anche al fine di consentire l'esercizio dei propri diritti); sottolinea la necessità che agli interessati siano assicurati strumenti di tutela adeguati quantomeno equivalenti a quelli esistenti nel proprio stato; ricorda la necessità di inserire specifiche garanzie sui trasferimenti ulteriori, compreso il divieto di trasferire i dati verso paesi privi di un livello di protezione appropriato.

PNR

Il 9 ottobre 2019, il Comitato ha inoltre adottato una lettera di risposta alla parlamentare europea Sophie in't Veld, che aveva chiesto quale fosse la posizione dello stesso in merito al nuovo Accordo sul PNR (*Passenger Name Record*) oggetto della negoziazione tra la Commissione europea e il Canada. La nota di risposta richiama le posizioni già espresse dal Gruppo Art. 29 subito dopo il parere 1/2017 della Corte di giustizia sulla prima bozza di Accordo, in particolare sulla necessità che, in linea con gli orientamenti della Corte, gli accordi PNR rispettino pienamente i principi della CDFUE e anticipa l'intenzione di predisporre un proprio parere sulla nuova bozza di accordo non appena disponibile.

Commissione di controllo coordinato

Dopo la plenaria del Comitato del 3 dicembre 2019, si è svolto il primo incontro della Commissione di controllo coordinato sul trattamento dei dati svolto nell'ambito dei grandi sistemi informativi dell'UE che rafforzerà la cooperazione tra le diverse autorità di protezione dei dati in tale settore e garantirà verifiche più efficaci. La Commissione, istituita nell'ambito del Comitato e che riunisce le autorità europee di protezione dei dati, l'EDPS e le autorità di controllo degli Stati extra-UE che partecipano al sistema Schengen, si occuperà di vigilare sui sistemi informativi e sugli organismi, gli uffici e le agenzie operanti nei settori delle frontiere, dell'asilo e della migrazione (SIS, EES, ETIAS e VIS), della cooperazione di polizia e giudiziaria (SIS, EPPO, Eurojust, ECRIS-TCN) e del mercato interno (IMI). Nel corso della sua prima riunione, la Commissione ha eletto il Segretario generale del Garante Giuseppe Busia quale coordinatore e Iris Gnedler dell'Autorità federale tedesca in qualità di vice-coordinatore, per un mandato di due anni, ed ha altresì adottato il proprio regolamento interno.

Protezione dei dati e nuove tecnologie

In materia di nuove tecnologie e protezione dei dati, il tema dominante del 2019 è stato quello della possibile revisione della direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (cd. direttiva *e-Privacy*). Incessanti sono state infatti le discussioni, specie in seno al Consiglio dell'Unione, al fine di pervenire ad un testo condiviso da portare al trilogo con il Parlamento. Il Comitato è intervenuto sul tema adottando, il 13 marzo 2019, la Dichiarazione 3/2019 sul regolamento *e-Privacy* (*Statement* 3/2019), con la quale ha invitato gli Stati membri a finalizzare le proprie posizioni

21

Direttiva *e-Privacy* e RGPD

sulla proposta di regolamento *e-Privacy*, la cui adozione completerebbe il quadro europeo per la protezione dei dati fornendo ulteriori forti salvaguardie per tutti i tipi di comunicazioni elettroniche. Il Comitato ha invitato il legislatore dell'Unione a garantire che il futuro regolamento *e-Privacy* non fornisca una protezione inferiore a quella assicurata nell'attuale direttiva *e-Privacy*.

Su questo stesso tema, il Comitato ha adottato il 12 marzo 2019 il parere 5/2019 relativo all'interazione tra la direttiva UE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva *e-Privacy*) e il RGPD. Il parere – adottato a seguito di una richiesta avanzata, ai sensi dell'art. 64, par. 2, del RGPD, dall'Autorità belga di protezione dei dati – ha il fine di chiarire le competenze delle autorità di protezione dei dati nazionali allorché un trattamento di dati ricada sia sotto l'ambito applicativo del RGPD sia sotto quello della direttiva *e-Privacy*. L'Autorità belga aveva richiesto al Comitato chiarimenti in merito a, da un lato, competenza, compiti e poteri delle autorità di controllo per la protezione dei dati personali e, dall'altro, applicabilità dei meccanismi di cooperazione e coerenza del RGPD nei casi in cui al trattamento dei dati personali si applichi sia il RGPD che la direttiva *e-Privacy*.

In primo luogo, il parere rileva che vi sono molti esempi di attività di trattamento dei dati che rientrano nell'ambito di applicazione materiale sia della direttiva *e-Privacy* che del RGPD, come confermato anche dalla giurisprudenza della CGUE, ad esempio per l'uso di *cookie*. Il parere ribadisce che la direttiva *e-Privacy* prevede "norme speciali" in merito al trattamento dei dati personali nel settore delle comunicazioni elettroniche. Tra queste figurano le disposizioni dell'art. 5, par. 3 che richiedono il consenso dell'utente per conservare informazioni, compresi i dati personali, nel dispositivo dell'utente finale o per avere accesso a tali informazioni (ad es, tramite *cookie*) e l'art. 6, che limita esplicitamente le condizioni alle quali possono essere trattati i dati relativi al traffico, compresi i dati personali degli abbonati e degli utenti di un servizio di comunicazione elettronica accessibile al pubblico. Conformemente al principio della *lex specialis derogat legi generali*, queste disposizioni specifiche in materia di *e-Privacy* hanno la precedenza sulle disposizioni (più generali) del RGPD (come l'art. 6 del RGPD, che individua le basi giuridiche possibili per il trattamento dei dati personali). In tutti gli altri casi in cui il trattamento dei dati personali non è specificamente disciplinato dalla direttiva *e-Privacy* (o per cui la direttiva *e-Privacy* non prevede una "norma speciale"), si applica il RGPD. Ad esempio, si applicheranno le disposizioni del RGPD relative all'esercizio dei diritti degli interessati in relazione ai loro dati personali, in quanto non previste delle disposizioni specifiche nella direttiva *e-Privacy*. Analogamente, qualsiasi successivo trattamento di dati personali (come i dati personali ottenuti tramite i *cookie*) deve fondarsi su una delle basi giuridiche ai sensi dell'art. 6 del RGPD per essere lecito e rispettare tutte le altre disposizioni del RGPD.

Quanto alla competenza delle autorità, il parere precisa che qualora il trattamento dei dati personali rientri nell'ambito di applicazione materiale sia del RGPD sia della direttiva *e-Privacy*, le autorità sono competenti a vigilare sulle operazioni di trattamento dei dati che sono disciplinate dalle norme nazionali in attuazione della direttiva *e-Privacy* solo se la legislazione nazionale conferisce loro tale competenza. Inoltre, tale controllo deve avvenire attraverso i poteri di vigilanza attribuiti all'autorità di protezione dei dati dalla legislazione nazionale che attua la direttiva *e-Privacy*. La competenza delle autorità ai sensi del RGPD rimane intatta per quanto riguarda le operazioni di trattamento dei dati non soggette a norme speciali contenute nella direttiva *e-Privacy*. Il semplice fatto che una parte del trattamento rientri anche nel campo di applicazione della direttiva *e-Privacy* non limita infatti

la competenza delle autorità di controllo ai sensi del RGPD. Nell'esercizio dei loro compiti e poteri ai sensi del RGPD, le autorità di protezione dei dati possono tener conto delle disposizioni della direttiva *e-Privacy* solo se: una violazione del RGPD costituisce anche una violazione delle disposizioni nazionali di attuazione della direttiva *e-Privacy*. La decisione dell'autorità per la protezione dei dati dovrà tuttavia essere giustificata sulla base del RGPD se la suddetta autorità non è competente, in base al diritto nazionale, ad applicare direttamente le disposizioni nazionali di attuazione della direttiva *e-Privacy*.

Quanto ai meccanismi di cooperazione e coerenza a disposizione delle autorità nell'ambito del RGPD, il parere prevede che gli stessi non si applicano per l'attuazione nazionale della direttiva *e-Privacy*. Tuttavia, i meccanismi di cooperazione e coerenza restano pienamente applicabili ai trattamenti soggetti alle disposizioni generali del RGPD (e non a una "norma speciale" contenuta nella direttiva *e-Privacy*).

Net Neutrality

In vista della revisione delle proprie linee guida in materia di *Net Neutrality*, l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC - *Body of European Regulators for Electronic Communications*) ha inviato al Comitato alcune domande in tema di protezione dei dati sia con riferimento al RGPD che alla direttiva *e-Privacy,* in particolare in relazione alla gestione dei dati di traffico e della fatturazione (offerte a cd. *zero-rating*). La nota di risposta, datata 3 dicembre 2019, richiama l'attenzione sul rispetto del principio di necessità e proporzionalità: i dati trattati per le finalità sopra richiamate devono essere quelli strettamente necessari al loro perseguimento (ovvero il loro trattamento deve essere "*required, unconditional and without alternative*") e i *service provider* devono essere in grado di dimostrare il rispetto di questi principi ogniqualvolta trattano i dati a tale scopo. A parere del Comitato, i dati relativi agli indirizzi URL e ai nomi di dominio possono essere trattati per finalità di fatturazione solo con il consenso dell'interessato. La lettera invita gli *Internet service provider* a utilizzare sistemi di gestione del traffico meno invasivi evitando la *"deep inspection*" dei pacchetti, indicando due possibili esempi (*Explicit Congestion Notification* - ECN o *Differentiated Services Code Point* - DSCP).

Linee guida sulla videosorveglianza

Alla luce delle novità tecnologiche che negli ultimi anni hanno caratterizzato l'ambito della videosorveglianza, il Comitato ha adottato, il 10 luglio 2019, le nuove linee guida sulla videosorveglianza (linee guida 3/2019) che chiariscono in quali termini il RGPD si applichi al trattamento dei dati personali quando si utilizzano dispositivi video e che mirano a garantirne un'applicazione coerente.

Le linee guida, modificate a gennaio 2020 all'esito della procedura di consultazione pubblica, riguardano sia i dispositivi video tradizionali sia i dispositivi video intelligenti. Per quanto concerne questi ultimi, le linee guida si concentrano sulle norme relative al trattamento di categorie particolari di dati. Altre tematiche affrontate nel documento riguardano, tra l'altro, la liceità del trattamento, l'applicabilità dei criteri di esclusione relativi ai trattamenti per finalità strettamente personali e la divulgazione di filmati a terzi.

Le linee guida ribadiscono che, nell'utilizzare i sistemi di videosorveglianza, devono prioritariamente essere rispettati i principi sanciti dall'art. 5 del RGPD applicabili al trattamento di dati personali, tra i quali i principi della liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati. Prima dell'installazione, è necessario accertare che lo strumento sia proporzionato alla finalità perseguita. Il Comitato considera la videosorveglianza come una *extrema ratio* consentendone l'utilizzo solamente quando gli scopi perseguiti non possono essere raggiunti con altre modalità meno invasive. Per minimizzare la raccolta dei dati, il

21

Comitato suggerisce di ricorrere a soluzioni di cancellazione automatica mediante sovrascrittura del registrato, con video accessibili solo in caso di necessità e, quali misure necessarie alla corretta gestione e alla raccolta dei dati personali provenienti da sistemi di videosorveglianza, individua le seguenti: redazione di una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35, par. 3, lett. *c*), del RGPD, in tutti i casi in cui vi sia una sorveglianza sistematica su larga scala di una zona accessibile al pubblico; designazione di un Rpd nei casi in cui vi sia un monitoraggio regolare e sistematico degli interessati su larga scala, ai sensi dell'art. 37, par. 1, lett. *b*), del RGPD.

Linee guida in materia di protezione dei dati *by design* e *by default*

Sempre in tema di nuove tecnologie, il Comitato ha adottato il 13 novembre 2019 le linee guida 4/2019 in materia di *data protection by design* e *by default* nel testo sottoposto a consultazione pubblica, il cui termine è scaduto il 16 gennaio 2020.

Il documento si concentra sugli obblighi fissati in materia dall'art. 25 del RGPD. L'obbligo fondamentale in questo caso è l'attuazione efficace dei principi in materia di protezione dei dati e dei diritti nonchè delle libertà degli interessati fin dalla progettazione e per impostazione predefinita. Ciò richiede che i titolari del trattamento mettano in atto adeguate misure tecniche e organizzative volte ad assicurare l'efficace implementazione dei principi di protezione dei dati. Le linee guida sviluppano questi temi e il Comitato sottolinea più volte che la *data protection by design* e *by default* (DPbDD) è un requisito fondamentale che tutti i titolari devono soddisfare, anche quelli di piccole dimensioni, così come disciplinato dall'art. 25 del RGPD, tenendo conto di una molteplicità di fattori (alcuni dei quali menzionati dal Regolamento stesso). Sia al tempo in cui si determinano i mezzi del trattamento (progettazione del trattamento) e sia all'atto del trattamento stesso, il titolare deve adottare le adeguate misure tecniche ed organizzative per soddisfare i requisiti del RGPD e tutelare i diritti degli interessati.

Il Comitato chiarisce anche il significato di DPbDD dal punto di vista pratico: le linee guida elencano "*design and default elements*" per attuare efficacemente i principi di protezione dei dati facendo ricorso ad esempi; inoltre, esse entrano nel merito dei meccanismi di certificazione menzionati dall'art. 25, par. 3, del RGPD, chiarendo che gli organismi di certificazione dovranno valutare il processo di progettazione (cioè, il processo di determinazione dei mezzi di trattamento), la *governance* e le misure organizzative nonché le misure di garanzia, il tutto nel contesto del trattamento. Il Comitato ribadisce che le autorità di controllo valuteranno la presenza di tali certificazioni ma non ne saranno vincolate (art. 42, par. 4). Infine, nel responsabilizzare non solo il titolare ma anche i responsabili del trattamento ed i *technology providers*, rammentando che tali operatori rivestono un ruolo chiave in vista della DPbDD, il Comitato fornisce 11 raccomandazioni su come i titolari e i responsabili del trattamento nonché i fornitori di tecnologia possano cooperare per raggiungere gli obiettivi di DPbDD.

Linee guida sui criteri relativi al diritto all'oblio

In data 2 dicembre 2019 sono state adottate dal Comitato linee guida sui criteri per l'esercizio del diritto all'oblio relativo ai motori di ricerca (linee guida 5/2019), poste in consultazione pubblica fino al 5 febbraio 2020. Loro obiettivo è quello di fornire una corretta interpretazione del diritto all'oblio (art. 17 del RGPD) nei casi di richiesta di de-indicizzazione (cd. *delisting*) da parte degli interessati che rivolgono l'istanza ai motori di ricerca, alla luce di quanto statuito dalla CGUE all'esito del noto caso C-131/12 (Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja González, sentenza del 13 maggio 2014) e sono state adottate alla luce dei numerosi reclami pervenuti alle autorità di controllo in relazione al rifiuto da parte dei fornitori dei motori di ricerca di aderire a molte delle richieste di cancellazione ricevute.

21

Le linee guida si compongono di due parti: la prima si sofferma sui presupposti che inducono l'interessato ad effettuare una richiesta di deindicizzazione; la seconda, invece, si sofferma sul regime di eccezioni, che consentono al titolare del trattamento di non adempiere alla richiesta dell'interessato.

L'art. 17 del RGPD riconosce all'interessato il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo, se sussiste almeno uno dei sei motivi elencati dalla lett. *a*) alla lett. *f*) del suo par. 1. Nel soffermarsi su ciascuno di tali motivi, il Comitato stabilisce che nel primo caso, ossia quando i dati personali non sono più necessari in relazione alle finalità per le quali sono stati raccolti o altrimenti trattati, nell'analizzare le richieste di *delisting* e al fine di contemperare il diritto alla protezione dei dati con il diritto degli utenti di internet ad accedere alle informazioni, le autorità nazionali devono valutare se, nel corso del tempo, i dati personali sono diventati obsoleti o non sono stati aggiornati, in relazione alle finalità del trattamento originario e ai connessi periodi di conservazione. In merito al secondo motivo – l'interessato ha revocato il consenso su cui si basa il trattamento – le linee guida chiariscono che tale disposizione non si applica ai gestori del motore di ricerca, atteso che il consenso è stato fornito dall'interessato non a tali operatori, ma, ove necessario, ai titolari delle pagine web indicizzate. Pertanto, nel caso in cui l'interessato revochi il proprio consenso all'uso dei dati che lo riguardano su una determinata pagina web, sarà il titolare di quest'ultima a dover richiedere la de-indicizzazione ai motori di ricerca.

In ogni caso, l'istante potrà ottenere la cancellazione dei dati personali, opponendosi al trattamento (terzo caso), purché non vi siano motivi legittimi prevalenti sugli interessi, i diritti e le libertà del richiedente, motivi la cui sussistenza, peraltro, dovrà essere provata dal *provider* del motore di ricerca. Se, quindi, un risultato di ricerca reca un pregiudizio all'interessato quando fa domanda per un lavoro o mina la sua reputazione, il fornitore dovrà considerare il diritto all'informazione, il ruolo pubblico dell'istante, il legame tra le informazioni indicizzate e la vita professionale del medesimo, la circostanza che le informazioni costituiscano incitamento all'odio o configurino un reato (es. diffamazione, calunnia) o che, infine, siano risalenti nel tempo.

Con riferimento al quarto motivo – i dati personali sono stati trattati illecitamente –, secondo il Comitato, l'illiceità deve essere interpretata in senso lato, avendo riguardo non solo alle norme del RGPD, ma anche alle leggi nazionali o alle decisioni giudiziarie di ciascuno Stato membro.

Rispetto al quinto motivo – la richiesta di cancellazione è basata su un obbligo legale previsto dalla normativa nazionale o europea o da un provvedimento dell'autorità giurisdizionale –, la richiesta di cancellazione ha una base normativa specifica e quindi non dovrebbero porsi problemi applicativi o interpretativi di rilievo.

Circa il sesto motivo – i dati personali di cui si richiede la cancellazione sono stati raccolti in relazione all'offerta di servizi della società dell'informazione resi a un minore –, le linee guida precisano che le attività dei gestori di motori di ricerca potrebbero rientrare tra i servizi della società dell'informazione e pertanto si dovrebbero eliminare i contenuti relativi ai minori.

Dopo aver analizzato le ipotesi in cui è possibile esercitare il diritto all'oblio, le linee guida affrontano i casi in cui la richiesta di eliminazione non può essere accolta, in base all'art. 17 del RGPD. Quest'ultimo non si applica, *in primis*, quando il trattamento dei dati personali è necessario per l'esercizio del diritto alla libertà di espressione, incluso il libero accesso alle informazioni. Il Comitato richiama quanto specificato dalla CGUE sul bilanciamento tra diritto all'informazione e diritto alla protezione dei dati, ovvero che l'equilibrio tra tali interessi contrapposti dipende,

in particolare, dal ruolo svolto dall'interessato nella vita pubblica, nonché dal preponderante interesse del grande pubblico ad avere accesso alle informazioni oggetto della richiesta di cancellazione. Altro motivo per cui non si applica l'art. 17 è l'esistenza di disposizioni di legge che obblighino a non cancellare i dati personali. Sul punto, le linee guida ritengono sia improbabile che i fornitori dei motori di ricerca siano obbligati per legge a diffondere determinate informazioni e ciò in quanto essi non creano informazioni. Non viene tuttavia esclusa la possibilità che la legge di uno Stato membro possa imporre tale obbligo ai *provider*, stabilendo, peraltro, un limite di tempo alla pubblicazione, superato il quale, l'esenzione non è più applicabile e la richiesta di *delisting* può essere accolta.

Al di là di tale possibilità, il Comitato afferma che l'esistenza di un obbligo legale di pubblicazione imposto ai titolari dei siti web sorgente non implica necessariamente che il fornitore del motore di ricerca debba rigettare la richiesta di cancellazione. Il diritto di cui all'art. 17 del RGPD è escluso invece nel caso in cui il trattamento avvenga in esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di un pubblico potere. Il Comitato precisa che i fornitori di motori di ricerca, non essendo autorità pubbliche, non esercitano poteri pubblici ed è altresì improbabile che le leggi degli Stati membri possano stabilire diversamente, ovvero che la loro attività o parte di essa sia necessaria per il raggiungimento di un interesse pubblico.

Quanto alle finalità di archiviazione nell'interesse pubblico, della ricerca scientifica o storica o per scopi statistici che legittimerebbero il rigetto della richiesta di *delisting*, in base alle linee guida il fornitore del motore di ricerca deve essere in grado di dimostrare che la cancellazione di un determinato contenuto della pagina dei risultati rappresenta un grave ostacolo o impedisce il raggiungimento delle citate finalità, le quali, secondo il Comitato, possono tra l'altro essere perseguite obiettivamente dal *provider*, senza che sia necessario un collegamento tra il nome dell'interessato e i risultati della ricerca.

Dichiarazione 2/2019 sull'uso di dati personali nel corso di campagne politiche

Il Comitato ha adottato il 13 marzo 2019 la Dichiarazione 2/2019 sull'uso di dati personali nel corso di campagne politiche. In vista delle elezioni europee e di altre elezioni svoltesi in diversi Stati membri nel 2019 (e oltre), il Comitato ha richiamato l'attenzione sull'uso dei dati personali durante le campagne elettorali. Ad avviso del Comitato, le tecniche di trattamento dei dati a fini politici possono comportare gravi rischi, non solo in relazione alla *privacy* e alla protezione dei dati, ma anche rispetto all'integrità del processo democratico. Nel proprio *statement*, il Comitato ha così evidenziato una serie di punti chiave che devono essere presi in considerazione quando i partiti politici elaborano i dati personali nel corso delle attività elettorali.

Protezione dei dati e *e-Health*

In materia di *e-Health* è proseguito il lavoro del Comitato sul tema del trattamento dei dati dei pazienti nell'ambito dell'*e-Health Network*, la rete volontaria di collegamento delle autorità nazionali responsabili dell'assistenza sanitaria *online* degli Stati membri prevista dall'art. 14 della direttiva 2011/24/UE sull'assistenza sanitaria transfrontaliera (cfr. anche Relazione 2018, p. 194).

A seguito di una richiesta di consultazione da parte della Commissione, avanzata ai sensi dell'art. 42, par. 2, del regolamento (UE) 2018/1725 e dell'art. 70, par. 1, del RGPD, in merito alla revisione della decisione di esecuzione della Commissione 2011/890/EU che disciplina l'*e-Health Network*, il Comitato e il GCPD hanno adottato il primo parere congiunto (1/2019) volto a fornire alcune indicazioni sugli aspetti relativi alla protezione dei dati personali riguardanti il trattamento delle informazioni sui pazienti (prescrizioni elettroniche e *patient summary*) posto in essere dall'infrastruttura dei servizi digitali per l'*e-Health* (eHDSI) messa a disposi-

zione dalla Commissione (si tratta di una rete IT privata denominata TESTA che consente lo scambio dei dati sanitari elettronici tra i punti di contatto nazionali per l'*e-Health* dei 22 Stati membri partecipanti e facilita l'interoperabilità dei sistemi europei di sanità elettronica). Il Comitato ha fornito indicazioni circa il possibile ruolo di responsabile della Commissione in relazione al trattamento dei dati personali dei pazienti attraverso la messa a disposizione dell'eHDSI e ha richiamato l'attenzione della stessa sulla necessità di introdurre l'elenco degli obblighi del responsabile, ai sensi dell'art. 28, par. 8, del RGPD, nella revisione della decisione di esecuzione n. 2011/890/UE del 22 dicembre 2011 che stabilisce le norme per l'istituzione, la gestione e il funzionamento dell'*e-Health network*.

