GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione Annuale 2020

www.gpdp.it

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

Fabio Mattei, *Segretario Generale*

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

GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione annuale 2020

I numeri del 2020

Provvedimenti collegiali **278**

7
Pareri su norme di rango primario

60
Pareri su atti regolamentari e amministrativi

18
Pareri in materia di accesso civico

148
Decisioni su reclami e segnalazioni

8.984
Riscontri a reclami e segnalazioni

422
Riscontri a quesiti

€ 38.448.895
Sanzioni riscosse

21
Ispezioni

179
Riunioni internazionali

8
Comunicazioni all'Autorità giudiziaria

15.040 Riscontri URP

65
Comunicati e *Newsletter*

5.829.946
Accessi al sito web

Indice

Indice

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

II - L'ATTIVITÀ SVOLTA DAL GARANTE

Indice

Avvertenza ed elenco delle abbreviazioni e degli acronimi più ricorrenti

La presente Relazione è riferita al 2020 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
cfr.	confronta
cons.	considerando
C.d.S.	Consiglio di Stato
c.p.	codice penale
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
Cad	codice dell'amministrazione digitale
cap.	capitolo
CDFUE	Carta dei diritti fondamentali dell'Unione europea
cd.	cosiddetto/i
CEDU	Carta europea dei diritti dell'uomo
Cepd o Comitato	Comitato europeo per la protezione dei dati
cfr.	confronta
CGUE	Corte di giustizia dell'Unione europea
cit.	citato
Codice	Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101)
Consob	Commissione nazionale per le società e la borsa
Corte EDU	Corte europea dei diritti dell'uomo
Cost.	Costituzione
DAD	didattica a distanza
DDI	didattica digitale integrata
d.d.l.	disegno di legge
d.l.	decreto-legge
d.lgs.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica

doc.	documento
Dsu	dichiarazione sostitutiva unica
es.	esempio
FAQ	*Frequently Asked Questions*
Fse	fascicolo sanitario elettronico
Gepd	Garante europeo per la protezione dei dati
Gruppo Art. 29	Gruppo dei garanti europei istituto dall'art. 29 della direttiva 95/46/CE
G.U.	Gazzetta ufficiale della Repubblica italiana
GUUE	Gazzetta ufficiale dell'Unione europea
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
n.	numero
p.	pagina
p.a.	pubblica amministrazione/pubbliche amministrazioni
par.	paragrafo
Pec	posta elettronica certificata
provv.	provvedimento del Garante
r.d.	regio decreto
reg.	regolamento
RGPD o Regolamento	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
Rpd	Responsabile della protezione dei dati
Rpo	Registro pubblico delle opposizioni
Rspp	Responsabile del servizio prevenzione e protezione
See	Spazio economico europeo
sez.	Sezione
Spid	Sistema pubblico dell'identità digitale
Ssn	Servizio sanitario nazionale
tab.	tabella
T-PD	Comitato consultivo della Convenzione del Consiglio d'Europa n. 108/1981
t.u.	testo unico
TFUE	Trattato sul funzionamento dell'Unione europea
Tulps	Testo unico delle leggi di pubblica sicurezza
UE	Unione europea
URL	*Uniform resource locator*
v.	vedi

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

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

RELAZIONE ANNUALE
2020

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

1 Introduzione

1.1. Emergenza epidemiologica da Covid-19: è la locuzione che, variamente declinata, con insistenza fa capolino nella Relazione di attività riferita al 2020. Anno che rimarrà (contras)segnato dalla pandemia, i cui effetti si sono prodotti – e non poteva essere diversamente – anche sui temi portati all'attenzione dell'Autorità e sulla sua stessa operatività che, pur nella modalità di "lavoro agile" (parr. 25.3 e 25.5) e ad eccezione dell'inevitabile flessione delle attività ispettive *in loco* (cap. 18), non ha tuttavia subito battute d'arresto. Ed anzi, specie nei settori variamente connessi all'emergenza sanitaria, essa ha registrato – anche in seno al Comitato europeo per la protezione dei dati (cfr. par. 21.1) come pure in tutti i gruppi di lavoro sovranazionali (cfr. par. 21.3) – una severa impennata. Il Garante, infatti, sin dal primo manifestarsi della pandemia, è stato immediatamente "catturato" (con una pressione che tuttora non si allenta) dai riflessi dell'articolata risposta istituzionale approntata per fronteggiare, sul piano sanitario (cap. 5) e su quello economico-sociale (parr. 4.1 e 4.2), gli effetti della pandemia; risposta largamente incentrata sul trattamento, anche massivo, di informazioni personali (non di rado di particolare delicatezza).

1 Executive Summary

1.1. 'COVID-19-related epidemiological emergency': this is the wording to be found, albeit with some variations, throughout the Italian SA's 2020 Annual Report. The year 2020 will unquestionably be labelled as the pandemic year, and the relevant effects also impacted – which was bound to happen – the