Sperimentazione clinica e RGPD

A seguito di una richiesta di consultazione indirizzata al Comitato dalla Commissione europea (DG SANTE) su alcune FAQ che la stessa intendeva predisporre in ordine al rapporto tra il RGPD e il regolamento (UE) n. 536/2014 sulla sperimentazione clinica di medicinali per uso umano, il Comitato ha reso, ai sensi dell'art. 70, par. 1, lett. *b*), del RGPD, un parere relativo all'interazione tra i due regolamenti (parere 3/2019).

Il documento si sofferma sulle differenti basi giuridiche per il trattamento dei dati nel contesto delle sperimentazioni cliniche e dei trattamenti ulteriori, per finalità di ricerca, dei dati raccolti nel corso delle stesse. Il Comitato ricorda che le basi giuridiche possono essere differenti a seconda delle finalità cui sono preordinate le diverse operazioni di trattamento e che il consenso informato, richiesto per la partecipazione allo studio clinico dal regolamento sulle sperimentazioni, è essenzialmente una misura per garantire la dignità e l'integrità delle persone che partecipano allo studio in conformità alla dichiarazione di Helsinki e non la base giuridica del trattamento dei dati.

Processo di revisione del Codice mondiale Anti-doping

Il Gruppo di lavoro sugli sport del Consiglio dell'UE si è rivolto al Comitato per chiedere una valutazione sulla compatibilità con il quadro UE del progetto di Codice mondiale Anti-doping per il 2021 e dei relativi "*International Standard*", con particolare riferimento a quello riguardante la protezione dei dati e alla tutela della *privacy* (ISPPPI).

La lettera di risposta del Comitato, datata 9 ottobre 2019, nel prendere atto dei miglioramenti apportati dall'Agenzia mondiale Anti-doping (WADA) a tali regole nel corso delle precedenti revisioni delle stesse, in linea con le indicazioni fornite a suo tempo dal Gruppo Art. 29 (cfr. i pareri del Gruppo Art. 29 4/2009 - WP 162 e 3/2008 - WP156 nonché la lettera del 5 marzo 2013, Ref. Ares (2013)289160), si focalizza su alcune questioni (molte delle quali già evidenziate dallo stesso Gruppo) che sollevano qualche criticità specie alla luce del nuovo quadro giuridico introdotto dal RGPD e fornisce alcune indicazioni al riguardo. In particolare, il Comitato si sofferma sulla possibilità di estendere l'applicazione delle regole Anti-doping ad atleti che svolgono attività sportiva ricreativa, considerandola un'interferenza sproporzionata nel diritto alla *privacy* e alla protezione dei dati degli atleti; sulla liceità del trattamento dei dati personali, rispetto alla quale si ribadisce che il consenso dell'atleta non può essere considerato una valida base giuridica; sulla vincolatività dello standard internazionale sulla protezione dei dati rispetto alle previsioni dello stesso Codice mondiale Anti-doping o di eventuali altre norme applicabili che forniscano un livello inferiore di protezione; sui periodi di conservazione dei dati e dei campioni biologici degli atleti, ritenuti in alcuni casi non proporzionati; sugli obblighi di pubblicazione in Internet delle violazioni delle regole Anti-doping, rilevandone il carattere automatico e indiscriminato.

21

21.2. *La cooperazione delle autorità di protezione dati nel settore libertà, giustizia e affari interni*

Europol Cooperation Board

In virtù del nuovo quadro normativo creato 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, il controllo sulla legittimità della comunicazione di dati ad Europol da parte delle Forze di polizia 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*) che si è riunito, nel 2019, l'8 maggio e il 28 novembre. Nel corso di queste riunioni sono state condivise le informazioni sulle attività di vigilanza su Europol, ivi comprese quelle sui principali risultati delle ispezioni svolte, sul numero crescente di dati inviati a Europol dagli Stati membri, sul trattamento dei dati su indagati di età inferiore ai 18 anni, sulle conseguenze della Brexit e su FIU.net (una rete informatica che supporta le unità di informazione finanziaria nell'UE nella loro lotta contro il riciclaggio di denaro e il finanziamento del terrorismo).

Gruppo di coordinamento della supervisione del Sistema d'informazione Schengen (SIS II)

Il sistema d'informazione Schengen (SIS II) è il sistema d'informazione centralizzato su larga scala che viene utilizzato come strumento d'ausilio per i controlli sulle persone e sugli oggetti alle frontiere esterne dello spazio Schengen. Secondo quanto previsto dal quadro giuridico del SIS II (regolamento CE 1987/2006 e decisione del Consiglio 2007/533/GAI), la supervisione coordinata del sistema è ad oggi 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), alla quale è rimessa la gestione del sistema centrale.

Nel corso del 2019 il Gruppo di coordinamento della supervisione SIS II si è riunito due volte, il 19 giugno e il 26 novembre (i documenti sono reperibili presso il sito del Gruppo alla pagina: https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en). Nel corso della prima riunione si è riflettuto sugli effetti della Brexit (anche con riferimento alle importanti conseguenze di un eventuale cd. *no deal*) rispetto all'utilizzo del sistema SIS II. A decorrere dal 2021, infatti, il Regno Unito diventerà a tutti gli effetti un Paese terzo e, di conseguenza, a partire da tale data le sue autorità di controllo non potranno più accedere al sistema CSIS. È stato poi affrontato il tema dell'impatto sulla disciplina di protezione dei dati della cd. interoperabilità dei sistemi di informazione di larga scala (l'EES, il VIS, l'ETIAS, l'Eurodac, il SIS e l'ECRIS- TCN) prevista dai due regolamenti, adottati nel maggio 2019, proprio al fine di istituire un quadro per l'interoperabilità tra i sistemi di informazione dell'UE, da un lato, nel settore delle frontiere e dei visti e, dall'altro, nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione (reg. n. 2019/817 e 2019/818). I regolamenti prevedono, tra l'altro, la creazione di un *European Search Portal* (ESP) attraverso cui le autorità competenti degli Stati membri e le agenzie dell'Unione possano ottenere un accesso rapido ai sistemi di informazione dell'UE, ai dati Europol e alle banche dati Interpol. L'ESP non fornirà informazioni a cui l'utente non ha accesso ai sensi della normativa nazionale applicabile e dell'Unione.

Nel corso della seconda riunione si è discusso dell'aumento delle richieste di accesso al SIS da parte di Paesi terzi – nonché della proposta di regolamento che

stabilisce le condizioni per l'accesso ad altri sistemi di informazione dell'UE ai fini dell'*European Travel Information and Authorisation System* (ETIAS).

Il Gruppo ha inoltre discusso del futuro della supervisione sul sistema informativo SIS II che, come per gli altri sistemi informativi dell'Unione nei settori delle frontiere, dell'asilo e della migrazione (EES, ETIAS e VIS), della cooperazione di polizia e giudiziaria (SIS, EPPO, Eurojust, ECRIS-TCN) e del mercato interno (IMI), sarà affidato alla Commissione di controllo coordinato sul trattamento dei dati istituita nell'ambito del Cepd (v. *supra*).

Gruppo di supervisione del sistema Eurodac

Il Gruppo di supervisione del sistema Eurodac (i cui documenti sono rinvenibili sul sito internet alla pagina: https://edps.europa.eu/data-protection/european-it-systems/eurodac_en) è competente per assicurare il rispetto della protezione dei dati personali all'interno del sistema istituito per la comparazione delle impronte digitali dei richiedenti asilo. Il Gruppo, riunitosi il 20 giugno e il 27 novembre 2019, ha continuato il lavoro per il perfezionamento del regolamento relativo alle tecniche adottate per la raccolta delle impronte digitali e ha adottato il *report* sui risultati di un questionario sui diritti degli interessati fatto circolare tra gli Stati membri, da cui è emersa una sostanziale uniformità delle procedure adottate per la raccolta delle impronte digitali, per la distribuzione di opuscoli informativi e per assicurare la correzione e cancellazione dei dati.

È stato inoltre concordato il contenuto di un volantino, preparato in collaborazione con la *European Union Agency for Fundamental Rights* (FRA), di ausilio alle autorità che si apprestano a svolgere il processo di raccolta delle impronte sia dei richiedenti asilo che degli altri cittadini extracomunitari a cui possono essere prese (*migrants apprehended at the external border*).

Infine è stato illustrato il programma triennale 2019-2021 ed eletto il nuovo presidente del sottogruppo, la delegata della Grecia Eleni Maragou.

Gruppo di coordinamento della supervisione del Sistema informativo visti (VIS)

Il Gruppo di supervisione VIS è competente per il monitoraggio del sistema d'informazione visti, 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.

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) ha tenuto due riunioni, il 20 giugno ed il 27 novembre, in occasione delle quali è stato discusso il *Work Programme* 2019-2021. Il Gruppo è stato altresì aggiornato dall'Agenzia EU-LISA (*European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice*) circa alcuni dati dalla stessa acquisiti monitorando il funzionamento del sistema relativamente al periodo 10 gennaio/30 ottobre 2019 ed è stato aggiornato dalla Commissione sullo stato di avanzamento dei lavori relativi all'entrata in funzione dei sistemi EES *Entry-Exit-System* – sistema che si pone l'obiettivo di registrare in una banca dati unica le informazioni in entrata ed uscita di persone di nazionalità non appartenente all'UE che attraversano i confini esterni dell'Unione – e del sistema ETIAS (*European Travel Information and Authorization System*).

Il Gruppo ha lavorato su un rapporto relativo alla formazione del personale delle autorità nazionali che accedono al VIS sulla base delle risposte pervenute a un precedente questionario fatto circolare in materia e ha adottato un rapporto sull'esercizio dei diritti da parte degli interessati nei diversi Stati membri.

21

SID

Il Sistema informativo doganale è volto a consentire la cooperazione tra le autorità nazionali competenti per la prevenzione, la ricerca e il perseguimento di gravi infrazioni delle leggi nazionali in materia (decisione 2009/917/GAI e della decisione quadro 2008/977/GAI) e quelle competenti a contrastare le violazioni di natura amministrativa (sulla base del regolamento (EC) n. 515/1997, consolidato nel 2008). Per i trattamenti effettuati in ambito di polizia e giustizia, la supervisione è attribuita all'Autorità comune di controllo dogane (ACC Dogane) mentre per la cooperazione di tipo amministrativo la competenza è attribuita al Gruppo di coordinamento della supervisione del Sistema informativo doganale (sito internet alla pagina: https://edps.europa.eu/data-protection/supervision-coordination/customs-information-systems_en).

Nel 2019 il Gruppo di coordinamento della supervisione SID si è riunito a Bruxelles il 7 maggio. Il segretariato, in una relazione concernente il piano di lavoro programmato per il biennio 2017-2018, ha rappresentato che quasi tutti gli obiettivi sono stati raggiunti, con particolare riferimento all'adozione di un *format* comune per interrogare il SID, e ha predisposto un questionario relativo alla AFIS *Security Policy*. Sono state inoltre formulate proposte per il nuovo programma di lavoro, che interesserà il biennio 2020-2021, tenendo in considerazione anche eventuali aggiornamenti del quadro legislativo del SID nonché valutando l'opportunità di prevedere sessioni di *training* per coloro che dovranno effettivamente svolgere operazioni di consultazione del Sistema.

21.3. *La partecipazione dell'Autorità in seno al Consiglio d'Europa e ad altri gruppi di lavoro internazionali*

T-PD

È proseguita l'intensa attività dell'Autorità nell'ambito del Consiglio d'Europa, in particolare attraverso la partecipazione al Comitato consultivo della Convenzione n. 108/1981, cd. T-PD, presieduto dalla dottoressa Alessandra Pierucci del Garante dal 2016.

Le due riunioni plenarie del Comitato, tenutesi a Strasburgo il 13-14 giugno e il 19-21 novembre – cui si sono come di consueto aggiunte le tre riunioni annuali del *Bureau*, il gruppo ristretto del Comitato –, sono state caratterizzate da un'altissima partecipazione delle Parti, spesso rappresentate da delegazioni nazionali nutrite, composte da rappresentanti provenienti sia dai ministeri sia dalle autorità di protezione dati, segno della crescente attenzione da parte degli Stati nei confronti delle attività del T-PD.

Nel corso dell'anno sono stati adottati importanti documenti e avviata la riflessione su nuove tematiche che saranno oggetto del programma di lavoro del Comitato per il biennio 2020-2021.

Il Protocollo emendativo della Convenzione 108 che ha dato vita alla cd. Convenzione 108+ ha continuato a mantenere un ruolo centrale nelle attività del T-PD e a suscitare largo interesse tra gli Stati come standard globale di protezione dei dati.

Nel corso del 2019, sedici nuovi Stati hanno firmato il Protocollo emendativo, portando a trentotto il numero complessivo di firme. Tra gli Stati firmatari, oltre all'Italia che ha sottoscritto il Protocollo il 5 marzo 2019, si segnalano anche tre Paesi che non fanno parte del Consiglio d'Europa (Argentina, Tunisia e Uruguay), a sottolineare la "vocazione globale" della Convenzione. Nel corso del 2019 si sono anche registrate le due prime ratifiche (Bulgaria e Croazia) del Protocollo. Si tratta di un ottimo risultato, che va tuttavia completato con una tempestiva ratifica del Protocollo emendativo che può entrare in vigore (oltre che nel caso della ratifica di

tutte le attuali Parti della 108), anche ove nei 5 anni successivi all'apertura alla firma si raggiunga la ratifica di almeno 38 Parti.

Sempre con riferimento alla Convenzione 108+, il Comitato ha continuato il lavoro sui meccanismi, la cui competenza sarà attribuita al futuro comitato convenzionale, di valutazione (*evaluation*) dei futuri candidati ad accedere alla 108+ e di periodico riesame (*follow up*) per verificarne la persistente aderenza ai principi della Convenzione stessa. Oltre al documento descrittivo che spiega i meccanismi di *evaluation* e *follow up*, il Comitato ha lavorato su una bozza di questionario che sarà sottoposto a candidati e Parti nell'ambito di tali procedure. Per completare il lavoro sulle procedure è stato deciso di costituire un gruppo di lavoro composto dai componenti del *Bureau* e dalle delegazioni interessate. Tutto ciò tenendo conto del fatto che, se da una parte l'entrata in vigore della Convenzione (tra almeno cinque anni) consentirebbe una riflessione approfondita su tali procedure, dall'altra, la loro finalizzazione appare di fatto più urgente, in base all'art. 36.2 del Protocollo emendativo. Tale disposizione prevede infatti che a partire dall'apertura alla firma del Protocollo (avvenuta il 10 ottobre 2018) qualunque nuova richiesta di accedere alla 108 debba essere accompagnata dalla richiesta di accessione alla 108+ rendendo quindi necessaria una pronta predisposizione dei meccanismi valutativi previsti da quest'ultima.

Il Comitato ha inoltre proseguito le attività previste dal programma di lavoro per l'anno 2019.

All'esito di procedura scritta, il 25 gennaio 2019 sono state adottate le linee guida in materia di intelligenza artificiale e protezione dei dati (*Guidelines on Artificial Intelligence and Data Protection*) che si rivolgono a *policy makers*, sviluppatori e fornitori di servizi fondati sull'intelligenza artificiale (I.A.) e offrono indicazioni affinché l'impiego di tale tecnologia avvenga nel rispetto dei principi della Convenzione 108+. Nonostante quest'ultima non sia ancora entrata in vigore, essa rappresenta ormai il parametro di riferimento delle raccomandazioni e linee guida del T-PD. Tra i punti più significativi delle linee guida in materia di I.A., si segnalano: la necessità di avere un approccio fondato sulla preventiva valutazione dell'impatto che soluzioni I.A. possono avere sui diritti fondamentali, anche in ragione dei possibili effetti discriminatori che possono da essa derivare e l'opportunità di inserire nel processo di valutazione nuove "forme partecipatorie", basate sul coinvolgimento di individui e gruppi potenzialmente interessati dagli effetti dell'I.A. Ciò per evitare che le scelte sull'utilizzo di tali nuove tecnologie, che rischiano di cambiare radicalmente il nostro modo di stare nella società, siano appannaggio esclusivo di chi detiene il sapere tecnologico.

Raccomandazione (2019) 2

Il 27 marzo è stata adottata dal Comitato dei ministri del Consiglio la raccomandazione (2019) 2 sulla protezione dei dati relativi alla salute. L'adozione della Raccomandazione chiude il lungo percorso di revisione della Raccomandazione (97)2 attualizzando i preesistenti principi di tutela dei dati a fronte delle molte sfide determinate dalla diffusione di nuove tecnologie e della digitalizzazione del settore sanitario (T-PD(2018)06rev). Diversamente dall'originaria raccomandazione, che si riferiva ai "dati sanitari", il nuovo documento muove da una più ampia definizione di "dati relativi alla salute" che comprende i dati personali riferibili alla salute mentale o fisica di un individuo, inclusi quelli che riguardano la fornitura di servizi di cura o che rivelano informazioni sulle condizioni di salute pregresse, presenti e future della persona. Specifiche previsioni riguardano le garanzie rafforzate che, in base all'art. 6 della Convenzione 108+, devono assistere i trattamenti di dati sulla salute. Sono previste ulteriori garanzie per il trattamento dei dati genetici (particolarmente sensibili per il loro carattere predittivo), nonché sulla condivisione dei dati di salute

21

del paziente da parte di più professionisti del settore al fine di garantire la migliore assistenza medica nel rispetto dei diritti delle persone. Ulteriori previsioni riguardano l'uso di dati ai fini di ricerca scientifica, in particolare per assicurare il rispetto del principio di trasparenza. Infine, viene affrontata la questione dei sempre più diffusi dispostivi sanitari mobili (impiantati o meno sulla persona) ai quali si applicano tutti i principi della raccomandazione: segnatamente, stringenti misure di sicurezza, obblighi di trasparenza volti ad informare adeguatamente gli interessati, nonché la necessità di adottare strumenti che garantiscano il pieno controllo sui propri dati.

Il tema protezione dei dati e salute è stato al centro anche di un confronto del T-PD – a margine della plenaria di giugno – con lo *Special Rapporteur* delle Nazioni Unite sul diritto alla *privacy* Joe Cannataci, in particolare in merito alla Raccomandazione – predisposta da un'apposita *Task Force* in ambito ONU – sulla protezione e l'uso dei dati relativi alla salute. In tale incontro rappresentanti della *Task Force* e del T-PD si sono confrontati anche al fine di favorire la coerenza delle rispettive raccomandazioni.

Criminalità informatica

Il Comitato ha inoltre proseguito la discussione in merito alle implicazioni sulla protezione dei dati delle revisioni alla Convenzione di Budapest sulla criminalità informatica. A seguito della pubblicazione da parte del Comitato *cybercrime* del Consiglio d'Europa (T-CY) della bozza del secondo protocollo addizionale alla Convezione di Budapest sottoposto a consultazione pubblica, il T-PD ha potuto valutare le disposizioni concernenti l'accesso diretto da parte delle autorità di *law enforcement* di un Paese ai dati personali relativi agli utenti di servizi di telecomunicazione detenuti dai relativi fornitori stabiliti in un altro Paese e all'accesso ai medesimi attraverso altra autorità dello Stato terzo. Nella plenaria di novembre il Comitato ha adottato un parere su tale bozza di protocollo con il quale sono stati messi in evidenza alcuni punti critici del *draft*, e sottolineato che: a) la soluzione ideale nella predisposizione di qualsiasi nuovo quadro di regole per l'accesso ai dati in questione è che le Parti coinvolte siano anche invitate a ratificare la Convenzione 108+ al fine di assicurare adeguate garanzie sul piano della tutela dei diritti; b) ove ciò non fosse possibile, l'auspicio del Comitato è che siano inserite nel protocollo opportune garanzie in linea con la Convenzione 108+. Il parere del Comitato è stato presentato nella sessione dedicata alla protezione dei dati in ambito di giustizia della Conferenza Octopus tenutasi a Strasburgo dal 20 al 22 novembre 2019 che ha riunito ministri, esperti, rappresentanti della società civile, del *business online* e delle autorità di protezione dei dati per discutere del bilanciamento tra le esigenze investigative e la tutela dei diritti fondamentali.

Dopo l'adozione di importanti lavori come quelli citati, il Comitato ha discusso delle tematiche da affrontare nel successivo biennio. La plenaria di giugno ha adottato, su proposta del *Bureau*, il programma di lavoro 2020-2021.

Profilazione

Tra i temi inclusi nel programma e già oggetto di discussione delle successive riunioni del *Bureau* nonché della plenaria di novembre, si segnala la revisione della Raccomandazione (2010)13 in materia di profilazione. Il Comitato ha infatti concordato sull'opportunità di tornare sul tema, anche per tenere conto delle nuove questioni emerse in tema di *Big data* e intelligenza artificiale (entrambi peraltro oggetto di linee guida nel frattempo approvate dal Comitato), delle crescenti forme di profilazione in ambito pubblico, nonché delle più recenti e frequenti tecniche di manipolazione degli utenti della rete fondate sulla raccolta di dati personali (ad es. Cambridge Analytica). Se infatti la raccomandazione del 2010 aveva un ambito di applicazione trasversale, nei fatti ha tenuto in maggiore considerazione la profilazione da parte di soggetti privati in ambito commerciale, trascurando quella effettuata in altri ambiti o da soggetti pubblici.

Il Comitato ha inoltre concordato di includere nel programma di lavoro il tema del riconoscimento facciale, avviando la discussione al riguardo. Con l'ausilio di due esperti, sono state discusse le implicazioni tecniche e giuridiche di tale tecnologia alla luce dei criteri previsti dalla Convenzione modernizzata sui dati biometrici, inclusi nelle categorie particolari di dati che meritano una protezione rafforzata in base all'art. 6 della Convenzione 108+.

Protezione dei dati nei sistemi scolastici

È stata avviata la discussione relativa alle sfide per la protezione dei dati derivanti dall'uso di nuove tecnologie nell'ambito dell'istruzione (dalle piattaforme di *e-learning*, ai registri elettronici, all'impiego di biometria per l'accesso a istituti scolastici) e dalla progressiva tendenza a inserire gli studenti, fin dalla più giovane età, in *cluster* che ne condizionano lo sviluppo. Anche in questo caso il Comitato ha discusso con gli esperti che, oltre a predisporre un *report* sul tema, hanno elaborato una bozza di raccomandazione sulla quale il Comitato continuerà a lavorare in vista dell'adozione di linee guida.

Le due plenarie sono state occasione anche per ulteriori eventi e discussioni. La plenaria di giugno è stata infatti anticipata da una consultazione pubblica sulla raccomandazione in materia di protezione dei dati relativi alla salute lanciata dallo *Special Rapporteur* delle Nazioni Unite sul diritto alla *privacy* Joe Cannataci (11 e 12 giugno), alla quale ha partecipato la presidente del T-PD e alcuni membri del Comitato anche al fine di favorire la coerenza di tale documento con la mensionata raccomandazione CoE (2019)2 e da una conferenza sulla Convenzione 108+, occasione per un interessante confronto sulle implicazioni pratiche e l'importanza della 108+ in un contesto extra-europeo.

Il Comitato ha continuato a cooperare con gli altri comitati del Consiglio d'Europa sugli aspetti di propria competenza, in particolare, come si è detto, con il Comitato *cybercrime*, per ciò che concerne i profili di protezione dati derivanti dall'applicazione della Convenzione di Budapest; con il Comitato della Convenzione Macolin, contro la manipolazione delle gare sportive; con il Comitato sui *Media* e la Società dell'informazione, fornendo un parere sulla bozza di raccomandazione predisposta dallo stesso CD.MSI sull'impatto dei sistemi algoritmici sui diritti umani.

Premio Rodotà

In occasione della Giornata europea della protezione dei dati (28 gennaio 2019) è stato assegnato per la prima volta il Premio Stefano Rodotà istituito dal Comitato per ricordare il grande giurista e primo Presidente del Garante. Il Premio, destinato a ricercatori e studenti allo scopo di valorizzare e dare visibilità a progetti di ricerca innovativi e originali nel campo della protezione dei dati personali sviluppati in ambito universitario, è stato assegnato a Ingrida Milkaite and Eva Lievens per un progetto dedicato ai diritti del minore presentato dalle vincitrici nella plenaria del Comitato; è stata altresì conferita la menzione speciale a Jef Ausloos per il lavoro condotto sul diritto all'oblio.

CAHAI

Con una decisione dell'11 settembre 2019 del Comitato dei ministri è stato costituito l'*Ad Hoc Committee on Artificial Intelligence* (CAHAI). Il Comitato, sulla base di ampie consultazioni con le parti interessate, ha avuto mandato di esaminare la fattibilità e i principali elementi di un quadro giuridico per lo sviluppo, la progettazione e l'applicazione dell'intelligenza artificiale, basato sulle norme del Consiglio d'Europa in materia di diritti umani, democrazia e stato di diritto. Nell'adempiere a tale compito, il comitato *ad hoc* tiene conto delle norme esistenti in ambito CoE in tale settore, *in primis* le ricordate linee guida in materia di protezione dati e intelligenza artificiale.

Il primo incontro del CAHAI, al quale ha partecipato il Segretario generale del Garante insieme al rappresentante del Mise, si è tenuto a Strasburgo il 18-20

21

novembre. La riunione è stata l'occasione per presentare gli strumenti principali esistenti a livello internazionale e regionale, nonchè per svolgere una prima riflessione sugli elementi e le proposte volte ad indirizzare i lavori del Comitato, in particolare con riferimento alla possibilità che da strumenti di *soft law* si possa passare ad una cornice regolatoria vincolante per le Parti, e sul metodo di lavoro del Comitato.

Il CAHAI, il cui mandato ha una durata di due anni, presenterà un primo rapporto contenente proposte per il Comitato dei ministri entro maggio 2020.

OCSE – WP-DGP

Il Garante ha attivamente partecipato ai lavori dell'OCSE, in seno al WP-DGP, Gruppo di lavoro nato dalla trasformazione del WPSPDE (*Working Party on Security and Privacy in Digital Economy*) in *Working Party on Policies for Digital Data Governance and Privacy* con relativo *spin off* del tema della sicurezza digitale nel neocostituito "*Working Party on Digital Security Policy*" (SDE). Nel corso della prima riunione di novembre 2019 del WP-DGP è stata confermata come vice presidente del *Bureau* per il 2020 la dottoressa Manuela Siano del Garante.

La "ristrutturazione" del WPSPDE si è resa necessaria in quanto, quando il Gruppo WPSPDE è stato creato (nel 1995), la *data governance/privacy* e la *digital security* erano due tematiche emergenti nella maggior parte dei Paesi ed è stato possibile affrontare insieme i due temi e raggiungere una massa critica che ha aumentato la visibilità di ogni area a livello internazionale. Ciò ha permesso all'OCSE di ponderare l'agenda internazionale di entrambe le tematiche per oltre 20 anni e di influenzarle attraverso il lavoro analitico e la produzione di otto raccomandazioni del Consiglio OCSE. Tuttavia negli anni la sicurezza digitale e la *governance* dei dati hanno assunto una tale rilevanza che il doppio mandato del Gruppo di lavoro, che ne era stato un punto di forza, cominciava a limitare la capacità dell'OCSE di fornire sufficiente spazio di discussione a ciascuna area tematica e di elaborare un'agenda strategica altrettanto ambiziosa in entrambi gli ambiti. Pertanto durante la riunione del WPSPDE di maggio 2019 è stata condivisa la necessità di un cambiamento per consentire all'OCSE di mantenere la propria *leadership* in materia di sicurezza digitale e *governance* dei dati/*privacy*. Tale cambiamento si è tradotto nella formazione del citato WP-DGP che raccoglie ora tutte le questioni strettamente dedicate alla sicurezza digitale. Questo Gruppo di lavoro riunisce i responsabili delle politiche di sicurezza digitale dell'OCSE al fine di consentire a questa comunità di: i) fissare l'agenda politica nel settore della sicurezza digitale per la prosperità; ii) sviluppare politiche di sicurezza digitale basate sull'evidenza e una guida pratica per creare fiducia nella trasformazione digitale e sostenere la resilienza, la continuità e la sicurezza delle attività critiche; iii) cooperare, condividere le migliori pratiche e condurre discussioni tra le parti interessate sulla sicurezza digitale.

Revisione delle *Privacy guidelines*

Nel corso delle riunioni del WPSPDE (maggio 2019) e del WP-DGP (novembre 2019) si è dato il via al lavoro di revisione delle linee Guida OCSE sulla *Privacy* (*Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*), adottate dal Consiglio OCSE nel 2013. Il neo-costituito gruppo di esperti (PGEG), a cui il Garante partecipa, sta guidando il lavoro di revisione in corso. Si ricorda che le prime *Privacy guidelines* risalgono al 1980 e rappresentano il primo *set* di principi di protezione dati internazionalmente riconosciuti. Contengono le definizioni rilevanti in materia di *data protection* e forniscono otto principi fondamentali per la relativa applicazione nazionale: limitazione della raccolta dati, qualità dei dati, specificazione degli obiettivi, limitazione dell'uso, salvaguardia della sicurezza, apertura, partecipazione individuale e responsabilità (*accountability*). Con la revisione del 2013 è stata riaffermata la validità dei predetti principi che restano la base su cui articolare il nuovo lavoro di aggiornamento. Le *Privacy guidelines* del 2013 sono state adottate in forma di

21

Raccomandazione contenente un'istruzione del Consiglio OCSE al *Committee on Digital Economy Policy* (CDEP) di "monitorarne l'attuazione, riesaminare il contenuto e riferire al Consiglio entro cinque anni dalla loro adozione". Pertanto la nuova revisione si è resa necessaria e sta procedendo con *focus* iniziale sul monitoraggio delle misure intraprese dai governi in loro attuazione, quali buone pratiche e strumenti per affrontare le nuove sfide poste dalla tecnologia nel contesto della dimensione globale della protezione dati e del nuovo quadro europeo per la protezione dei dati, soprattutto in merito alla semplificazione ed omogeneizzazione delle norme europee. Il PGEG ha concentrato la prima fase del lavoro di revisione sull'analisi dei citati principi fondamentali delle *Privacy guidelines* nel contesto attuale e sui risultati di un apposito questionario (*Privacy guidelines questionnaire*) che i membri del WPSPDE hanno compilato nel corso dell'anno.

Al fine di approfondire il non facile lavoro di revisione delle *Privacy guidelines*, nel corso delle riunioni del WPSPDE e del WP-DGP si sono tenute due tavole rotonde, su temi chiave in vista dell'aggiornamento del testo. All'esito della prima, incentrata sul tema dell'*accountability* e co-organizzata dal WPSPDE e dal CIPL (*Centre for Information Policy Leadership*) si è sottolineata la necessità di una comprensione comune della locuzione nonché dell'individuazione degli elementi fondamentali della stessa. Nel corso della seconda, organizzata congiuntamente dalla DPA britannica (ICO) e dall'*Electronic Privacy Information Centre* (EPIC), sono state esaminate le sfide da affrontare in materia di *privacy* e protezione dei dati personali, anche nel contesto delle nuove tecnologie, che potrebbero richiedere approcci politici innovativi e una forte collaborazione transfrontaliera. Si è affrontato il tema delle sfide per le PEAs (*Privacy Enforcement Authorities*) nel mettere al centro delle *policy* di I.A. la protezione dei dati e il potenziale ruolo e impatto della raccomandazione OCSE sull'intelligenza artificiale [OCSE/LEGAL/0449] (Raccomandazione AI).

Protezione dei minori *online*

Il WPSPDE ha avviato il lavoro di revisione della Raccomandazione OCSE sulla protezione dei minori *online*, adottata dal Consiglio OCSE nel 2012, in relazione alla quale è stato istituito un gruppo di esperti che sta guidando la *review* cui pure il Garante prende parte. La Raccomandazione è stata ritenuta non più al passo con i tempi, essendo trascorsi più di cinque anni dalla sua adozione ed essendo profondamente mutato il contesto delle attività dei minori in rete. Pertanto il gruppo di esperti ha iniziato l'analisi dei nuovi rischi emergenti per i minori *online*. Vi è inoltre un dibattito nazionale e internazionale in corso sulla possibilità di rendere giuridicamente vincolanti i codici di condotta adottati dall'industria, monitorati da un regolatore indipendente e sostenuti da un regime di sanzioni. Il Segretariato ha presentato un *progress report* che include gli esiti della seconda consultazione informale del gruppo di esperti tenutasi in sede OCSE il 30 settembre – 1° ottobre 2019. Si segnala un generale scetticismo sull'efficacia dei tradizionali strumenti di *data protection*, in particolare del consenso, sia in ragione della limitata consapevolezza dei minori sui contenuti che gli stessi diffondono in rete, sia per la sempre maggiore importanza commerciale assunta dai dati "inferiti", che per loro natura sono al di fuori della sfera di controllo individuale e maggiormente nella sfera di controllo del soggetto che tratta i dati. Conseguentemente, solo in via residuale le raccomandazioni attingono ai principi stabiliti nel RGPD, e fanno invece maggiore affidamento sulla promozione di azioni preliminari di carattere educativo; su efficaci interventi regolatori *ex post* (sulla scorta del paradigma *notice-and-take-down* impiegato per la tutela del diritto d'autore), con precise attribuzioni di responsabilità ai differenti attori nella catena della pubblicazione di materiale *online*; su un robusto insieme di tutele tecnologiche (*privacy by design* e *by default*) applicate in particolare ai dati che

21

possono avere un impatto sulla vita *offline* (ad es. dati di localizzazione). Oggetto di discussione ha formato altresì la struttura della Raccomandazione che potrebbe essere suddivisa in gruppi tematici (ad es. cittadinanza digitale e alfabetizzazione; risposte proporzionali ed efficaci; coinvolgimento delle parti interessate; risposte basate sulla tecnologia ecc.). Infine è stata condivisa la necessità che la revisione miri a creare un documento in grado di resistere nel tempo ai cambiamenti tecnologici rimanendo tecnologicamente neutrale.

IWGDPT

È proseguita la partecipazione dell'Autorità all'*International Working Group on Data Protection in Telecommunications* (cd. Gruppo di Berlino) che si è riunito il 9-10 aprile a Bled (Slovenia) e il 10-11 ottobre a Bruxelles. Come di consueto le riunioni sono state l'occasione per un proficuo scambio di informazioni tra le autorità di protezione dati riguardo alle attività e l'esperienza maturata nel settore delle telecomunicazioni.

Nel corso della prima riunione sono stati adottati due *working paper*, rispettivamente sugli *smart devices* destinati a minori e sulla tutela della *privacy* dei minori *online* (reperibili sul sito web: https://www.datenschutz-berlin.de/).

Il primo documento offre una panoramica dei rischi sulla protezione dei dati riferiti ai minori derivanti dall'impiego di dispositivi intelligenti (dai cd. *smart toys* ai dispositivi per il controllo dei bambini anche attraverso localizzazione e tracciamento) e contiene specifiche raccomandazioni destinate ai diversi attori coinvolti nei relativi trattamenti di dati personali: produttori dei dispositivi, terze parti (ad es. i fornitori di applicazioni), organismi di standardizzazione, utenti (genitori/tutori e minori), scuole e insegnanti, autorità di protezione dei dati.

Con riferimento ai rischi, si evidenziano la mancanza di trasparenza sulle finalità del trattamento, sui tempi di conservazione e sugli utilizzi secondari dei dati, sulla possibilità che le condizioni di uso degli stessi siano modificate senza che gli utenti ne siano consapevoli, nonché in ordine alle misure di sicurezza. Particolare attenzione è prestata al cd. *best interest of children*, criterio fondamentale nella valutazione delle questioni relative ai minori e di cui occorre tenere conto fin dalla fase di progettazione.

A fronte delle criticità emerse, il documento evidenzia l'importanza di promuovere dispositivi che siano stati precedentemente certificati (anche tenendo conto del nuovo *framework* in materia di *cybersecurity*); di mitigare con specifici impegni assunti dai produttori i rischi di *nudging* (ossia il processo con cui si induce una persona a compiere azioni sfruttando un'asimmetria informativa o uno sbilanciamento di forze, attraverso un piccolo incentivo); di innalzare il livello di trasparenza, chiarendo con esattezza lo scopo dei trattamenti e modulando l'informativa a seconda dei destinatari (minori e genitori/tutori) e notificando a questi ultimi ogni eventuale modifica delle condizioni di uso del dispositivo; di assicurare l'assenza di usi secondari (se non legittimati da un valido presupposto giuridico); di indicare con precisione tutti gli obblighi contrattuali con gli utenti, in accordo con il principio di necessità.

Agli utenti (minori e genitori/tutori) nonché alle scuole e agli insegnanti viene raccomandato di adottare una speciale cautela affinché sia assicurato un uso consapevole e responsabile dei dispositivi.

Il documento relativo alla tutela della *privacy* dei minori *online*, anch'esso adottato nella riunione di Bled, fornisce specifiche raccomandazioni volte a: rafforzare le garanzie per i minori nei servizi *online* con un uso più ampio del consenso genitoriale; innalzare la trasparenza con un linguaggio pensato per i minori e ad essi specificamente rivolto; mitigare i rischi di lungo termine con un pronto esercizio dei diritti, in particolare di cancellazione, in ogni momento e specie una volta

raggiunta la maggiore età; promuovere un atteggiamento proattivo da parte dei titolari del trattamento nella verifica del consenso individuale (e non più parentale) in corrispondenza del passaggio dell'interessato all'età adulta (naturalmente senza che ciò comporti un tracciamento sistematico del minore, e solo nei casi in cui il momento del passaggio all'età adulta è noto al titolare); promuovere l'impiego di protocolli di verifica dell'età (*age verification*) basati su tecniche crittografiche di tipo *zero-knowledge proof*, che non richiedono la conoscenza dell'età ma il superamento di una soglia.

Il Gruppo ha anche avviato il lavoro sui temi della *data portability*, ritenuto particolarmente importante dalle delegazioni dei Paesi in cui questo diritto non è ancora riconosciuto, e della profilazione.

GPEN

Anche nel corso del 2019 è stato lanciato il *Privacy Sweep*, l'iniziativa 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) ha riguardato il tema della gestione delle violazioni di dati personali (*data breach*) da parte di soggetti pubblici e privati che operano sui rispettivi territori nazionali. Allo *Sweep* 2019 hanno partecipato, oltre a quella italiana, altre 15 autorità garanti della *privacy* di vari Paesi del mondo, ognuna delle quali ha scelto autonomamente lo specifico settore su cui concentrare l'analisi.

Dall'indagine internazionale è emerso che le organizzazioni intervistate hanno mostrato un alto livello di consapevolezza delle migliori pratiche da utilizzare per rispondere adeguatamente alle violazioni dei dati. La stragrande maggioranza delle predette organizzazioni ha provveduto, ad esempio, alla nomina di un *team* dedicato alla gestione delle violazioni dei dati, mentre un'ampia maggioranza delle stesse, ha dichiarato di avere procedure "molto buone" o "buone" in caso di una violazione dei dati e al fine di prevenirne la reiterazione.

Sul fronte interno, il Garante ha analizzato le aziende del settore *e-commerce*. L'indagine svolta in Italia ha visto un tasso molto basso di risposta (circa 17 questionari ricevuti su 254 aziende interpellate), ancorché si sia registrata una complessiva consapevolezza del quadro giuridico in materia di violazioni dei dati personali. La maggior parte delle imprese ha dichiarato di non avere subito violazioni di dati personali; il livello di implementazione di politiche e procedure è generalmente correlato alla dimensione delle aziende (quelle più grandi hanno procedure meglio strutturate), ma nessuna ha previsto procedure basate sugli standard internazionali (es. ISO/IEC 27035). L'80% delle imprese ha designato un Rpd che, di solito, è coinvolto nella stesura delle procedure e delle politiche organizzative e nella gestione della violazione dei dati. Con riguardo alla formazione del personale, è risultato che i programmi di formazione non sono stati specifici o incentrati sul riconoscimento delle violazioni dei dati.

21.4. *Le Conferenze internazionali ed europee*

41ma Conferenza internazionale - ICCD.PC

La 41ma Conferenza internazionale delle autorità di protezione dei dati, intitolata "*Convergence and connectivity raising global data protection standards in the digital age*", si è tenuta a Tirana dal 21 al 24 ottobre. Il riconoscimento della *privacy* come diritto fondamentale per il corretto funzionamento delle democrazie, la lotta sui *social media* ai messaggi inneggianti al terrorismo, una maggiore cooperazione tra le autorità che tutelano i dati personali e quelle che operano a tutela dei consumatori e della concorrenza, nonché la riduzione dell'errore umano quale causa delle vio-

21

lazioni dei dati, sono alcuni dei temi principali definiti nel corso della conferenza dalle oltre 120 autorità intervenute all'evento annuale, le quali hanno lavorato per delineare un programma di lavoro comune in grado di rafforzare la protezione dei dati su scala globale. Nel corso dei lavori sono state adottate sei risoluzioni:

- la Risoluzione sulla *privacy* come diritto fondamentale e precondizione per la democrazia (che ha visto come *co-sponsor* il Garante), che riconosce il ruolo fondamentale di questo diritto per il corretto funzionamento delle democrazie sottoposte, tra l'altro, ai rischi generati dalla profilazione e dall'uso di messaggi manipolatori in campo politico. A tale proposito, è stato chiesto un intervento efficace anche a governi, legislatori e mondo imprenditoriale;
- la Risoluzione sul ruolo dell'errore umano nei *data breach*, che evidenzia la necessità di un'adeguata formazione del personale, di ulteriori misure per la riduzione del rischio e della costituzione di un archivio globale nel quale tener traccia delle violazioni;
- la Risoluzione sulla promozione di strumenti concreti di breve e lunga durata e una continuativa strategia giuridica per un'efficace cooperazione nell'*enforcement* transnazionale, mappando di eventuali impedimenti giuridici riscontrati nelle procedure di cooperazione, così da favorire l'individuazione di apposite soluzioni;
- la Risoluzione per supportare e facilitare la cooperazione tra autorità di protezione dati e le competenti autorità per la tutela dei consumatori, nonché per individuare elevati standard di protezione dati nell'economia digitale, sì da ampliare lo spettro di azione delle autorità, auspicando e chiedendo un miglior coordinamento con altri importanti regolatori del mercato digitale;
- la Risoluzione sui *social media* e i contenuti *online* estremisti, che propone misure urgenti contro i messaggi d'odio, senza limitare il diritto di espressione;
- la Risoluzione che delinea il piano d'azione della Conferenza fino al 2021 e prevede di garantire un'organizzazione più strutturata alla rete globale di Autorità *privacy* (ICD.PPC), trasformandola, a decorrere dal 15 novembre 2019, in un nuovo organismo permanente, la *Global Privacy Assembly* (GPA).

Spring Conference

La *Spring Conference*, tenutasi a Tbilisi (Georgia) il 9-10 maggio, si è articolata in 4 sessioni principali dedicate rispettivamente al RGPD, alla Convenzione 108+, alla protezione dei dati relativi ai minori e ai requisiti dei trattamenti effettuati dalle organizzazioni internazionali.

Nella prima sessione è stato presentato un primo bilancio del RGPD a un anno dalla sua piena applicazione, in particolare tenendo conto delle principali linee guida e raccomandazioni adottate dal Comitato, nonché delle questioni relative alla cooperazione tra autorità anche alla luce dei nuovi poteri e risorse ad esse riconosciute.

Nella seconda sessione è stato proposto un aggiornamento sulla Convenzione 108+ (ad un anno dalla *Spring Conference* tenutasi in Albania, quando gli esiti della modernizzazione erano ancora incerti). È stato sottolineato che la Convenzione 108+ ha già ricevuto un alto numero di firme da parte degli Stati, nell'auspicio di addivenire ad un altrettanto alto numero di ratifiche.

Nella terza sessione, dedicata alla protezione dei dati relativi ai minori, specie con riferimento alle novità introdotte dal RGPD e dalla Convenzione 108+, il Segretario generale del Garante Giuseppe Busia ha presentato l'esperienza dell'autorità italiana in tale settore, ed in particolare le competenze del Garante nell'ambito del cyberbullismo. La sessione ha inoltre trattato il tema della cd. *age verification* nei servizi *online*, soffermandosi sulle esperienze relative alla sensibilizzazione dei minori sui rischi derivanti da internet.

Nella quarta sessione sono state presentate le *policy* adottate da alcune organizzazioni internazionali per adeguarsi ai principi del RGPD, specie con riferimento ai trasferimenti di dati all'estero. Come in altre occasioni, forte è stata la richiesta delle stesse organizzazioni affinché sia rafforzato il dialogo con gli interlocutori europei, anzitutto le autorità di protezione dati, il Comitato e la Commissione.

Nel corso della Conferenza, dopo una lunga discussione, la maggioranza delle delegazioni ha votato a favore dell'accreditamento della Turchia tra i Paesi partecipanti alla *Spring Conference*.

X Conferenza internazionale "*Personal Data Protection*" – Mosca

L'Autorità ha preso parte alla X Conferenza internazionale "*Personal Data Protection*" (Mosca, 7 novembre 2019) organizzata dal "*Roskomnadzor*" (il Servizio federale di supervisione delle comunicazioni di massa). Alla conferenza sono stati invitati rappresentanti di autorità della protezione dei dati personali dall'Europa, Asia, America del Nord ed America Latina, rappresentanti di autorità pubbliche della Federazione russa, nonché enti ed aziende che trattano dati personali su larga scala ed esperti di settore. Le tematiche in discussione hanno riguardato l'economia digitale e altri fattori che influenzano lo sviluppo del sistema di protezione della *privacy*; gli approcci alla depersonalizzazione e all'anonimizzazione dei dati come base per pianificare e prevedere i processi sociali ed economici; la regolamentazione normativa sul trasferimento di dati personali nel contesto della digitalizzazione dell'economia; la formazione di un mercato dei dati nel contesto della sovranità elettronica nazionale (RGPD, localizzazione di banche dati, flussi di informazioni transfrontalieri). Nel corso dell'evento è stato particolarmente approfondito il tema della conformità alle normative internazionali in materia di protezione dati, anche ai fini di sviluppo economico, industriale e di apertura dei Paesi ai mercati internazionali.

21.5. *I progetti per l'applicazione del RGPD finanziati dall'UE: T4DATA e SMEDATA*

T4DATA

Nel 2019 si sono concluse le attività previste dal progetto europeo T4DATA (*Training For Data*), avviato nel 2017 nell'ambito della selezione della Commissione europea denominata "*Support training activities on the data protection reform*", e coordinato dalla Fondazione Basso in consorzio con il Garante, nonché con le autorità di protezione dati di Spagna, Polonia, Croazia e Bulgaria. Il progetto si è rivolto ai soggetti pubblici con l'obiettivo di formare i "formatori", intesi sia come autorità di protezione dei dati, sia come Rpd in quanto responsabili di vigilare e promuovere la corretta applicazione del RGPD. Si è articolato in due fasi di implementazione, distinte ma strettamente connesse: la prima, dedicata primariamente alle autorità di protezione dati, conclusasi nel 2018 con la predisposizione di un "Manuale per gli Rpd", pubblicato sul sito del Garante a inizio 2019 in versione italiana. La seconda, svoltasi nel corso del 2019, si è incentrata sullo svolgimento di attività formative prevalentemente a livello nazionale, con il raggiungimento di due risultati essenziali:

- l'erogazione, attraverso una piattaforma *web-based* dedicata, di *webinar* destinati ai Rpd del settore pubblico;
- l'organizzazione di incontri formativi (*local seminar*) in diverse aree geografiche del Paese al fine di avvicinare i Rpd operanti nei diversi contesti nazionali in ambito pubblico e offrire occasioni di formazione gratuita.

La piattaforma contiene i *webinar* realizzati con la collaborazione di funzionari e dirigenti del Garante, suddivisi in quattro moduli per un totale di oltre 40 ore di lezione: 1) I fondamentali della protezione dei dati; 2) Ruolo e competenze del

21

Rpd nel settore pubblico; 3) Il *toolkit* del Rpd; 4) Approfondimenti settoriali. A disposizione degli utenti anche le *slides* utilizzate per ciascun *webinar*, un breve questionario di autovalutazione e il richiamato Manuale. I seminari di formazione (con uno spazio dedicato a domande e risposte) sono stati organizzati in quattro regioni, anche grazie alla collaborazione delle autorità locali, affrontando tematiche diverse: Ancona (Il trattamento dei dati personali per finalità di cura e ricerca); Catanzaro (La protezione dei dati personali e la trasparenza della Pubblica amministrazione dopo il Regolamento (UE) 2016/679); Torino (La gestione del rischio e la sicurezza del trattamento); Roma (Le responsabilità del trattamento e le sanzioni). Tutti gli incontri hanno registrato un'elevata partecipazione.

La conclusione del progetto è stata segnata da due eventi di carattere transnazionale:

- un *workshop*, tenutosi a Roma il 14 novembre e riservato ai *partner* del progetto, con l'obiettivo di fare il punto sulle attività svolte e sottoscrivere un "protocollo di cooperazione" al fine di proseguire le attività di disseminazione dei contenuti formativi a livello nazionale secondo criteri comuni e condivisi;
- una conferenza internazionale conclusiva, tenutasi a Roma il 15 novembre presso il Centro Alti Studi del Ministero della difesa. La conferenza, che ha registrato un'elevata partecipazione, si è articolata su un'intera giornata con quattro diverse sessioni; è stata l'occasione per allargare l'analisi a temi anche di scenario partendo dal lavoro svolto nel progetto, grazie ai contributi dei relatori (fra cui rappresentanti del Gepd e studiosi di chiara fama) e dei *partner* del progetto.

SMEDATA

SMEDATA è un progetto della durata di 24 mesi, iniziato il 1° dicembre 2018 e cofinanziato all'80% dalla Commissione europea, che ha come obiettivo di garantire l'effettiva applicazione del RGPD attraverso la sensibilizzazione, la moltiplicazione della formazione e lo sviluppo sostenibile delle capacità per le Pmi e le professioni legali. Il consorzio di progetto è composto da sette *partner* appartenenti a due Stati membri, Bulgaria e Italia, i quali rappresentano tutti i principali soggetti che si occupano di protezione dei dati personali. Il coordinatore del progetto è la Commissione per la protezione dei dati personali della Repubblica di Bulgaria; alcune importanti attività del progetto sono guidate dal Garante. Altri membri del consorzio sono l'APIS Europe JSC, l'Unione dei giuristi bulgari, Ernst & Young Bulgaria, l'Associazione europea delle donne avvocato - Bulgaria e l'Università "Roma Tre". Gli obiettivi del progetto per il 2019 sono stati:

- *Sensibilizzazione e formazione:* sono stati organizzati 24 eventi regionali di sensibilizzazione (12 in Italia e 12 in Bulgaria). I predetti 12 eventi di formazione regionali di competenza italiana, organizzati tra settembre e novembre in collaborazione con il Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, sono stati tenuti da dirigenti e funzionari dell'Autorità, professori universitari ed esperti giuridici, per un totale di oltre 70 ore di lezione. Gli eventi formativi si sono tenuti tra settembre e novembre e hanno fatto tappa in 6 città (Milano, Genova, Firenze, Roma, Salerno e Cosenza) coinvolgendo complessivamente oltre 1.400 partecipanti, tra imprenditori delle Pmi e professionisti;
- *Strumento di autovalutazione per una sensibilizzazione sostenibile, basato sulle specifiche necessità e trattamenti delle Pmi dalla prospettiva della protezione dei dati personali:* come da requisito di progetto, è stata elaborata una proposta di criteri per la costruzione di uno strumento di autovalutazione che intende fornire alle Pmi di differenti dimensioni e appartenenti a differenti settori economici, il supporto ad un'autonoma valutazione del proprio livello di con-

formità al RGPD. Il progetto richiede inoltre che tale proposta sia sottoposta al giudizio di esperti, quali rappresentanti di Pmi, associazioni di categoria e docenti universitari. A tal fine sono stati organizzati, nel mese di ottobre, 2 *workshop* in cui è stato presentato il documento contenente la bozza di criteri per la costruzione dello strumento di autovalutazione. Ai *workshop* hanno partecipato dirigenti e funzionari di Confcommercio, Confartigianato, Confapi, AEPI, Federfarma, AIIP e di Pmi a queste associate, nonché rappresentanti delle università. Alla presentazione è seguito un confronto tra i partecipanti, che hanno avuto occasione di offrire pareri e riscontri sul documento illustrato;

- *Sviluppo di un'applicazione mobile per i cittadini e le Pmi:* al fine di aiutare i cittadini e le Pmi a comprendere e adempiere al RGPD, è stata sviluppata, con il contributo del Garante, un'applicazione mobile gratuita e *open source* intitolata "*RGPD in your pocket*", ricca di contenuti informativi in materia di protezione dati.

22 Attività di normazione tecnica internazionale e nazionale

Il Garante ha proseguito la collaborazione in tema di elaborazione di norme tecniche internazionali nell'ambito del *Working Group 5* del sottocomitato SC27, che si occupa della sicurezza delle informazioni all'interno del comitato tecnico JTC1 dell'organizzazione internazionale per la normazione (ISO). Il gruppo di lavoro segue gli aspetti di sicurezza nella gestione delle identità relativamente alle tecnologie biometriche e alla protezione dei dati personali.

Armonizzando la propria posizione con quelle delle altre autorità di protezione dei dati tramite il Cepd, che ha una *liason* in proposito con ISO, l'Autorità ha seguito lo sviluppo delle norme tecniche di seguito riportate:

- ISO 27701 - *Information technology - Security techniques – Enhancement to ISO/IEC 27001 for privacy management – Requirements*, che stabilisce i requisiti di un sistema di gestione della *privacy* delle informazioni (PIMS) a completamento di un sistema di gestione per la sicurezza delle informazioni (ISMS - ISO 27001);
- ISO 29184 - *Guidelines for online privacy notice and consent*, che definisce una serie di requisiti per fornire l'informativa e acquisire il consenso *online* in modalità *user friendly*;
- ISO 27570 - *Privacy guidelines for smart cities*, che fornisce linee guida sull'utilizzo degli standard *privacy* nell'ambito *smart cities*;
- 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/periodi di mantenimento, di classi di cancellazione, di 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*.

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*".

L'Autorità inoltre contribuisce all'elaborazione di norme tecniche europee nell'ambito del comitato tecnico 8 del Cen Cenelec che si occupa dello sviluppo di norme su "*Privacy management in products and services*" su mandato della Commissione europea (Direzione generale sicurezza e affari interni) per l'elaborazione di norme tecniche per la "*Privacy by Design and by Default*", a supporto degli artt. 42 e 43 del RGPD per la definizione di requisiti armonizzati a livello europeo, in accordo con lo *European Qualifications Framework* – EQF.

Nello stesso tempo è proseguita la collaborazione con Uninfo, l'ente di normazione federato con Uni (Ente nazionale italiano di unificazione), contribuendo all'elaborazione della Circolare Tecnica DC N. 10/2019 – Disposizioni in merito all'accreditamento norma ISO/IEC 27701.

23 L'attività di comunicazione, informazione e di rapporto con il pubblico

23.1. *La comunicazione del Garante: profili generali*

Il Garante affida da sempre un ruolo particolarmente importante all'attività di informazione e comunicazione istituzionale ritenendola fondamentale per la diffusione e la crescita di una "cultura della protezione dati" tra tutti gli attori della società: cittadini, imprese, enti, istituzioni.

In quanto Autorità pubblica, inoltre, valorizza le attività di comunicazione e informazione per garantire il corretto adempimento delle finalità connesse alla trasparenza dell'azione amministrativa, all'ottimizzazione dell'efficacia e dell'efficienza delle procedure svolte e dei servizi resi, nonché per garantire in modo corretto e soddisfacente la relazione con il cittadino e l'ascolto dell'utenza.

Per svolgere al meglio i compiti e le finalità descritte, già da qualche anno l'Autorità ha rinnovato le strategie ed i canali di comunicazione, sperimentato nuove tecniche, come lo *storytelling*, testato nuove forme di linguaggio (soprattutto audiovisivo) e scelto di volta in volta nuovi prodotti ritenuti più idonei a veicolare in modo efficace le informazioni relative agli interventi operati dal Collegio su settori di interesse sociale e semplificare la comprensione dei principali provvedimenti adottati e delle nuove norme europee. Nel 2019 sono stati potenziati soprattutto i canali *social* ed è stata particolarmente curata la produzione multimediale di campagne di informazione destinate al web.

La consapevolezza di vivere in una società che rischia di scivolare nella classificazione di massa e nella ipersorveglianza senza ritorno – attraverso il ricorso massiccio all'uso di tecnologie sempre più evolute e alla raccolta, conservazione e utilizzo di quantità enormi di informazioni – ha indotto il Garante a mantenere alta l'attenzione sui problemi della sicurezza digitale, a livello nazionale ed internazionale, e ad intensificare la sua azione di informazione e comunicazione per promuovere il rispetto del diritto alla protezione dei dati personali degli individui.

I dati sono diventati un fattore strategico nella produzione, nella competizione dei mercati, nelle innovazioni di importanti settori pubblici e privati, nella crescita economica, nell'offerta di servizi innovativi, nello sviluppo di servizi per la salute e nel progresso sociale. Il loro trattamento tuttavia comporta potenziali rischi per la riservatezza.

E proprio il tema delle connessioni tra tecnica, società e diritto è stato oggetto del convegno "I confini del digitale. Nuovi scenari per la protezione dei dati", organizzato dall'Autorità nel mese di gennaio per celebrare la Giornata europea per la protezione dei dati personali.

Particolarmente attento a quanto accade nella dimensione digitale, il Garante ha svolto attività di informazione e prevenzione concentrando il proprio impegno su alcuni grandi temi prioritari: il *cybercrime* diffuso ed il furto d'identità; i grandi monopoli della rete, l'intrusione informatica e la perdita di dati (*data breach*); la profilazione occulta attraverso algoritmi, le rilevazioni biometriche, le *app* per il controllo di massa a fini di sicurezza e giustizia, o di condizionamento dell'opinione pubblica per scopi politici o economici, analisi statistiche e di mercato.

I temi

Anche il variegato mondo dei *social network* è stato seguito dal Garante, con

23

particolare riguardo al contrasto al cyberbullismo ed alla violenza in genere, soprattutto se perpetrata su minori, disabili, donne: il *revenge porn*, il *sexting*, l'*hate speech*, e la conseguente necessità del rafforzamento della disciplina del diritto all'oblio e la promozione e sensibilizzazione ad un uso responsabile della rete.

Per i giovani, sono state promosse anche attività di "comunicazione alternativa" sulle tematiche *privacy* in ambito scolastico. L'Ufficio ha coadiuvato il Miur nella realizzazione e nella promozione dello spettacolo teatrale "A Scuola con la *privacy*", andato in scena il 12 giugno 2019 presso il teatro Eliseo di Roma: si è trattato di una rilettura teatrale, recitata da bambini di 10-12 anni, della normativa *privacy* italiana ed europea, in un'ottica di *peer education* con l'obiettivo di divulgare tali temi utilizzando un linguaggio semplice ed evocativo, compatibile con l'età dei giovani interpreti, ma in grado di intercettare anche l'interesse degli adulti (genitori, dirigenti scolastici, corpo docente, personale amministrativo e tecnico, alunni di ogni ordine e grado).

Altri ambiti verso i quali l'Autorità ha rivolto l'attività di informazione sono stati: il *telemarketing* aggressivo; il contrasto all'evasione fiscale; il reddito di cittadinanza; la *digital economy*; settori della finanza e la sfida delle piattaforme web per gestire i dati delle transazioni finanziarie e le criptovalute; le intercettazioni, segnatamente mediante captatori informatici; i sistemi di videosorveglianza; le rilevazioni biometriche; il mondo dei lavoratori; la scuola.

T4DATA e SMEDATA

L'attività di sensibilizzazione rispetto alle innovazioni correlate al RGPD si è concretizzata anche attraverso una specifica campagna di comunicazione istituzionale legata al progetto formativo internazionale T4DATA, finanziato con i fondi del *Rights, Equality and Citizenship Programme* dell'UE (2014-2020), rivolto ai Rpd pubblici nei vari Paesi UE (Bulgaria, Croazia, Italia, Polonia e Spagna). Entro la medesima cornice va inscritto anche il progetto formativo internazionale SMEDATA, dedicato alle Pmi e ai consulenti giuridici in ambito *privacy*, nato da una *partnership* tra il Garante e l'Autorità per la protezione dati della Bulgaria, al quale ha collaborato anche l'Università degli studi Roma Tre (par. 21.5).

I seminari

Come anticipato (par. 5.4.3 e 21.5), sono stati organizzati quattro seminari di formazione in quattro diverse città italiane da nord a sud (Torino, Ancona, Roma e Catanzaro), da giugno a novembre, con la partecipazione di oltre 1.300 Rpd operanti presso i soggetti pubblici. Ogni seminario è stato dedicato all'approfondimento di tematiche specifiche – trattamento dei dati personali per finalità di cura e ricerca; protezione dei dati personali e trasparenza della p.a. dopo il RGPD; gestione del rischio e sicurezza del trattamento; responsabilità del trattamento – per un totale di circa 30 ore di formazione, con interventi di dirigenti e funzionari del Garante. In ogni incontro è stato riservato ampio spazio alle risposte ai quesiti posti dai partecipanti.

Contemporaneamente agli eventi sul territorio, nel mese di ottobre è stata lanciata anche una piattaforma *online* con più di 30 *webinar* gratuiti di approfondimento su varie tematiche rivolta alla vasta platea dei Rpd operanti presso i soggetti pubblici; l'Ufficio ha curato l'ideazione progettuale dei seminari e la produzione di tutti gli elementi grafici di supporto, promuovendo gli eventi sui canali *social* istituzionali. Sulla piattaforma sono stati messi a disposizione numerosi materiali di approfondimento, come le *slide* presentate nel corso dei convegni, questionari di auto-valutazione per chi segue i *webinar* e un dettagliato manuale per i Rpd in lingua italiana e inglese.

La rete dei comunicatori del Comitato

È stata inoltre sviluppata una collaborazione sistematica con il gruppo di comunicazione del Cepd per realizzare attività coordinate di comunicazione in merito all'azione delle Autorità di garanzia europee e dello stesso Comitato. L'Ufficio ha

23

GPEN e *Privacy Sweep*

collaborato alla stesura di 7 comunicati stampa congiunti con il Cepd e le altre autorità europee nell'ambito del Gruppo di comunicazione europeo nonché di altrettante attività di comunicazione sui *social* per il rilancio di attività comuni. Ha partecipato alla definizione dei messaggi chiave europei per il primo anno di applicazione del RGPD e ha contribuito con propri rappresentanti ai lavori del *Communication network meeting* che si è tenuto a Vienna.

Come anticipato (par. 21.3), il 23 settembre è stato lanciato il *Privacy Sweep* 2019, l'indagine a carattere internazionale dedicata quest'anno alla gestione dei *data breach* da parte di soggetti pubblici e privati. Lo *Sweep* (indagine a tappeto) fa seguito ad analoghe indagini effettuate negli scorsi anni che hanno preso in esame il principio di responsabilizzazione (*accountability*), le informative *privacy* su siti web e le *app* per la telefonia mobile, i servizi *online* destinati a minori, l'internet delle cose. Le autorità di protezione dei dati partecipanti all'indagine hanno analizzato i processi e le procedure adottati per la gestione delle violazioni dei dati personali dai titolari dei trattamenti che operano sui rispettivi territori nazionali. L'iniziativa è coordinata dalla *Global privacy enforcement network* (GPEN), la rete internazionale nata per rafforzare la cooperazione tra le Autorità della *privacy* di diversi Paesi, di cui il Garante fa parte. Allo *Sweep* 2019 hanno partecipato, oltre a quella italiana, 17 autorità di protezione dei dati di vari Paesi del mondo. Il Garante ha concentrato la sua attività sul settore dell'*e-commerce* attraverso l'analisi di un campione di imprese italiane.

L'attività del Garante ha trovato largo spazio e attenzione sui *media*. Il Servizio relazioni con i mezzi di informazione ha selezionato oltre 67.950 articoli nazionali di interesse dell'Autorità e circa 2.370 articoli provenienti da testate e siti web esteri. Sulla base della rassegna stampa elaborata quotidianamente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali e dei *media online* che hanno trattato i temi legati alla *privacy* sono state 8.300, delle quali 6.470 dedicate esclusivamente all'attività del Garante. Le interviste, gli interventi e le dichiarazioni del Presidente e dei Componenti dell'Autorità pubblicate e riprese sulla carta stampata e web sono state complessivamente 716; andate in onda su tv e radio nazionali e locali 52; si contano infine 360 articoli relativi ai comunicati stampa e 515 riguardanti gli argomenti trattati dalle *Newsletter*.

23.2. *I prodotti informativi*

Nel corso del 2019 sono stati diffusi 55 comunicati stampa, 12 *Newsletter* e sono state trasmesse 22 puntate di una rubrica radiofonica su Radio Radicale.

La *Newsletter* del Garante è una pubblicazione periodica, giunta al XXI anno di diffusione (per un totale di 460 numeri e di 1.575 notizie). Nata in forma cartacea, oggi è inviata esclusivamente via *e-mail* a redazioni, professionisti, amministrazioni pubbliche, imprese e singoli cittadini che ne fanno esplicita richiesta o si iscrivono autonomamente *online* attraverso la funzione "Iscriviti alla *Newsletter*", attiva sul sito istituzionale. Al 31 dicembre la lista di distribuzione contava oltre 13.000 destinatari effettivi. La *Newsletter* è un valido strumento funzionale alla divulgazione dei più importanti provvedimenti adottati dall'Autorità, alla sua attività in ambito sia nazionale che europeo ed internazionale, ed alle molteplici iniziative legate alla protezione dei dati personali e alla tutela dei diritti fondamentali, fornendo un vasto panorama di questioni e problematiche. Tra i numerosi provvedimenti adottati dal Garante viene operata una scelta tra quelli di maggiore interesse pubblico che vengono rielaborati in chiave giornalistica. Generalmente ogni *Newsletter* è composta

23

da 3-4 notizie che, in vista della pubblicazione sul sito dell'Autorità, sono composte graficamente e completate con l'aggiunta di immagini allo scopo di offrire un prodotto più sofisticato e adatto al web. Sul sito è sempre possibile consultare l'archivio tematico che raccoglie per categorie i 21 anni di articoli prodotti dalla redazione. Sul sito è altresì consultabile l'archivio dei comunicati stampa divulgati.

Nell'attività di divulgazione vanno ricordate le 22 puntate della rubrica "Il Bollettino del Garante della *Privacy*", in onda su Radio Radicale: un contributo informativo tenuto dal Responsabile del Servizio relazioni esterne e media dell'Autorità, che illustra i principali provvedimenti adottati dal Garante e, più in generale, le tematiche legate alla protezione dei dati personali. Nel 2019 i temi trattati hanno riguardato, tra gli altri, gli adempimenti introdotti dal RGPD e la nuova figura del Rpd; lo *spam* e il *marketing* telefonico indesiderato; il controllo dei lavoratori; le piattaforme digitali; il diritto all'oblio; la sanità dopo il RGPD; la propaganda elettorale; il *food delivery*; i sistemi di informazione creditizia.

23.3. *Il sito istituzionale, i prodotti multimediali e le pubblicazioni*

Nuovi prodotti editoriali e multimediali si sono aggiunti alla già ricca collezione dell'Autorità.

Nell'ambito della Collana editoriale del Garante, "Contributi", è stato pubblicato il volume "I confini del digitale: Nuovi scenari per la protezione dei dati", che raccoglie i contributi degli studiosi e degli esperti intervenuti al Convegno organizzato dall'Autorità in occasione della celebrazione della XIII Giornata europea per la protezione dei dati personali 2019.

A luglio sono state pubblicate due edizioni del nuovo codice "Il diritto alla protezione dei dati personali. Normativa essenziale": una prima versione in italiano appositamente realizzata per il progetto formativo T4DATA, ed una seconda italiano/inglese.

A ottobre è stato curato e realizzato il volume "Applicare il GDPR. Le linee guida europee": una pubblicazione ragionata, organizzata in un volume unico, pensata per un pubblico specializzato e per esperti del settore. Per la realizzazione del volume è stato svolto un lavoro approfondito di analisi delle linee guida del Cepd in italiano, approvate in via definitiva nel primo anno di attività, mantenendo la coerenza con le versioni originali. Si è provveduto a: definire una linea grafica comune rispetto a documenti estremamente diversi tra di loro, curando internamente l'impaginazione dei testi; seguire la stampa; realizzare la progettazione grafica della copertina.

Nell'anno è stato ulteriormente incrementato il numero di prodotti grafici e multimediali da destinare alla diffusione sul web e sui canali *social* istituzionali del Garante su Linkedin, YouTube, Telegram e Instagram. In particolare, è stata avviata la sperimentazione di *stories* per Instagram (anche attraverso l'impiego di specifici *tool*) e di video brevi destinati soprattutto alla diffusione virale su Instagram, Telegram e Igtv. Tutti i prodotti multimediali sono stati realizzati con un bassissimo costo e utilizzando esclusivamente personale del Servizio relazioni esterne e media, che ne ha curato tutte le fasi della creazione (scrittura e adattamento testi, progetto grafico, impaginazione, sceneggiatura, sviluppo animazione e selezione/costruzione degli elementi visivi, scelta delle musiche e sincronizzazione, registrazione dei testi, adattamento audio, montaggio e post-produzione). I profili dell'Autorità sui *social network* sono stati costantemente implementati con nuovi contenuti. Complessivamente i tre profili aperti hanno raggiunto circa 34.800 *follower*. Il profilo del Garante sul servizio di messaggistica Telegram conta 1.940 *follower*.

Nel quadro di un più vasto progetto dedicato all'informazione nel campo dell'Internet delle cose (IoT) – in riferimento alle tematiche della *data protection* – è stata ideata e realizzata una campagna informativa destinata a sviluppare l'uso consapevole della rete.

Con l'intento di migliorarne la funzionalità e per rispondere ai cambiamenti introdotti dal decreto legislativo 10 agosto 2018, n. 101, si è provveduto alla riorganizzazione dell'architettura dell'informazione e dei contenuti del sito. Gli aggiornamenti hanno riguardato circa 90 tra pagine e sezioni informative, che sono state aggiornate o create *ex novo* (in numero di 24).

Le sezioni dedicate ai Temi (www.garanteprivacy.it/temi) e alle FAQ (www.garanteprivacy.it/FAQ) sono state totalmente riorganizzate nell'architettura dell'informazione e nella presentazione per aumentare la fruibilità e l'interconnessione tra i contenuti ed arricchite con numerose nuove schede infografiche e pagine di testo; tra le tante se ne segnalano alcune di maggior interesse sociale quali: Brexit; Videosorveglianza; *Spam*; Scuola; *Smartphone* e *tablet*; Foto e immagini *online*; *Social network*; Diritto all'oblio; *Cybersecurity*; *IoT* (*Internet of Things*), Domotica (*Smart Home*); *Smart toys*; *Smart cars*; AI (Intelligenza artificiale).

Le schede infografiche e le pagine informative del Garante si sono confermate anche nel 2019 il canale comunicativo privilegiato per veicolare informazioni e concetti normativi soprattutto attraverso il web ed i canali *social*. Sono tutti prodotti divulgativi con contenuti caratterizzati da chiarezza e sinteticità espressiva, grafica innovativa e forte vocazione *social*. Per tutti, il progetto è nato dall'ideazione di una strategia di viralizzazione sui *social media*, funzionale anche a sfruttare le potenzialità della cosiddetta "coda lunga" del web, che appaiono particolarmente utili a supportare le necessità comunicative del Garante e le esigenze informative dell'utenza.

È stata intensificata l'attività divulgativa sul RGPD nell'anno della sua prima ed integrale applicazione. Le campagne di informazione hanno avuto come principale obiettivo quello di offrire indicazioni operative per l'attuazione corretta delle norme, offerte in particolare dalle linee guida del Comitato. Sul sito web istituzionale la sezione Regolamento (www.garanteprivacy.it/regolamentoue) è stata oggetto di numerosi interventi. Le pagine tematiche disponibili nella sezione sono state oggetto di *restyling*, sia per aumentare l'*appeal* e l'usabilità, sia per adeguarle a criteri *mobile responsive*.

Il sistema Thesaurus del sito web del Garante è stato ampiamente e completamente aggiornato per rispondere ai cambiamenti introdotti dalle innovazioni normative rispetto al RGPD e al Codice aggiornato al d.lgs. n. 101/2018 e dare attuazione alla pubblicazione di atti e documenti previsti dalla disciplina sulla trasparenza. L'arricchimento dei *tag* utilizzati per classificare i documenti ne facilita notevolmente la ricerca (strumenti di *semantic* web).

23.4. *Le manifestazioni e le conferenze*

Il 28 gennaio di ogni anno ricorre la Giornata europea della protezione dei dati personali. Promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le autorità europee per la *privacy* viene celebrata dal 2006 per ricordare in tutta Europa l'adozione della Convenzione di Strasburgo n. 108/1981 ed ha come obiettivo quello di sensibilizzare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali.

Per celebrare la XIII Giornata europea, la prima dopo l'entrata in vigore del RGPD, il Garante ha organizzato un convegno intitolato: "I confini del digitale.

23

Nuovi scenari per la protezione dei dati", che si è svolto a Roma, nell'Aula del Palazzo dei Gruppi Parlamentari. È stata l'occasione per affrontare una serie di temi particolarmente rilevanti nella società attuale e futura: l'impatto delle tecnologie digitali sulle libertà degli individui e sugli stessi modelli di democrazia; il confronto tra Europa e Cina sul concetto di sovranità digitale; le nuove forme di controllo sociale realizzate attraverso le applicazioni dell'intelligenza artificiale e dell'Internet delle cose; le frontiere cibernetiche verso cui si stanno spostando i conflitti tra Stati; il ruolo che in questi nuovi scenari può giocare la protezione dei dati personali.

I lavori sono stati aperti da Antonello Soro, presidente dell'Autorità, e chiusi dall'allora Ministro per la pubblica amministrazione, Giulia Bongiorno. Al convegno articolato in tre sessioni – moderate dalle Componenti dell'Autorità Garante, Augusta Iannini, Licia Califano, Giovanna Bianchi Clerici – hanno preso parte autorevoli relatori quali: Erica Palmerini, docente della Scuola Superiore Sant'Anna di Pisa; Francesco Radicioni, giornalista di Radio Radicale; Stefano Mele, avvocato specializzato in diritto delle tecnologie, *privacy* e *cybersecurity*; Roberto Baldoni, vice Direttore Generale del Dis; Giuliano Amato, giudice costituzionale; Maurizio Molinari, Direttore de "La Stampa".

Il presidente Soro, nel suo intervento, ha rappresentato le sfide presenti e quelle future della "rivoluzione digitale" non nascondendo forti preoccupazioni e lanciando un invito a tenere sempre più alto il livello di attenzione sulla questione della protezione dei dati, cruciale per la stessa tenuta della democrazia nel mondo digitale. "Viviamo in un tempo nel quale la tecnologia digitale concorre alla definizione di criteri valoriali e orienta sempre più le decisioni private e pubbliche". Se prive di regole, è stato l'allarme lanciato da Soro, "le nuove tecnologie possono alimentare un regime della sorveglianza tale da rendere l'uomo una non-persona, l'individuo da addestrare o classificare, normalizzare o escludere". "Quella cibernetica – ha concluso Soro – è la frontiera su cui si sta spostando in misura sempre più invasiva la dinamica delle conflittualità tra Stati e soggetti. Ancora una volta, contro ogni rischio di espropriazione del diritto da parte della tecnica, è proprio questa proiezione, nella dimensione digitale, dello Stato e della sua stessa sovranità a dimostrare come la protezione dei dati possa divenire presupposto di sicurezza, promuovendo quella resilienza indispensabile per la difesa della democrazia nel rispetto della sua identità e con mezzi democratici".

Ad ascoltare il dibattito sono stati invitati, tra gli altri, anche gli studenti della IV classe del Liceo classico "Tacito" di Roma. Gli interventi di tutti i relatori sono stati raccolti nel volume "I confini del digitale. Nuovi scenari per la protezione dei dati".

Il 4 marzo, organizzata dal Dipartimento di Scienze giuridiche dall'Università di Firenze, il presidente Soro ha tenuto una *lectio magistralis* dal titolo "Dalla *privacy* alla protezione dei dati nella società digitale" affrontando temi quali: il bilanciamento necessario tra il diritto alla *privacy* e il diritto alla sicurezza; i rischi per le libertà personali connessi con la profilazione degli utenti; le pressioni delle *lobby* delle grandi piattaforme digitali alla vigilia dell'approvazione del RGPD; le norme UE sulla protezione dei dati e le difficoltà per le piccole e medie imprese ad adeguarsi al RGPD. Quanto al conflitto sempre più evidente tra le esigenze della *privacy* e quelle della sicurezza, Soro ha tracciato un percorso che dovrà tenere nella massima considerazione entrambi i fattori: "Non ci può essere un diritto alla sicurezza che prevale rispetto alla protezione del dato, vanno bilanciati: diversamente – ha affermato – arretriamo verso uno Stato illiberale rispetto al quale saremo sempre più indifesi".

Sullo stesso tema anche il seminario "Piattaforme digitali, libertà fondamentali e rischi per la democrazia" organizzato dall'Università di Chieti il 14 maggio, che ha

visto la partecipazione del presidente Soro.

Il 25 giugno all'Università Bocconi di Milano si è tenuto il convegno "*Privacy Data protection, Technology, Cybersecurity* - Il complesso rapporto tra diritto e tecnologia", al quale è intervenuta Augusta Iannini, vice presidente dell'Autorità, che si è soffermata sulle problematiche legali connesse all'incessante sviluppo delle tecnologie e alla necessità di tenere conto, fin dalla fase di progettazione, anche degli aspetti legati alla protezione dati.

In merito al nuovo Regolamento è stata messa in campo una diffusa azione di informazione pubblica volta ad illustrare le nuove disposizioni e a chiarire le procedure da seguire e numerosi sono stati gli incontri e i dibattiti a cui hanno partecipato i componenti del Collegio, il Segretario generale e i dirigenti dell'Autorità. Vari gli aspetti trattati: etica ed efficacia delle nuove disposizioni europee; il diritto all'oblio e il diritto all'informazione; il diritto alla portabilità dei dati; il principio di responsabilizzazione; la sfida culturale della tutela dei dati dopo il RGPD; un bilancio del primo anno di applicazione del nuovo Regolamento europeo.

Giovanna Bianchi Clerici ha partecipato, il 2 aprile, al convegno organizzato da Fapav, Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali e dalla Luiss *Business School*, "Il prezzo della gratuità: Pirateria e rischi informatici". La Componente dell'Autorità ha rappresentato come la facilità di accesso ai contenuti multimediali offerta dalle nuove tecnologie di *streaming*, *download*, Iptv riduce l'attenzione dell'utente alle tracce che in questo modo lascia in rete; la relatrice ha evidenziato come le regole già in vigore sarebbero effettivamente sufficienti ad arginare fenomeni di furto e perdita dei dati personali e ciò che manca sia piuttosto la piena consapevolezza degli utenti stessi sui rischi cui si espongono accedendo a prodotti e servizi pirata. Bianchi Clerici ha partecipato inoltre, il 13 giugno, al convegno su "Ricerca e selezione del personale secondo il GDPR e il diritto del lavoro: i *background checks*", soffermandosi sulla più recente casistica, dalla quale è emersa la richiesta al Garante di operare un delicato bilanciamento tra il legittimo interesse delle aziende e il diritto alla riservatezza dei lavoratori.

Di "Diritto alla trasparenza degli algoritmi e alla tutela dei dati" si è parlato invece alla XIV edizione dell'annuale appuntamento con le *Authority* italiane organizzato da *Consumer's Forum*, l'associazione indipendente composta dalle più importanti associazioni di consumatori, istituzioni, imprese industriali ed associazioni di categoria (21 novembre a Roma). Il tema di fondo su cui si è dibattuto è stato quello del controllo e della conoscenza di ciò che la rivoluzione digitale sta provocando sulla vita e sui diritti dei cittadini. Il segretario generale Busia nel suo intervento ha ribadito che "la protezione dei dati rappresenta oggi il diritto senza il quale anche tutti gli altri diritti vengono meno. Solo garantendo a cittadini e consumatori che le loro informazioni personali siano usate in modo trasparente, per fini specifici e previo il loro consenso, possiamo riuscire a tutelare anche la loro libera scelta e difenderli dagli abusi". Tanto più nella dimensione digitale questo è vero, ha sottolineato Busia, per il quale "l'evoluzione vorticosa della tecnologia, la concentrazione di enormi quantità di dati nelle mani di pochi, i sistemi sempre più sofisticati e invasivi di raccolta e profilazione dei consumatori sulla base di gusti, abitudini, opinioni, delineano uno scenario nel quale è imprescindibile la crescita ed il rafforzamento di una effettiva cultura della protezione dati".

Il 7 maggio alla presenza dei Presidenti della Camera e del Senato, on. Roberto Fico e sen. Maria Elisabetta Alberti Casellati, di Ministri, rappresentanti del Parlamento, delle Istituzioni, del mondo dell'impresa e delle associazioni di categoria si è svolta la cerimonia di presentazione della Relazione annuale per l'anno 2018 facendo il punto sullo stato di attuazione della legislazione in materia di protezione

23

dei dati alla luce del nuovo Regolamento ed indicato gli scenari futuri. L'intero evento è stato trasmesso in diretta TV ed in *streaming* sul sito web istituzionale.

23.5. *L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi*

Tramite l'Ufficio relazioni con il pubblico l'Autorità ha continuato a fornire assistenza al pubblico – sia ai visitatori in sede, che a distanza mediante il canale telefonico o gestendo le numerosissime richieste pervenute via *e-mail* (cfr. parte IV, tab. 12) – promuovendo la consapevolezza sulle tematiche afferenti alla protezione dei dati personali.

In aggiunta a tali attività "correnti", al fine di svolgere una sempre più efficace azione di supporto e divulgazione al pubblico, l'Urp ha altresì predisposto, tenendo conto delle questioni di maggiore interesse per gli utenti e con la collaborazione del Dipartimento interessato, alcune FAQ relative ai trattamenti di dati personali in ambito scolastico e alla fatturazione elettronica e curato l'aggiornamento delle FAQ relative alla procedura telematica per la comunicazione dei dati del Responsabile per la protezione dei dati, fornendo poi assistenza a titolari, responsabili del trattamento e Rpd.

Nella maggior parte dei casi, le numerose richieste pervenute hanno avuto ad oggetto gli adempimenti e, in generale, il nuovo approccio previsto dal RGPD (*accountability* e *privacy by design* e *by default*). Ancorché il numero delle *e-mail* sia diminuito rispetto ai picchi raggiunti a ridosso del 25 maggio 2018, anche grazie ai chiarimenti progressivamente forniti dall'Autorità, il numero dei contatti dell'Ufficio permane comunque elevato, con un totale di quasi 16.000 richieste ricevute, delle quali circa 10.900 pervenute via *e-mail*; 233 sono stati poi gli affari definiti e 290 i visitatori ricevuti in sede.

L'Ufficio ha gestito la mole di contatti sopra ricordata avendo cura di mantenere sempre elevati i propri standard di efficienza e professionalità, garantendo al tempo stesso approfondita e aggiornata conoscenza giuridica delle questioni esaminate, cortesia e tempestività nella risposta. Il contatto diretto e costante con l'utenza tramite l'Urp ha consentito peraltro di cogliere con tempestività le problematiche più rilevanti e trasferirle mediante *report* interni alle altre unità organizzative come pure di sottoporre con urgenza alle unità competenti le vicende più delicate.

Tematiche d'interesse

Tra le tematiche di maggiore interesse di carattere generale si segnalano, anche per il 2019, gli adempimenti introdotti dal RGPD (oltre 1.900 *e-mail* ricevute). L'attenzione dei titolari del trattamento si è concentrata su particolari contesti (come quello del *marketing*) e su taluni adempimenti, tra questi la necessità di inserire nell'informativa da rendere agli interessati l'indicazione del periodo di conservazione dei dati personali o, ove ciò non sia possibile, dei criteri utilizzati per determinarlo; aspetto quest'ultimo in relazione al quale si sono non di rado rappresentate le difficoltà incontrate nello stabilire *ex ante* la durata del trattamento e, quindi, i tempi di conservazione dei dati.

Anche la designazione del Rpd e la procedura *online* realizzata dal Garante per la comunicazione dei dati di contatto dello stesso sono state oggetto di ricorrenti richieste di assistenza all'Ufficio, intensificatesi dopo il mese di maggio, quando numerosi incarichi sono giunti a scadenza e molti Rpd hanno contattato l'Autorità per verificare se e quali nomine fossero ancora attive nei loro confronti presso l'Autorità.

Numerosissimi i quesiti concernenti l'individuazione dei casi nei quali sorge la necessità di effettuare una valutazione d'impatto sulla protezione dei dati o anche la

successiva consultazione preventiva del Garante (artt. 35 e 36).

Un gran numero di richieste ha avuto ad oggetto la perdurante validità delle pronunce e dei provvedimenti dell'Autorità adottati anteriormente al 25 maggio 2018 (quali, a mero titolo esemplificativo, il provvedimento in materia di amministratori di sistema del 2008, quello in materia di videosorveglianza del 2010 o, infine, quello del 2005 relativo alle *fidelity card* e alla *data retention* nell'ambito della profilazione della clientela). Al riguardo l'Ufficio, alla luce della previsione di cui all'art. 22, comma 4, d.lgs. n. 101/2018, ha confermato che è necessario effettuare, di volta in volta e in relazione alle diverse previsioni contenute nei suindicati provvedimenti, una verifica della compatibilità delle stesse con il RGPD e con il Codice, come aggiornato dallo stesso decreto legislativo n. 101/2018.

Anche il rapporto tra titolari e responsabili del trattamento di cui all'art. 28 del RGPD è stato al centro dell'interesse degli utenti, con particolare riferimento alla definizione del ruolo, delle competenze e delle responsabilità da attribuire ad alcune specifiche figure, quali ad esempio quella del medico competente in ambito lavorativo.

Si registra ancora una grande attenzione dei cittadini nei confronti dei trattamenti di dati personali effettuati per finalità di *marketing* (circa 1.400 *e-mail* ricevute) e, in particolare, nei confronti del *telemarketing*, persistente fonte di grande fastidio per gli utenti.

Richieste di chiarimento hanno riguardato anche i nuovi adempimenti concernenti la fatturazione elettronica, con particolare riferimento ai soggetti che erogano prestazioni sanitarie. I trattamenti di dati personali svolti da tali soggetti, unitamente ad altre questioni pure più volte evidenziate dall'utenza, sono stati al centro di apposite FAQ predisposte dall'Ufficio, disponibili al *link* https://www.gpdp.it/home/FAQ/fatturazione-elettronica.

Analogamente, sono state predisposte alcune FAQ (https://www.gpdp.it/home/FAQ/scuola-e-privacy) relative alle questioni afferenti ai trattamenti di dati personali effettuati nell'ambito delle istituzioni scolastiche, anch'esse oggetto di molte richieste da parte dell'utenza (100 *e-mail*). L'accesso alla documentazione relativa ad alunni e studenti in possesso della scuola, il trattamento dei dati personali degli allievi disabili o con disturbi specifici dell'apprendimento, il trattamento dei dati nell'ambito delle comunicazioni scuola-famiglia e l'utilizzo degli *smartphone* all'interno delle scuole sono soltanto alcuni dei temi affrontati dall'Ufficio.

Grande attenzione si registra anche nei confronti dei trattamenti in ambito bancario (oltre 470 *e-mail*) e delle centrali rischi (oltre 420 *e-mail*).

Elevato è stato il numero delle richieste relative al tema della videosorveglianza sia in ambito privato sia in ambito pubblico (circa 500 *e-mail*), con particolare riguardo ai settori scolastico, socio-sanitario e lavorativo.

Oltre alle problematiche poste dalla videosorveglianza, nel contesto lavorativo si registrano molte richieste di chiarimento che hanno riguardato anche quest'anno l'uso di internet e della posta elettronica da parte dei dipendenti, il trattamento effettuato sulle *e-mail* dei soggetti che abbiano cessato il rapporto di lavoro e l'uso di sistemi di rilevazione biometrica sul posto di lavoro (427 *e-mail*).

Numerose sono state anche le istanze volte ad ottenere chiarimenti e assistenza in merito alla notificazione al Garante dei *data breach* mediante la modulistica e la nuova procedura messa a punto sul sito a seguito del provv. 30 luglio 2019, n. 157 (doc. web n. 9126951), come pure in relazione alle questioni concernenti le sanzioni irrogate dal Garante, con particolare riguardo alle cartelle esattoriali ricevute da molti titolari del trattamento a seguito della mancata adesione, anche in tempi non recenti, alla procedura di definizione agevolata (cfr. par. 19.3).

23

Si segnala, da ultimo, il costante interesse mostrato nei riguardi delle questioni concernenti i trattamenti di dati personali in internet e nei *social network*, nonché in ambito giornalistico (circa 900 *e-mail*), in modo particolare con riferimento alle richieste di deindicizzazione dei dati personali dai motori di ricerca al fine di esercitare il cd. diritto all'oblio di cui all'art. 17 del RGPD.

24 Studi e documentazione

Relazione annuale

Il Servizio studi e documentazione ha coordinato la predisposizione del testo della Relazione annuale allo scopo di dare attuazione ad un importante adempimento che la legge pone in capo al Garante, ovvero quello di dare conto dell'attività svolta al Parlamento e al Governo (cfr. art. 154, comma 1, lett. *e*), del Codice nonché l'art. 59 del RGPD). La pubblicazione del testo della Relazione sul sito istituzionale del Garante consente altresì di perseguire una più ampia finalità di trasparenza sull'attività svolta dall'Autorità non soltanto rispetto ai soggetti destinatari *ex lege* della stessa, ma anche nei confronti dell'intera collettività, rappresentando in pari tempo un prezioso strumento di conoscenza per diverse categorie di utenti a vario titolo interessati all'applicazione della disciplina in materia di protezione dei dati personali. In questa prospettiva, la struttura della Relazione, che presenta tradizionalmente una parte generale e molteplici sezioni tematiche (ivi comprese quelle contenenti informazioni di natura statistica), agevola la consultazione, in modo rapido e sintetico, 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.

A ciò si aggiunga che, come è noto, in conformità a quanto previsto dall'art. 22, d.l. n. 90/2014 convertito in l. 11 agosto 2014, n. 114, la Relazione annuale del Garante (non diversamente da quella delle altre autorità amministrative indipendenti) viene altresì trasmessa alla Corte dei conti (attività che con regolarità è stata assolta dal 2014) nonché messa a disposizione del pubblico, della Commissione europea e del Comitato (art. 59 del RGPD).

Attività di studio, documentazione e supporto giuridico

Studi e ricerche sono state condotte su molteplici questioni tecnico-giuridiche di attualità nonché su materie di interesse dell'Autorità, dando particolare rilievo alle tematiche del procedimento amministrativo e sanzionatorio in considerazione della complessiva rivisitazione dei regolamenti interni nn. 1 e 2 dell'Autorità. L'attività di documentazione viene svolta mediante la predisposizione di un osservatorio ad uso interno (nell'anno di riferimento di cadenza mensile) prodotto del costante monitoraggio della giurisprudenza, dottrina e documentazione nazionale, comunitaria ed internazionale, in particolare in materia di protezione dati, nonché mediante approfondimenti su questioni o settori specifici: in tale prospettiva hanno formato oggetto di esame (anche in prospettiva applicativa), la tematica del *Big data*, l'istituto dell'accesso civico generalizzato e le figure del titolare, contitolare e responsabile del trattamento.

PAGINA BIANCA

L'Ufficio del Garante

PAGINA BIANCA

III - L'Ufficio del Garante

25 La gestione amministrativa e dei sistemi informatici

25.1. *Il bilancio e la gestione economico-finanziaria*

La gestione amministrativa del Garante è stata improntata ad una prudente valutazione delle entrate ed all'osservanza di generali principi di attenta programmazione della spesa. L'Autorità ha osservato le procedure ed i vincoli contenuti in disposizioni legislative e regolamentari, avendo cura di contemperare le ineludibili esigenze di oculatezza nell'amministrazione delle risorse pubbliche con gli obblighi derivanti dal perseguimento delle finalità istituzionali.

Le nuove disposizioni recate dal RGPD e dal successivo decreto legislativo di modifica ed integrazione del Codice hanno trovato applicazione a decorrere dall'esercizio 2019 e tale arco temporale è stato caratterizzato anche dalla piena attuazione del completamento del percorso di revisione del finanziamento dell'Autorità, correlato alla piena applicazione della nuova disciplina europea in materia di protezione dei dati personali.

Rispetto al 2018, il finanziamento complessivo erogato al Garante nell'anno ha fatto registrare un incremento derivante dalle misure già adottate dal Parlamento con la legge n. 205/2017; il relativo stanziamento aggiuntivo, infatti, era stato preordinato proprio allo svolgimento degli adempimenti istituzionali previsti dalle richiamate misure dell'Unione europea.

La gestione amministrativa del Garante ha risentito degli inevitabili riflessi che decisioni dell'autorità governativa e dello stesso Parlamento hanno prodotto in relazione alle funzioni da esercitare. Nel corso dell'anno, infatti, in occasione della naturale scadenza degli organi di vertice, si sono succeduti più provvedimenti legislativi, a partire dal decreto-legge 7 agosto 2019, n. 75, con i quali il Garante è stato autorizzato a continuare ad attendere alle proprie funzioni entro i limiti degli atti di ordinaria amministrazione e di quelli indifferibili e urgenti.

La situazione che si è determinata, se da un lato ha consentito l'operatività dell'Autorità, ne ha tuttavia limitato le potenzialità in termini di programmazione della spesa, sia in termini temporali che per le funzioni da esercitare. In tale contesto, caratterizzato da successive proroghe delle funzioni per periodi limitati, anche il procedimento di spesa è stato preordinato ad assicurare soltanto adempimenti gestionali di ordinaria attività e quelli configurabili come indifferibili ed urgenti.

L'Autorità ha continuato a porre in essere tutti gli opportuni adempimenti per gestire i propri servizi con criteri di economicità, in considerazione delle specifiche esigenze connesse alle attività istituzionali e nel rispetto delle vigenti disposizioni. Nello svolgimento delle ordinarie attività gestionali è stata ottimizzata la sistema-

25

zione dei locali, sia per una più funzionale distribuzione degli spazi, sia per assicurare la disponibilità di postazioni di lavoro aggiuntive da destinare al personale assunto nell'ambito del programma di potenziamento connesso alle maggiori competenze derivanti dalla nuova disciplina in materia di protezione dei dati personali. La sede degli uffici è condotta in locazione e l'Autorità non detiene immobili adibiti ad abitazione o foresteria.

Nel corso dell'esercizio il Garante non ha conferito incarichi di studio e di consulenza, secondo una politica gestionale ormai consolidata di propendere per una valorizzazione delle risorse interne.

La gestione amministrativa è stata assoggettata agli ordinari e periodici controlli dell'organo preposto alla verifica della regolarità amministrativo-contabile e nel corso delle verifiche effettuate nell'esercizio 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 importante avanzo di amministrazione, pari a oltre 4,9 milioni di euro. Tale risultato è stato determinato da una dinamica della spesa più contenuta rispetto a quanto ipotizzato in sede di previsione, anche per una politica gestionale tendenzialmente volta a valorizzare la salvaguardia delle risorse erariali.

In tale contesto l'Autorità ha comunque disposto l'assunzione di un numero di funzionari adeguato alle esigenze dell'Ufficio, anche per attendere alle maggiori incombenze istituzionali.

Nel 2019, al netto delle partite di giro, le entrate complessivamente acquisite dall'Autorità sono state di 29,5 milioni di euro a fronte delle quali sono stati registrati impegni di spesa per 24,6 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 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 2019 è stato di 2,6 milioni di euro, con una variazione di poco inferiore al 10 per cento.

Con riferimento alla spesa, invece, gli oneri complessivi registrati nell'anno, pari a 24,6 milioni di euro, risultano in crescita di 1,2 milioni di euro rispetto alla spesa complessiva del precedente anno 2018, corrispondente ad una variazione di circa il 5 per cento. Tale incremento è da ricondurre in via generale a maggiori oneri per il personale, determinati anche dalle nuove immissione in ruolo nel corso dell'anno.

La spesa complessiva è da imputare in massima parte alla gestione corrente, nella misura di 24,2 milioni di euro, mentre la parte residuale di 0,4 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 2019 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. Va doverosamente evidenziato, tuttavia, che puntuali disposizioni legislative prevedono che la retribuzione del personale del Garante debba essere commisurata alla misura dell'ottanta per cento, e quindi in misura più contenuta, rispetto a quanto riconosciuto al personale di altre autorità amministrative indipendenti.

L'indennità di carica riconosciuta al Presidente ed ai componenti del Collegio del Garante non ha subito variazioni rispetto al precedente esercizio ed il loro importo è rimasto entro i prescritti limiti di legge.

Con riferimento, infine, agli oneri strettamente connessi alle esigenze gestionali, nel corso dell'anno risultano in generale rispettati i prescritti limiti di legge.

Si rinvia alla tab. 15 nella sez. IV 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.

25.2. *L'attività contrattuale, la logistica e la manutenzione dell'immobile*

Come è noto, l'entrata in vigore del decreto-legge 18 aprile 2019, n. 32 (cd. decreto sblocca-cantieri), convertito con modificazioni dalla legge n. 55/2019, ha introdotto ulteriori significative modifiche al codice dei contratti pubblici, talune delle quali aventi immediata applicazione, mentre altre avranno efficacia soltanto dopo l'approvazione di ulteriori atti, tra i quali si segnala il regolamento unico di attuazione del codice, in sostituzione delle linee guida dell'Anac. L'Autorità si è prontamente conformata alle sopravvenute disposizioni, adeguando le relative procedure, finalizzate a perseguire, oltre che la costante legittimità delle stesse, anche obiettivi di ulteriore razionalizzazione e contenimento della spesa.

Proseguendo nell'attuazione dei processi di ottimizzazione delle attività di acquisizione di beni e servizi – come disciplinate dall'art. 22, comma 7, d.l. n. 90/2014 e s.m.i., riguardante la razionalizzazione delle autorità amministrative indipendenti – ed in considerazione del fatto che la programmazione degli acquisti effettuata nell'anno 2018 non prevedeva nel periodo in esame lo svolgimento di procedure di gara gestite in comune con altre autorità indipendenti, l'Ufficio ha partecipato alle riunioni organizzative comunque tenutesi tra tali autorità, volte a riepilogare le future esigenze di acquisizione e a coordinare le connesse attività, ponendo le basi per alcune procedure comuni da avviare nel 2020, con particolare riguardo al settore dei contratti assicurativi.

Nell'ambito delle attività realizzate in collaborazione con altre autorità amministrative indipendenti, svolta un'approfondita istruttoria di concerto con l'Anac, è stato istituito, con avviso pubblicato in data 7 maggio 2019, un elenco di avvocati del libero foro cui ricorrere per gli incarichi di patrocinio legale nell'interesse del Garante, nei limitati casi in cui lo stesso non possa essere rappresentato e difeso dall'Avvocatura dello Stato.

Consolidando un'attività ormai decennale di progressivo ricorso ai sistemi di *e-procurement*, l'attività in materia di appalti ha spaziato su ciascuno dei principali strumenti resi disponibili in tale direzione da Consip s.p.a. sul portale Acquistinretepa.it: convenzioni, Richieste di offerta (sia di tipo aperto che ad inviti), Trattative dirette, Ordini diretti d'acquisto nonché, per la prima volta, Sistema dinamico di acquisizione.

Iniziando da quest'ultimo, preso atto della perdurante indisponibilità della convenzione Consip "*Facility Management 4* - lotto n. 10" (relativo ad immobili siti nel I Municipio di Roma) – che già negli anni precedenti determinò la proroga del contratto al tempo in essere, risultante dall'adesione alla precedente edizione della medesima convenzione Consip – l'Ufficio ha completato una lunga ed onerosa istruttoria nell'ambito del Sistema dinamico di acquisizione della pubblica ammi-

nistrazione per la fornitura dei servizi di pulizia e igiene ambientale degli immobili, giungendo così nel mese di giugno ad avviare la relativa procedura di gara, che si prevede possa essere aggiudicata nel 2020.

Mediante lo strumento dell'adesione a contratto quadro, l'Autorità ha stipulato contratti esecutivi di fornitura di carburante per autotrazione e di gestione delle trasferte di lavoro; tramite convenzione, invece, sono stati acquisiti i servizi di telefonia (fissa e mobile) e di erogazione di energia elettrica, nonché taluni beni informatici.

Tramite Richiesta di offerta (Rdo) sono stati acquisiti beni e servizi diversificati, tra i quali si menzionano: fornitura triennale di toner per stampanti; supporto ad un *software* infrastrutturale; servizio di elaborazione delle competenze economiche del personale dell'Autorità. Nel corso dell'anno in esame è stata altresì esperita una Rdo riguardante i servizi di stampa delle pubblicazioni istituzionali del Garante, conclusa nel mese di gennaio 2020 con l'individuazione di un fornitore che gestirà il servizio per la durata di due anni.

Gli strumenti della Trattativa diretta e dell'Ordine diretto d'acquisto sono stati utilizzati per i residui affidamenti, in costanza dei relativi presupposti e, nella maggior parte dei casi, per importi inferiori a 10.000 euro. I relativi contratti hanno avuto ad oggetto le categorie merceologiche più disparate, tra le quali: manutenzione di macchine da ufficio, manutenzione piante da arredo, spedizione colli, abbonamenti a riviste giuridiche e a banche dati, servizi di traduzione, oltre alle più usuali come cancelleria, arredi, *hardware* e *software.* Riguardo a questi ultimi, con riferimento alle previsioni di cui alla legge di stabilità 2016 (art. 1, comma 512, l. 28 dicembre 2015, n. 208), si evidenzia che tutti gli acquisti di *hardware* e *software* sono stati effettuati utilizzando strumenti di acquisto e negoziazione del portale Consip.

Riguardo alle procedure gestite al di fuori degli strumenti di acquisto e negoziazione forniti dalla Consip, è stata avviata nel corso dell'anno una procedura aperta sotto soglia comunitaria per il servizio di monitoraggio delle attività delle Istituzioni nazionali; il relativo bando di gara è stato pubblicato all'inizio del 2020.

Inoltre l'Ufficio, avvalendosi della facoltà prevista in sede di gara, ha proceduto al rinnovo del contratto concernente la gestione del piano sanitario per il personale per la durata di un anno.

Per quanto attiene infine alla logistica e manutenzione dell'immobile, sono proseguite le attività di sistemazione della nuova sede, con riferimento agli ambiti di competenza, mediante assidua collaborazione con l'ufficio del consegnatario. Sono state effettuate attività di adeguamento funzionale e miglioramento dei locali e dei relativi arredi, di concerto con la società proprietaria dell'immobile e con il Responsabile del servizio prevenzione e protezione dell'Autorità, che ha costantemente coadiuvato l'Ufficio al fine di assicurare il rispetto della normativa sulla sicurezza nei luoghi di lavoro. È stata avviata la sistemazione dei locali adibiti ad archivio, che dovrebbe essere completata nei primi mesi dell'anno 2020.

25.3. *L'organizzazione dell'Ufficio*

Il personale

Al fine di supportare il nuovo assetto organizzativo, definito con provv. 22 febbraio 2018, n. 118 (doc. web n. 7896186), l'Autorità ha espletato nell'anno di riferimento una procedura selettiva, per titoli ed esami, finalizzata alla copertura di quattro posti di impiegato operativo, conclusasi con l'approvazione della graduatoria di merito e l'immissione dei vincitori nel ruolo organico del Garante già a partire da gennaio 2020. Sono proseguite le attività relative alle procedure selettive del

2019, per titoli ed esami, rispettivamente a n. 1 profilo dirigenziale in ambito giuridico-internazionale e n. 2 profili dirigenziali in ambito giuridico-amministrativo.

Sempre in tema di reclutamento del personale e per far fronte all'ampliamento dei compiti istituzionali dell'Autorità introdotti dal RGPD nonché dal d.lgs. n. 101/2018, è stato disposto l'utilizzo parziale di una graduatoria ancora in corso di validità presso l'Autorità, consentendo l'immissione in ruolo di n. 10 funzionari con profilo giuridico-amministrativo.

Diversamente, avuto riguardo alla Convenzione quadro in materia di procedure concorsuali congiunte per il reclutamento del personale delle autorità indipendenti siglata nel 2015, ai sensi dell'art. 22, comma 4, d.l. n. 90/2014, sono state bandite da altre autorità indipendenti procedure concorsuali alle quali tuttavia l'Autorità non ha aderito, in ragione della specificità dei profili richiesti.

Al 31 dicembre 2019 l'Ufficio poteva così contare su un organico di n. 162 unità, di cui 127 in servizio, al quale va aggiunto un contingente di n. 4 unità in servizio con contratto a tempo determinato (cfr. parte IV, tab. 14). Dai suddetti dati, si evidenzia che nell'anno considerato si è verificato un incremento di n. 6 unità di personale in servizio rispetto all'anno pregresso, tenuto anche conto dell'avvenuto collocamento in quiescenza nel corso del 2019 di n. 1 funzionario dell'Autorità. Vanno poi annoverate tra le unità in servizio presso l'Autorità il personale appartenente alla Guardia di finanza che, grazie alla prosecuzione dello specifico Protocollo d'intesa stipulato con quest'ultima, apportano da sempre un lodevole contributo alle attività ispettive demandate all'Autorità.

Relazioni con OO.SS.

Con riguardo alle relazioni con le Organizzazioni sindacali, il 2019 è stato segnato da diversi tavoli di confronto aventi ad oggetto, tra le differenti tematiche in esame, anche il trattamento economico-giuridico del personale del Garante.

Formazione

Particolare attenzione è stata riservata anche all'attività formativa per il personale. A tal fine, l'Autorità ha partecipato, come di consueto, ai periodici tavoli di coordinamento del Club dei formatori convocati dalla Scuola nazionale dell'amministrazione, il cui catalogo formativo, da sempre, rappresenta una proficua opportunità per il personale del Garante di perfezionamento delle proprie conoscenze e competenze. Una parte rilevante del personale ha usufruito nel 2019 dei corsi Sna a catalogo per adempiere alla formazione obbligatoria nelle materie dell'anticorruzione e della trasparenza amministrativa nonché alla formazione specifica in tema di rapporto di quiescenza del personale. Parallelamente, in accoglimento delle esigenze formative linguistiche segnalate dal personale, l'Autorità ha avviato al termine dell'anno una specifica istruttoria che nel 2020 porterà all'individuazione di una scuola di lingua inglese in grado di colmare, a vario livello, le esigenze formative richiamate.

Salute e sicurezza

Con riferimento agli adempimenti previsti dal d.lgs. n. 81/2008 in materia di tutela della salute e della sicurezza nei luoghi di lavoro, l'Autorità ha provveduto al progressivo completamento dei percorsi formativi obbligatori destinati ai dipendenti, alla designazione dei nuovi addetti alla squadra antincendio dell'Autorità (secondo quanto prescritto dall'art. 18, comma 2, d.lgs. n. 81/2008) ed alla contestuale formazione specifica normativamente prevista per l'assolvimento delle mansioni ad essi attribuite nonché al costante supporto e monitoraggio delle attività del Responsabile del servizio prevenzione e protezione incaricato e del medico competente nelle rispettive materie. Complessivamente sono state erogate circa n. 490 ore di formazione obbligatoria (anticorruzione, trasparenza, sicurezza nei luoghi di lavoro, ecc.) che hanno interessato circa il 31% del personale.

Tirocini

Riguardo alle consuete opportunità formative offerte dall'Autorità, sono state bandite due procedure selettive per tirocini di orientamento e formazione presso

25

l'Ufficio del Garante, anche grazie alle convenzioni in essere con differenti realtà universitarie italiane, che hanno rappresentato per dieci giovani laureati una proficua opportunità formativa negli ambiti giuridico e della comunicazione istituzionale.

In considerazione dell'interesse mostrato da alcune associazioni studentesche attualmente interessate allo studio della tutela dei dati personali, l'Autorità ha organizzato presso la propria sede un incontro con un gruppo di studenti di Giurisprudenza per illustrare le attività istituzionali del Garante.

Collaboratori esterni

Presso l'Autorità ha continuato ad operare il Servizio di controllo interno presieduto da un magistrato della Corte dei conti e composto da due dirigenti generali, rispettivamente, della Ragioneria generale dello Stato e della Presidenza del Consiglio dei ministri. L'Autorità si è avvalsa, inoltre, nei casi di impossibilità a farsi rappresentare dall'Avvocatura generale dello Stato, di professionisti del libero foro per la tutela in giudizio nonché di collaboratori esterni in occasione dell'espletamento dei menzionati concorsi.

Segreteria generale

L'attività del Garante è stata fondata sul metodo della programmazione e sul rispetto dei principi di economicità ed efficienza dell'azione amministrativa, in conformità al Regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'Ufficio, attraverso l'attività di coordinamento svolta dal Segretario generale, soggetto preposto all'Ufficio ai sensi dell'art. 156, comma 1, del Codice.

Il corretto espletamento da parte del Garante dei compiti e dei poteri attribuiti dalla disciplina vigente è stato assicurato dal Segretario generale attraverso il costante raccordo tra le Unità organizzative e il Collegio, la continua attività istruttoria degli schemi di provvedimento oggetto di esame (per un totale di circa cinquanta adunanze nel 2019), la partecipazione a diversi incontri e innumerevoli interlocuzioni con attori istituzionali e organismi rappresentativi di varie categorie, svolti anche in ambito europeo e internazionale. Ciò ha consentito, da un lato, di veicolare, in consessi istituzionali nazionali e internazionali, gli orientamenti maturati dall'Autorità, anche allo scopo di verificarne la piena fondatezza specie con riferimento alle tematiche di maggiore criticità in relazione alla protezione dei dati personali; dall'altro lato, la possibilità di un costante confronto e l'aggiornamento hanno permesso di riportare nell'Ufficio le buone prassi sviluppate all'estero con un proficuo arricchimento sotto il profilo della conoscenza delle problematiche di maggiore attualità.

In tale quadro, si segnala la partecipazione del Segretario generale alle sessioni plenarie del Comitato europeo per la protezione dei dati, la partecipazione alla *Spring Conference* che si è tenuta a Tbilisi (Georgia, 8-10 maggio 2019), nella quale ha effettuato un intervento dal titolo "*The Italian rules to prevent and counteract the phenomena of cyberbullism*", nonché la partecipazione alla 41ª *International Conference of Data Protection and Privacy Commissioners* – ICDPPC (21-24 ottobre 2019 dal titolo "*Convergence and connectivity*"), prendendo parte alla tavola rotonda sul tema "*Data protection and competition as converging digital regulation: from theory to practice*"). In aggiunta, egli ha preso parte ai lavori del *Ad Hoc Committee on Artificial Intelligence* – CAHAI, presso il Consiglio d'Europa (Strasburgo, 17-20 novembre 2019).

Nell'ambito del Comitato europeo per la protezione dei dati, il Segretario generale è stato eletto coordinatore, per un mandato di due anni, della Commissione di controllo coordinato istituita nel dicembre 2019 per vigilare sui sistemi informativi e sugli organismi, gli uffici e le agenzie operanti nei settori delle frontiere, dell'asilo e della migrazione (SIS, EES, ETIAS e VIS), della cooperazione di polizia e giudiziaria (SIS, EPPO, Eurojust, ECRIS-TCN) e del mercato interno (IMI). Tra i compiti

della Commissione rientreranno, tra l'altro, il sostegno alle autorità di controllo nazionali nello svolgimento di *audit* e ispezioni; gli approfondimenti sull'interpretazione o l'applicazione delle norme; lo studio dei problemi legati all'esercizio dei diritti degli interessati; l'elaborazione di proposte armonizzate per la soluzione dei problemi; le attività di sensibilizzazione rispetto ai diritti in materia di protezione dei dati. La Commissione si riunirà almeno due volte l'anno in una composizione variabile a seconda del sistema informativo, dell'organo o dell'agenzia soggetti a vigilanza.

La posizione del Garante è stata rappresentata dal Segretario generale anche in occasione di incontri, convegni e seminari aventi ad oggetto gli aspetti di maggiore criticità interpretativa e/o difficoltà applicativa emergenti dalla disciplina. Gli interventi hanno riguardato, fra i tanti, la libera circolazione dei dati personali e la società digitale, la *governance* digitale, i nuovi consumerismi, la revisione della normativa sulla trasparenza della pubblica amministrazione, *whistleblowing,* i problemi applicativi del RGPD, la politica della concorrenza nell'era della digitalizzazione, la *smart governance* e politiche di innovazione, *blockchain* e industria 4.0, le possibili nuove regole per internet, il regime della trasparenza tra Stati Uniti e Italia, le politiche antitrust su mercati digitali e *privacy*, l'innovazione tecnologica nella sicurezza, il contrasto al cyberbullismo.

Il Segretario generale ha partecipato, altresì, ai lavori di consolidamento del Comitato *Fintech* presso il Mef, in collaborazione con Consob, Banca d'Italia e AgID; è poi intervenuto all'incontro formativo conclusivo organizzato con altre autorità nazionali di controllo nell'ambito del progetto T4DATA (in partenariato con la Fondazione Lelio e Lisli Basso-Issoco sul progetto di formazione, approvato dalla Commissione europea, focalizzato sulla figura del Responsabile per la protezione dati).

In relazione al nuovo quadro normativo, si segnala la partecipazione del Segretario generale al Gruppo di lavoro, in rappresentanza del Garante, istituito presso il Ministero della giustizia, incaricato di provvedere alla redazione del decreto recante garanzie appropriate per i dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza di cui all'art. 2-*octies* del Codice.

Nel dicembre 2019, è stato designato componente della Commissione per la ricognizione e la revisione del sistema normativo e della trasparenza, istituita presso il Dipartimento della Funzione pubblica al fine di aggiornare la disciplina in materia.

Fra le attività necessarie ad assicurare la corretta applicabilità del RGPD, il Segretario generale ha provveduto a fornire periodicamente indicazioni, anche di carattere interpretativo della normativa, agli Uffici e all'occorrenza, ad attivare quanto ritenuto necessario per conformare le modalità operative al quadro normativo. Si è così provveduto ad avviare i lavori di revisione delle procedure interne, che sono sfociati, tra l'altro, nell'adozione 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) e nel regolamento n. 2/2019, concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante (doc. web n. 9107640).

Al fine di assicurare l'efficienza del Garante, sotto il profilo organizzativo, il Segretario generale ha provveduto altresì a gestire le problematiche riguardanti il personale, le risorse interne e strumentali, la contrattualistica, la digitalizzazione dell'Ufficio, e i rapporti con le altre autorità indipendenti nel quadro delle convenzioni stipulate sui servizi strumentali.

Nell'ambito dell'attività della segreteria del Collegio, ha continuato a seguire le attività dell'organo collegiale collaborando con gli Uffici dell'Autorità in rela-

zione alla predisposizione e distribuzione della documentazione necessaria per le adunanze (concernente in particolare schemi di provvedimento, appunti e note), la redazione e conservazione dei verbali delle riunioni e la custodia degli originali degli stessi e delle deliberazioni adottate. Ha altresì assicurato il controllo puntuale dei testi deliberati dal Collegio in vista della loro pubblicazione sul sito istituzionale dell'Autorità.

Si è altresì contribuito a gestire le richieste di oscuramento e di deindicizzazione di alcuni atti dell'Autorità, formulati da interessati e da titolari del trattamento coinvolti a vario titolo in alcune istruttorie condotte dall'Autorità, in particolare con riferimento a esigenze di riservatezza riguardo a casi di segreto industriale o *know-how* tecnologico.

Controllo di gestione

L'efficienza dell'Autorità è stata perseguita anche attraverso il controllo di gestione, che ha comportato un'analisi periodica degli affari assegnati alle diverse Unità organizzative mediante il sistema di protocollazione Archiflow, con la produzione di una reportistica mensile di carattere statistico che si è focalizzata sull'andamento della trattazione degli affari, il riepilogo dei flussi (fascicoli assegnati ed evasi) e il controllo delle pratiche esposte al rischio di arretrato.

Il Responsabile della protezione dei dati

Anche presso il Garante ha operato, nel corso dell'anno, la figura del Responsabile della protezione dei dati personali per lo svolgimento dei compiti indicati agli artt. 38 e 39 del RGPD.

25.4. *"Autorità trasparente" e adempimenti relativi alla disciplina anticorruzione*

L'Autorità ha continuato a dare attuazione alla disciplina di trasparenza alimentando la sezione "Autorità trasparente", all'interno della quale sono state tempestivamente pubblicate, in conformità a quanto previsto dall'art. 1, comma 14, l. n. 190/2012, sia la relazione annuale del Responsabile della prevenzione della corruzione e della trasparenza (Rpct) per l'anno 2019, relativa all'efficacia delle misure di prevenzione definite nel Piano triennale di prevenzione della corruzione e della trasparenza 2019-2021 (doc. web n. 9255597), sia la griglia di rilevazione di cui all'allegato 2 della delibera Anac n. 141/2018 che il Rpct è tenuto a pubblicare in assenza di Oiv o strutture equivalenti presso l'Autorità.

Nel 2019 è stato attuato il Piano triennale di prevenzione della corruzione e della trasparenza (Ptpct) 2019-2021 proseguendo l'adozione delle misure generali previste; tra queste, ha trovato applicazione anche la misura della rotazione del personale che ha interessato il profilo professionale dei funzionari.

Con l'approvazione da parte del Garante dei nuovi regolamenti interni n. 1/2019, concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante, e n. 2/2019, concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali, sono stati nuovamente mappati i processi dell'Autorità, anche in vista della predisposizione del nuovo Piano triennale di prevenzione della corruzione 2020-2022, adottato dal Garante con la deliberazione 30 gennaio 2020, n. 22 (doc. web n. 9265074).

Tenendo conto delle risorse disponibili e delle complessive esigenze di funzionamento nonché dei carichi di lavoro gravanti sull'Autorità, è proseguita l'attività formativa del personale dell'Autorità tramite i corsi organizzati dalla Scuola nazionale dell'amministrazione (Sna) (cfr. par. 25.3).

Con riguardo alla disciplina in materia di accesso civico introdotta con il d.lgs. n. 33/2013, l'Ufficio ha dato riscontro motivato a tutte le istanze pervenute.

25

In particolare, si segnalano due richieste di accesso civico generalizzato presentate ex art. 5, comma 2, d.lgs. n. 33/2013: l'una, avente ad oggetto la documentazione menzionata nell'elenco dei consulenti e collaboratori dell'anno 2018 (riportato nella sezione trasparenza del sito internet del Garante), con specifico riferimento agli incarichi professionali conferiti a due noti avvocati a decorrere dall'anno 2002 nonché avente ad oggetto la relativa documentazione contabile; l'altra, avente ad oggetto il rilascio degli atti utilizzati per il diniego a un'istanza di accesso civico presentata nel 2018 da un giornalista da parte del responsabile del procedimento dell'Ufficio del Garante, nonché degli atti istruttori propedeutici alla decisione del Collegio reso sulla successiva istanza di riesame.

Nel corso del primo procedimento, l'Ufficio ha proceduto ad un esame approfondito della richiesta, nonché degli atti e delle informazioni oggetto della medesima, valutando il ricorrere di casi di esclusione del diritto di accesso civico generalizzato di cui all'art. 5-*bis*, comma 3, d.lgs. n. 33/2013. Si è esaminato, in particolare, l'obbligo di pubblicazione ex art. 15, d.lgs. n. 33/2013, attinente solo a circoscritte e tassative informazioni concernenti i titolari di incarichi di collaborazione o consulenza e non anche ai documenti integrali cui le stesse informazioni fanno riferimento. Pertanto, anche in considerazione dell'ingerenza nel diritto fondamentale alla protezione dei dati personali, che deve essere limitata allo "stretto necessario" (cfr. Corte di giustizia dell'Unione europea, 8 aprile 2014, Digital Rights Ireland e Seitlinger e del 21 didembre 2016, Tele2 e Watson), il provvedimento con cui è stato negato l'accesso civico generalizzato è stato adottato e motivato in ragione della natura dei documenti e delle informazioni richieste (nota 11 aprile 2019), con specifico riferimento agli atti connessi alla difesa in giudizio del Garante ed alla documentazione sottoposta alla disciplina del segreto professionale, nonché in ragione delle più generali esigenze inerenti al diritto alla difesa e alla libera determinazione della condotta processuale (art. 24 Costituzione italiana; art. 6 Convenzione EDU; art. 47 Carta dei diritti fondamentali dell'unione europea).

Nel corso del secondo procedimento di accesso civico generalizzato, l'Ufficio ha esaminato l'istanza alla luce delle finalità dettate dalla norma di "favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico" (art. 5, comma 2, d.lgs. n. 33/2013). Per quanto, infatti, la legge non richieda l'esplicitazione della motivazione della richiesta di accesso civico generalizzato, deve intendersi implicita la necessaria rispondenza della stessa al soddisfacimento di un interesse che presenti una valenza pubblica (cfr. TAR Lazio, sez. II *bis*, 2 luglio 2018, n. 7326 e TAR Lazio, sez. III *quater*, 17 settembre 2019, n. 11024). Nella vicenda all'attenzione dell'Ufficio, se lo scopo della richiesta in esame fosse stata la verifica del corretto espletamento dell'attività procedimentale del Garante in relazione ad altra richiesta di accesso civico generalizzato, tale interesse doveva ritenersi già ampiamente soddisfatto all'esito della sentenza pubblica del Tribunale amministrativo regionale, che ha confermato la validità dei provvedimenti adottati dal Garante in relazione alla suddetta vicenda. Diversamente, la richiesta di conoscere il contenuto di atti utilizzati dal Garante in un altro procedimento relativo ad un accesso civico generalizzato non fa emergere alcun ulteriore interesse preordinato al controllo generalizzato del buon andamento dell'Autorità in ordine all'espletamento delle proprie funzioni istituzionali, nonché all'utilizzo corretto delle risorse pubbliche ed alla promozione della partecipazione al dibattito pubblico. Paradossalmente, viceversa, richieste con tale oggetto possono a loro volta generare ulteriori analoghe richieste, senza limite, in una spirale del tutto estranea alle finalità dello strumento, ed idonea invece ad aggravare, senza utilità alcuna, l'attività del soggetto pubblico,

25

in termini cui ben si attaglia la recente pronuncia del Consiglio di Stato secondo cui l'accesso civico "non è utilizzabile in modo disfunzionale rispetto alla predetta finalità ed essere trasformato in una causa di intralcio al buon funzionamento della P.A. e va usato secondo buona fede, sicché la valutazione del suo uso va svolta caso per caso e con prudente apprezzamento, al fine di garantire, secondo un delicato ma giusto bilanciamento che non obliteri l'applicazione di tal istituto, che non se ne faccia un uso malizioso e, per quel che concerne nella specie, non si crei una sorta di effetto *boomerang* sulla P.A. destinataria" (Cons. Stato, sez. VI, 13 agosto 2019, n. 5702). Ciò a prescindere da ogni aspettativa di riservatezza di chi presenta la prima richiesta di accesso, cui nella sostanza si riferisce ogni richiesta successiva. Per tali ragioni, è stata negata anche la seconda istanza di accesso civico generalizzato (nota 14 novembre 2019).

Merita altresì segnalare che in relazione a tutte le istanze di riesame (art. 5, comma 7, d.lgs. n. 33/2013) portate all'attenzione del Rpct presso l'Autorità è stato fornito tempestivamente riscontro (pari a complessive n. 4 trattazioni), come pure in relazione a n. 3 istanze di accesso civico relative a dati a pubblicazione obbligatoria (art. 5, comma 1, d.lgs. n. 33/2013), che in due casi hanno dato luogo ad un adeguamento dei contenuti del sito.

25.5. *Il settore informatico e tecnologico*

Sistema informativo e servizi ICT

Nel 2019 l'attività di sviluppo del sistema informativo è stata volta all'introduzione di migliorie nel sistema di protocollo informatico, piattaforma di base a diversi ambiti applicativi, e allo sviluppo di funzionalità nell'ottica di una maggiore adesione alle previsioni del Cad. Inoltre, negli ultimi mesi dell'anno è stato predisposto un capitolato tecnico per l'acquisizione nel 2020 di ulteriori servizi di sviluppo *software* nel medesimo ambito.

Intensa è stata l'attività del gruppo di lavoro istituito in vista dell'elaborazione di un progetto di digitalizzazione dei flussi documentali; tra le varie attività poste in essere, si segnala la predisposizione di un nuovo articolato titolario di classificazione dei fascicoli archivistici.

Nell'ambito dei servizi e delle applicazioni web, la piattaforma a supporto del sito istituzionale è stata trasferita in ambiente *cloud*, anche al fine di garantire superiori livelli di sicurezza e continuità, usufruendo dei servizi di gestione operativa e di conduzione applicativa previsti nella convenzione Consip "SPC Lotto 4". Inoltre, sono state messe a punto nuove funzionalità grazie alla disponibilità di *web services* e alla rapidità di implementazione delle opportune interfacce, mediante la stipulazione di un apposito contratto di manutenzione.

Al fine di migliorare l'usabilità e la capacità comunicativa del sito sono iniziati i lavori di reingegnerizzazione del portale.

Sono state implementate nuove funzionalità per consentire la comunicazione *online* dei dati di contatto dei Rpd, acquisendo nuovi servizi *cloud* da fornitori qualificati da AgID. Grazie agli sviluppi effettuati è stato possibile nel corso del 2019 ricevere un totale di 13.692 comunicazioni di dati di contatto, ripartite tra variazioni e nuove comunicazioni.

Sono stati definiti i requisiti utente e il progetto dei fabbisogni propedeutici alla stipulazione di un contratto di adesione all'accordo-quadro Consip "SPC Lotto 2" relativo ai servizi di sicurezza.

È stato stipulato con il Politecnico di Milano un accordo di collaborazione per la realizzazione della piattaforma *webinar* relativa al progetto T4DATA, dedicata, in

25

una prima fase, alla formazione dei Rpd.

Per il tramite del Dipartimento tecnologie digitali e sicurezza informatica – che ha risposto direttamente ad alcune richieste tecniche da parte di altre autorità europee secondo quanto previsto dall'art. 61 del RGPD – continuano ad essere amministrate le utenze IMI del personale dell'Autorità, in collaborazione con il segretariato del Cepd.

Le postazioni di lavoro gestite sono cresciute, anche a seguito dell'immissione in ruolo di nuove unità di personale per l'area giuridica e amministrativa a seguito di concorsi pubblici, per un totale di 280 postazioni tra fisse e mobili.

Sono infine continuate le ordinarie attività di gestione dell'infrastruttura ICT che hanno compreso un consistente ammodernamento dell'*hardware*, sia a livello di postazioni di lavoro sia a livello di infrastruttura di rete, con la sostituzione degli apparati di protezione perimetrale e dei VPN *server* per i collegamenti remoti sicuri e l'espansione della rete Wifi, mantenendo l'aggiornamento costante dei sistemi operativi *client*, dei sistemi antivirus e completando la migrazione dei sistemi di *backup* verso un'unica piattaforma integrata.

Tutti i lavori ordinari, straordinarie e le attività progettuali sono stati affrontati con una ridottissima dotazione di personale, ammontante a soli due funzionari tecnici, numericamente insufficiente a garantire per il futuro lo sviluppo dei sistemi informativi, anche se di particolare competenza e caratterizzato da dedizione e professionalità.

Sicurezza informatica dell'Ufficio

Non si sono registrate situazioni pregiudizievoli rispetto alla sicurezza informatica sulle postazioni individuali e sui sistemi *server*, né su altre componenti dell'infrastruttura. Si è registrato un solo attacco informatico condotto nei confronti di un sistema applicativo in via di dismissione (registro delle notificazioni, definitivamente disattivato a far data dal 1° gennaio 2020) contenente dati destinati alla pubblicazione *online* ed esterno al perimetro di sicurezza della rete.

Sono stati eseguiti periodici *vulnerability assessment* e *penetration test*, mirati sul portale web e sui servizi esposti all'accesso del pubblico che non hanno rivelato vulnerabilità significative a esclusione di alcuni servizi non critici per i quali sono state accelerate le procedure di migrazione o di dismissione, completate nel corso dell'anno.

La continuità dei servizi accessibili al pubblico è stata in linea coi valori degli anni precedenti, con *downtime* dei servizi intorno alle otto ore complessive nell'arco dell'anno per cause esterne (*black-out* elettrici di lunga durata) o per manutenzione programmata.

PAGINA BIANCA

I dati statistici

PAGINA BIANCA

IV - I dati statistici 2019

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	232
Pareri su norme di rango primario statale, delle regioni e delle autonomie	6
Pareri su atti regolamentari e amministrativi	46
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	33
Pareri ai sensi dell'art. 110 del Codice per progetti di ricerca medica, biomedica e epidemiologica nonché ex art. 36 del RGPD	1
Autorizzazioni di accordi amministrativi ai sensi dell'art. 46, par. 3, lett. *b*), 58, par. 3, lett. *i*) e 63, del RGPD	1
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché di accertamenti d'ufficio	63
Ordinanze-ingiunzione adottate dal Garante	36
Riscontri a segnalazioni e reclami (art. 11, reg. Garante n. 1/2019)	8.092
Riscontri a quesiti (art. 11, reg. Garante n. 1/2019)	482
Provvedimenti di approvazione di codici di condotta	2
Audizioni del Presidente del Garante e memorie scritte trasmesse al Parlamento	7
Riscontri dell'Urp a quesiti e altre istanze	15.821
Leggi regionali esaminate ai fini dell'impugnazione da parte del Governo ex art. 127 Cost.	4
Rilievi formulati in relazione a leggi regionali ai fini dell'impugnazione da parte del Governo ex art. 127 Cost.	3
Accertamenti e controlli effettuati *in loco* (artt. 157-158, d.lgs. n. 196/2003)	147
Violazioni amministrative (Codice previgente)	32
Misure correttive (art. 58, par. 2, del RGPD)	95
Sanzioni applicate con ordinanza-ingiunzione	277
Pagamenti derivanti dall'attività sanzionatoria	3.017.363
Comunicazioni di notizia di reato all'Autorità giudiziaria	9
Opposizioni (trattate) a provvedimenti del Garante	109
Ricorsi (trattati) ex art. 152, d.lgs. n. 196/2003	49
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 1, d.lgs. n. 33/2013	3
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 2, d.lgs. n. 33/2013	22
Istanze di riesame diniego accesso civico presentate al Rpct e riscontrate ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	4
Riunioni del Comitato europeo per la protezione dei dati personali	11
Partecipazione a sottogruppi di lavoro del Comitato europeo per la protezione dei dati personali	73
Riunioni e ispezioni autorità comuni di controllo/organismi di supervisione (Europol, SIS II, Dogane, Eurodac, VIS)	11
Conferenze internazionali	2
Riunioni presso il Consiglio d'Europa e l'Organizzazione per la cooperazione e lo sviluppo economico	9
Riunioni e *workshop* presso Consiglio/Commissione e altri organismi UE	13
Altre conferenze e incontri	18

Tabella 1. Sintesi delle principali attività dell'Autorità

Tabella 2. Attività di comunicazione istituzionale

Attività di comunicazione istituzionale	
Comunicati stampa	55
Newsletter	12
Bollettino radiofonico del Garante	22
Prodotti editoriali	4
Prodotti web	10
Video *spot*	5

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	**Provvedimenti**	**Pareri resi nell'anno***
Funzioni di interesse pubblico	Parere al Mef su schema d.lgs. recante modifiche alla normativa sull'utilizzo del sistema finanziario a scopo di riciclaggio e di finanziamento del terrorismo (doc. web n. 9126288)	1
Sanità	Parere a Regione Molise su proposta di legge regionale concernente test antidroga casuali e periodici per i consiglieri e assessori della Regione Molise (doc. web n. 9206457)	1
Settore privato	Parere a Provincia autonoma di Trento su proposta di disposizione integrativa dell'art. 4, legge provinciale 31 maggio 2012, n. 10 recante interventi urgenti per favorire la crescita e la competitività del Trentino (doc. web n. 9123419)	2
	Parere a Provincia autonoma di Trento su disegno di legge concernente la disciplina dell'agriturismo e modificazioni della legge provinciale 19 dicembre 2001, n. 10 e della legge provinciale 13 dicembre 1999, n. 6 (doc. web n. 9232560)	
Trasporti	Parere a Ministero delle infrastrutture e dei trasporti su schema d.lgs. recante revisione e integrazione del d.lgs. 18 luglio 2005, n. 171, recante codice della nautica da diporto (doc. web n. 9162642)	2
	Parere a Regione Lombardia su proposta normativa recante l'istituzione del registro regionale per la gestione coordinata degli accessi dei veicoli alla Ztl che verrà inserita nel progetto di legge regionale collegato 2020 a manovra di bilancio Regione Lombardia (doc. web n. 9232560)	
Totale		**6**

(*) inerenti anche ad affari pervenuti anteriormente al 2019

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	**Provvedimenti**	**Pareri resi nell'anno***
Attività di polizia, sicurezza nazionale e governo del territorio	Parere sullo schema di decreto di attuazione dell'art. 57 del Codice recante regolamento sulla disciplina delle procedure di raccolta, accesso, comunicazione, correzione, cancellazione ed integrazione dei dati e delle informazioni registrati nel Ced del Dipartimento di pubblica sicurezza del Ministero dell'interno (doc. web n. 9116046)	2
	Parere sullo schema di d.P.C.M. concernente disposizioni in materia di misure di protezione dei minori stranieri non accompagnati (doc. web n. 9162562)	
Digitalizzazione della p.a.	Parere sullo schema di decreto del Ministro per la p.a. recante le modalità di digitalizzazione delle procedure dei contratti pubblici (*e-procurement*) ai sensi dell'art. 44, d.lgs. 18 aprile 2016, n. 50 (doc. web n. 9113870)	3
	Parere Mise sul decreto relativo alle procedure di consultazione e accesso al sistema informativo nazionale federato delle infrastrutture (doc. web n. 9123563)	
	Parere sullo schema di decreto del Ministero dell'infrastrutture e dei trasporti concernente la disciplina delle modalità semplificate di trasmissione dei certificati medici attestanti l'idoneità psicofisica dei conducenti dei veicoli a motore (doc. web n. 9207176)	
Fisco	Parere sullo schema di decreto del Ministro dell'economia e delle finanze all'estensione alle strutture militari della rilevazione delle spese sanitarie (doc. web n. 9084299)	5
	Parere al Mef sullo schema di decreto della Ragioneria generale dello Stato relativo all'estensione alle strutture militari della rilevazione delle spese sanitarie (doc. web n. 9084311)	
	Parere su decreto attuativo al Ministero del lavoro e delle politiche sociali in materia di Isee precompilata (doc. web n. 9124390)	
	Parere sullo schema di decreto del Ministro dell'economia e delle finanze per l'estensione della rilevazione delle spese sanitarie attraverso il sistema TS a ulteriori categorie di esercenti le professioni sanitarie (doc. web n. 9162444)	
	Parere sullo schema di decreto del Ministero del lavoro e delle politiche sociali su proposta di Dichiarazione sostitutiva unica (Dsu) e istruzioni per la compilazione (doc. web n. 9163393)	
Funzioni di interesse pubblico	Parere sullo schema di regolamento recante la disciplina delle modalità di iscrizione in via telematica degli atti di ultima volontà nel registro generale dei testamenti su richiesta del notaio o del capo dell'archivio notarile, ai sensi dell'art. 5-*bis* della legge 25 maggio 1981 (doc. web n. 9113929)	6
	Parere sullo schema di regolamento recante modifiche al decreto del Ministro dell'interno 15 febbraio 2012, n. 23, concernente l'istituzione dell'elenco dei revisori dei conti degli enti locali e modalità di scelta dell'organo di revisione economico-finanziario (doc. web n. 9123427)	
	Parere su schema di decreto del Ministro del lavoro e delle politiche sociali in materia di Sistema informativo del Rdc (doc. web n. 9122428)	
	Parere su schema di decreto del Mef per le prestazioni del Fondo indennizzo risparmiatori (Fir) in applicazione delle disposizioni di cui all'art. 1, commi da 493 a 507, l. 30 dicembre 2018, n. 145 (doc. web n. 9126476)	
	Parere su schema di decreto del Ministro del lavoro e delle politiche sociali, di concerto con il Mef in materia di fruizione, mediante Carta Rdc, del beneficio economico spettante ai beneficari del Rdc (doc. web n. 9232574)	
	Parere su schema di d.P.C.M. recante modalità e criteri di attivazione e gestione del Servizio IT-*alert* (doc. web n. 9207188)	

(*) inerenti anche ad affari pervenuti anteriormente al 2019

Istruzione	Parere su schema di decreto del Ministro dell'istruzione, dell'università e della ricerca recante modifiche al regolamento 8 febbraio 2013 n. 45 sulle modalità di accreditamento delle sedi e dei corsi di dottorato e criteri per la istituzione dei corsi di dottorato da parte degli enti accreditati (doc. web n. 9102022)	4
	Parere su schema di regolamento del Mibac in tema di criteri e modalità di attribuzione e di utilizzo della Carta elettronica per i diciottenni (cd. *bonus* cultura) (doc. web n. 9195252)	
	Parere su schema di contratto tra il Mibac e Sogei in attuazione dell'art. 2, d.P.C.M. n. 16/2017 (doc. web n. 9082272)	
	Parere su schema di provvedimento Mibac recante le modalità e i tempi della gestione e conservazione dei dati personali raccolti in attuazione della disciplina in materia di attribuzione e di utilizzo della Carta elettronica prevista dall'art. 1, comma 604, l. 30 dicembre 2018, n. 145 (cd. *bonus* cultura) (doc. web n. 9220734)	
Lavoro pubblico e privato	Parere su schema di d.P.C.M. concernente la disciplina di attuazione della disposizione di cui all'art. 2, l. 19 giugno 2019, n. 56, recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo (doc. web n. 9147290)	2
	Parere su schema di d.P.C.M. concernente l'individuazione dei criteri, delle condizioni e degli adempimenti per richiedere l'anticipo Tfs/Tfr, nonché le modalità di funzionamento dell'istituendo Fondo di garanzia (doc. web n. 9126584)	
Sanità	Parere su schema di regolamento per l'attuazione della banca dati nazionale delle dichiarazioni anticipate di trattamento (Dat) (doc. web n. 9117770)	3
	Parere su schema di regolamento del Ministro della salute recante la disciplina degli obiettivi, delle funzioni e della struttura del Sit e del Registro nazionale dei donatori di cellule riproduttive a scopi di procreazione medicalmente assistita di tipo eterologo (doc. web n. 9131111)	
	Parere su schema di decerto del Ministro della salute che disciplina il Sistema di segnalazione delle malattie infettive (Premal) (doc. web n. 9124009)	
Telemarketing - Registro opposizioni	Parere su schema di regolamento che sostituisce il d.P.R. 7 settembre 2010, n. 178, recante disposizioni in materia di iscrizione e funzionamento del Registro pubblico delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato (doc. web n. 9109315)	1
Trasporti	Parere su schema di decreto recante modifiche al d.P.R. 19 settembre 2000, n. 358 che ha introdotto lo sportello telematico dell'automobilista (doc. web n. 9106322)	1
Totale		**27**

Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi ad altre Istituzioni		
Temi	**Provvedimenti**	**Pareri resi nell'anno***
Digitalizzazione p.a.	Parere sullo schema di linee guida AgID relative all'indice dei domicili digitali delle pp.aa. e dei gestori di pubblici servizi (IPA), art. 71 del Cad (doc. web n. 9113862)	3
	Parere sullo schema di linee guida AgID contenenti regole tecniche e raccomandazioni afferenti la generazione di certificati qualificati, firme e sigilli elettronici qualificati e validazione temporale elettronica qualificata (doc. web n. 9123455)	
	Parere sullo schema di linee guida AgID relative all'accessibilità degli strumenti informatici (doc. web n. 9207804)	
Funzioni di interesse pubblico	Parere su schema di provvedimento dell'Inps attuativo dell'art. 5, comma 1, d.l. 28 gennaio 2019, n. 4, di approvazione del modulo di domanda del Reddito e della Pensione di cittadinanza (doc. web n. 9106306)	4
	Parere sullo schema di deliberazione dell'Arera recante l'istituzione del Portale dei consumi di energia elettrica e di gas naturale (doc. web n. 9123551)	
	Parere sullo schema di decreto del Direttore dell'Agenzia delle dogane e dei monopoli in tema di regole tecniche per la produzione dei sistemi di gioco Vlt (doc. web n. 9126407)	
	Parere sullo schema schema di linee guida Anac in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro (cd. *whistleblowing*) (doc. web n. 9215763)	
Fisco	Parere su tre schemi di provvedimenti del Direttore dell'Agenzia delle entrate in tema di comunicazione all'Anagrafe tributaria di informazioni per l'elaborazione della dichiarazione dei redditi precompilata relativa all'anno d'imposta 2018 (doc. web n. 9082720)	10
	Parere sullo schema di provvedimento del Direttore dell'Agenzia delle entrate recante modalità tecniche di utilizzo dei dati delle spese sanitarie ai fini della elaborazione della dichiarazione dei redditi precompilata, a decorrere dall'anno d'imposta 2018 (doc. web n. 9084331)	
	Parere su schema di provvedimento del Direttore dell'Agenzia delle entrate relativo alla sperimentazione di una procedura di selezione basata sull'utilizzo delle informazioni fornite dall'Archivio dei rapporti finanziari e dai dati presenti in Anagrafe tributaria per l'individuazione di profili di evasione rilevanti (doc. web n. 9106329)	
	Parere sullo schema di provvedimento del Direttore dell'Agenzia delle entrate recante comunicazioni per la promozione dell'adempimento spontaneo nei confronti dei contribuenti che non hanno dichiarato, in tutto o in parte, le attività finanziarie detenute all'estero nel 2016, come previsto dalla disciplina sul monitoraggio fiscale, nonché gli eventuali redditi percepiti in relazione a tali attività estere (doc. web n. 9106360)	
	Parere su schema di provvedimento del Direttore dell'Agenzia delle entrate concernente la disciplina relativa ai sistemi di biglietterie automatizzate (doc. web n. 9122419)	
	Parere su schema di provvedimento del Direttore dell'Agenzia delle entrate inerente le modalità tecniche di utilizzo dei dati delle spese sanitarie e delle spese veterinarie (doc. web n. 9207155)	
	Parere su schema di provvedimento del Direttore dell'Agenzia delle entrate recante disposizioni in materia di memorizzazione elettronica e trasmissione telematica dei dati dei corrispettivi validi ai fini della lotteria di cui all'art. 1, commi da 540 a 544, l. 11 dicembre 2016, n. 232 (doc. web n. 9175238)	
	Parere su schema di provvedimento del Direttore dell'Agenzia delle entrate in tema di memorizzazione elettronica e trasmissione telematica dei dati dei corrispettivi giornalieri attraverso i registratori telematici (doc. web n. 9217337)	

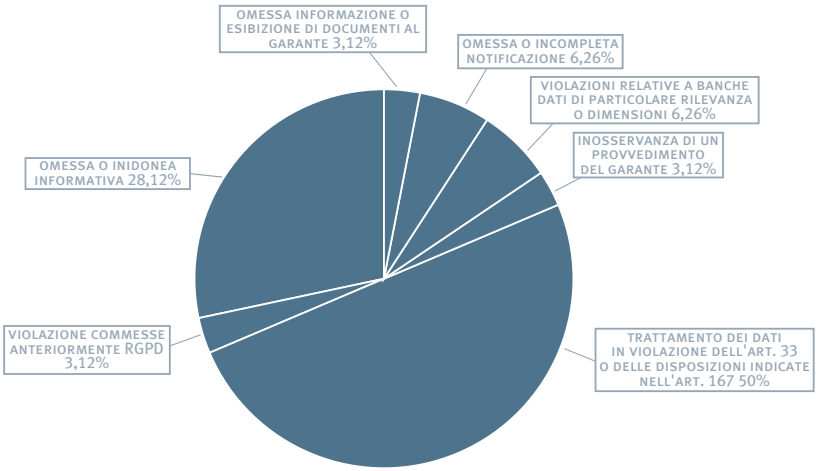
Tabella 5. Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi ad altre Istituzioni

(*) inerenti anche ad affari pervenuti anteriormente al 2019

Fisco	Parere su schema di provvedimento congiunto Inps e Agenzia delle entrate volto a disciplinare le specifiche tecniche per l'accesso alla Dsu precompilata (doc. web n. 9220741)	
	Parere su schema di provvedimento del Direttore dell'Agenzia delle entrate per l'accesso alla dichiarazione 730 precompilata (doc. web n. 9113901)	
Istruzione	Parere su schema di regolamento predisposto dall'Istituto nazionale per la valutazione del sistema educativo di istruzione e formazione, concernente le modalità di svolgimento delle prove Invalsi dell'ultimo anno della scuola secondaria di secondo grado (doc. web n. 9102421)	1
Sanità	Parere all'Istat su indagine europea sulla salute (EHIS) (doc. web n. 9113830)	1
Totale		**19**

Tabella 6. Violazioni amministrative (Codice previgente)

Violazioni amministrative (Codice previgente)	
Omessa o inidonea informativa (art. 161, d.lgs. n. 196/2003)	9
Violazione commesse anteriormente RGPD (artt. 24 e 25, d.lgs. n. 101/2018)	1
Trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, d.lgs. n. 196/2003)	16
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter*, d.lgs. n. 196/2003)	1
Violazioni relative a banche dati di particolare rilevanza o dimensioni (art. 164-*bis*, comma 2, d.lgs. n. 196/2003)	2
Omessa o incompleta notificazione (art. 163, d.lgs. n. 196/2003)	2
Omessa informazione o esibizione di documenti al Garante (art. 164, d.lgs. n. 196/2003)	1
Totale	**32**



Misure correttive (art. 58, par. 2, del RGPD)	
Ammonimenti a titolare/responsabile del trattamento per violazioni RGPD (art. 58, par. 2, lett. *b*)	5
Ingiunzioni a titolare/responsabile del trattamento a soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal RGPD (art. 58, par. 2, lett. *c*)	22
Ingiunzioni a titolare/responsabile del trattamento a soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal RGPD (art. 58, par. 2, lett. *c*)	8
Ingiunzioni a titolare del trattamento di comunicare all'interessato una violazione dei dati personali (art. 58, par. 2, lett. *e*)	4
Imposizioni di limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento (art. 58, par. 2, lett. *f*)	31
Ordini 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*)	21
Sanzioni amministrative pecuniarie ex art. 83 (art. 58, par. 2, lett. *i*)	4
Totale	**95**

Tabella 7. Misure correttive (art. 58, par. 2, del RGPD)

Comunicazioni di notizia di reato all'Autorità giudiziaria	
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168, d.lgs. n. 196/2003)	4
Inosservanza di provvedimenti del Garante (art. 170, d.lgs. n. 196/2003)	4
Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter*, c.p.)	1
Totale	**9**

Tabella 8. Comunicazioni di notizia di reato all'Autorità giudiziaria

Pagamenti derivanti dall'attività sanzionatoria	
Somme versate a titolo di oblazione in via breve	112.000
Somme versate in conseguenza di ordinanze-ingiunzione	1.978.786
Ulteriori entrate derivanti dalla riscossione coattiva	917.717
Entrate derivanti dalla definizione agevolata dei procedimenti sanzionatori (art. 18, d.lgs. n. 101/2018)	8.860
Totale	**3.017.363**

Tabella 9. Pagamenti derivanti dall'attività sanzionatoria

Segnalazioni e reclami		
	Pervenuti nell'anno	**Riscontri resi nell'anno (*)**
Affari legali e giustizia	163	77
Libertà di manifestazione del pensiero e cyberbullismo	651	372
Realtà economiche e produttive	2.541	2.484
Realtà pubbliche	943	835
Reti telematiche e *marketing*	3.762	3.670
Sanità e ricerca	308	235
Tecnologie digitali e sicurezza informatica	1.321	419
Totali	**9.689**	**8.092**

Tabella 10. Segnalazioni e reclami

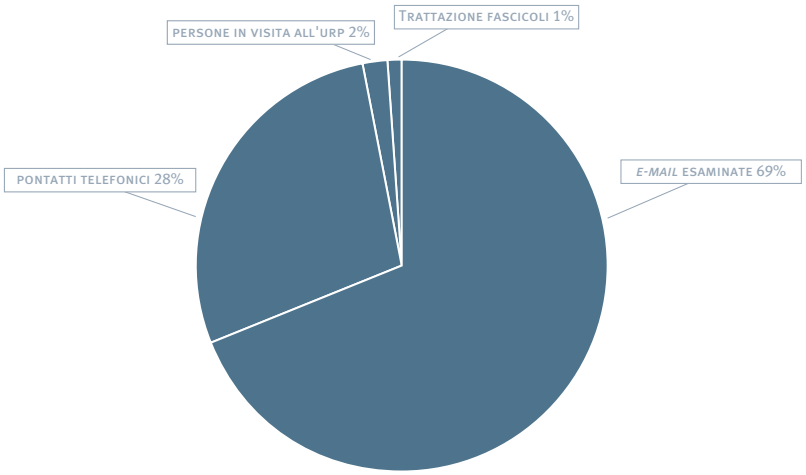
(*) inerenti anche ad affari pervenuti anteriormente al 2019

Tabella 11. Quesiti

Quesiti		
	Pervenuti nell'anno	**Riscontri resi nell'anno (*)**
Affari legali e giustizia	22	9
Libertà di manifestazione del pensiero e cyberbullismo	6	4
Realtà economiche e produttive	141	134
Realtà pubbliche	278	202
Reti telematiche e *marketing*	37	18
Sanità e ricerca	85	112
Tecnologie digitali e sicurezza informatica	6	3
Totali	**575**	**482**

Tabella 12. Attività dell'Ufficio relazioni con il pubblico

Attività dell'Ufficio relazioni con il pubblico	
E-mail esaminate	10.883
Contatti telefonici	4.415
Persone in visita	290
Trattazioni relative a fascicoli	233
Totale	**15.821**



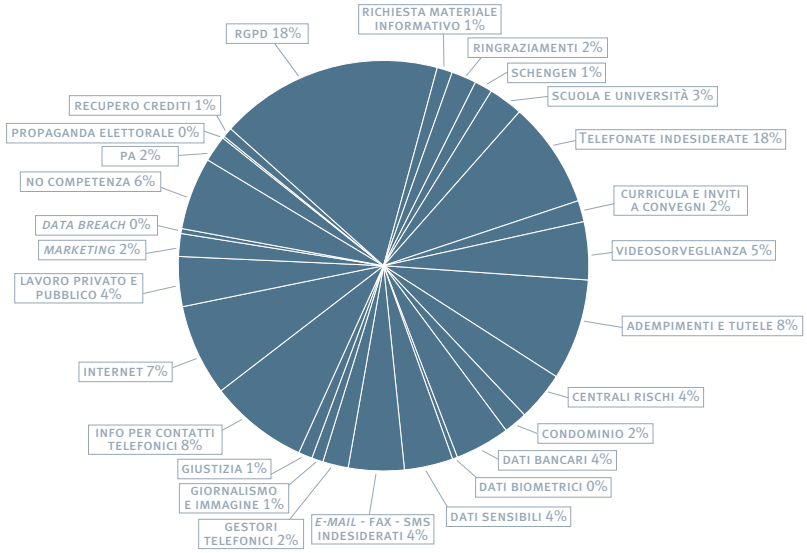


Grafico 13. Oggetto delle *e-mail* esaminate dall'Urp

Personale in servizio (*)				
Area	ruolo (a)	fuori ruolo (b)	comandato presso altre amm.ni o in aspettativa	impiegato dall'Ufficio (a-b+c)
Segretario generale	1			1
Dirigenti	13			13
Funzionari	91	3	4	92
Operativi	21			21
Esecutivi	0			
Totale	**126**	**3**	**4**	**127**
Personale a contratto (art. 156, comma 5, del Codice)				4

Tabella 14. Personale in servizio

Risorse finanziarie				
Entrate accertate	**Anno 2019**	**Anno 2018**	**Variazione**	
Entrate correnti	29.557.763	26.927.498	2.630.266	9,77%
Totale entrate	**29.557.763**	**26.927.498**		**9,77%**
Spese impegnate	**Anno 2019**	**Anno 2018**	**Variazione**	
Spese di funzionamento	23.799.145	22.882.095	917.050	4,01%
Spese in c/capitale	433.168	212.363	220.805	103,98%
Trasferimenti ad amministrazioni	392.825	360.775	32.051	8,88%
Totale spese	**24.625.138**	**23.455.233**	**1.171.906**	**5,01%**

Valori in euro

Tabella 15. Risorse finanziarie

(*) Situazione alla data del 31/12/2019

Tabella 16. Attività internazionali dell'Autorità

Unione europea			
COMITATO EUROPEO PER LA PROTEZIONE DEI DATI	Sessioni plenarie		22-23 gennaio 12 febbraio 12-13 marzo 9-10 aprile 14-15 maggio 4 giugno 9-10 luglio 10-11 settembre 8-9 ottobre 12-13 novembre 2-3 dicembre
	Riunioni dei sottogruppi	*Strategic Advisory*	9 gennaio 31 gennaio
		Border Travel Law Enforcement (BTLE)	19 febbraio 16 aprile 18 giugno 19 settembre 24 ottobre 12 dicembre
		Cooperation	20 febbraio 16 aprile 19-20 giugno 25 settembre 20-21 novembre
		Compliance, E-Government and Health	10 gennaio 31 gennaio 25 febbraio 27 marzo 6 maggio 3 giugno 24 giugno 14 ottobre 15 novembre 9 dicembre
		Financial Matters	14 gennaio 27 febbraio 20 maggio 20 settembre
		Rules of Procedures	11 aprile 5 giugno 4 luglio
		Key Provisions	15 gennaio 25-26 marzo 23 maggio 16 luglio 23 settembre 16 ottobre 25-26 novembre

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI	**Riunioni dei sottogruppi**	***International Transfers***	29 gennaio 19-20 marzo 21-22 maggio 18-19 giugno 17-18 settembre 15-16 ottobre 10-11 dicembre
		Technology	16 gennaio 20-21 febbraio 20-21 marzo 24-25 aprile 22 maggio 12-13 giugno 17 luglio 18 settembre 23-24 ottobre 20 novembre 17 dicembre
		IMI-GDPR ***Users Group***	17 gennaio 23 maggio 7 novembre
		Enforcement	22 febbraio 15 aprile 17 aprile 17 giugno 24 settembre 18 novembre
		Fining Task Force	21 febbraio 20 giugno 26 settembre 19 novembre
		Social Media Working Group	26 febbraio 17 aprile 11 giugno 20 settembre 27 novembre

Unione europea	
Europol Cooperation Board	8 maggio 3-7 giugno (ispezione) – L'Aja 28 novembre
Eurojust	23-27 settembre (ispezione) – L'Aja
Gruppo di coordinamento della supervisione SIS II	19 giugno 26 novembre
Gruppo di coordinamento della supervisione Eurodac	20 giugno 26 novembre
Gruppo di coordinamento della supervisione VIS	20 giugno 27 novembre
Gruppo di coordinamento della supervisione SID	7 maggio

Unione europea	
Riunioni di gruppi di esperti	
Internet Privacy Engineering Network* (IPEN) *Workshop	28 gennaio – Bruxelles
PSD2 and GDPR Workshop	27 febbraio – Bruxelles
Workshop on Data Controllers/Processors	25-26 marzo – Bruxelles
BCR *Workshop*	11-12 giugno – Oslo
ULD-ENISA *Workshop on Pseudonymisation*	12 novembre – Berlino
CPCS *Key User's Group*	13 giugno – Bruxelles 25 settembre – Bruxelles
Workshop on ePrivacy Reform	19 luglio – Bruxelles
Gruppo TLC su dossier *e-privacy*	22 ottobre – Bruxelles 7 novembre – Bruxelles 12 e 18 novembre – Bruxelles
***European Case Handling Workshop* 2019**	27-28 novembre – Bruxelles

Altri *forum* internazionali		
Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	**Comitato WPSPDE** ***Working Party on Security and Privacy in the Digital Economy***	5-7 maggio – Parigi
	Working Party on Data Governance and Privacy in the Digital Economy	18-19 novembre – Parigi
	Working Party on Security in the Digital Economy	19-20 novembre – Parigi
Consiglio d'Europa	**Comitato Consultivo Convenzione 108/1981 (T-PD)**	13-14 giugno – Strasburgo 19-21 novembre – Strasburgo
	T-PD ***Bureau***	20-22 marzo – Parigi 24-27 settembre – Parigi 11-13 dicembre – Strasburgo
	Ad Hoc Committee on Artificial Intelligence	17 novembre – Strasburgo

Conferenze internazionali	
Conferenza di primavera delle Autorità europee di protezione dati	9-10 maggio – Tbilisi
41ª Conferenza internazionale delle Autorità di protezione dati	21-24 ottobre – Tirana

Altre conferenze e incontri	
Gruppo internazionale di lavoro sulla protezione dei dati nelle telecomunicazioni (IWGDPT)	9-10 aprile – Bled 10-11 ottobre – Bruxelles
CPDP ***Conference***	30 gennaio – Bruxelles
CEN-CLC/JTC 8 "Privacy management in products and services"	27 marzo – Berlino 9-10 luglio – Saint Denis
European Cloud Service Data Protection Certification **(AUDITOR)**	11 aprile – Bruxelles
Communications Network Meeting	17 maggio – Vienna
UN ***Special Rapporteur on the Right to Privacy – Consultation on Health Data***	11 giugno – Strasburgo
CPC ***Workshop***	17-18 ottobre – Bruxelles
International Finance Corporation, World Bank, Session de sensibilization: nouveau cadre RGPD 2018 et liens avec la réglementation marocaine	13 giugno – Rabat
Conferenza progetto UE SMEDATA	27-28 novembre – Sofia
OCSE ***Multistakeholder Expert Group*** **per la revisione della raccomandazione OCSE sulla protezione dei dati dei minori** ***online***	30 settembre – Parigi
Incontro ISO/PC 317 ***Consumer Protection – Privacy by Design for Consumer Goods and Services***	7-8 febbraio – Berlino
X Conferenza internazionale ***Personal Data Protection***	7 novembre – Mosca
Convention 108+ ***Conference***	12 giugno – Strasburgo
IIC ***Annual Conference***	10-11- ottobre – Londra
Second Meeting of the Communications Network	17 ottobre – Bruxelles
27701 - ***Privacy Information Management System***	18 novembre – Bruxelles

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Redazione
Garante per la protezione dei dati personali

Piazza Venezia, 11
00187 Roma
tel. 06 696771
email: protocollo@gpdp.it
www.garanteprivacy.it

stampa:
Tiburtini srl - Roma

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

PAGINA BIANCA

181360106630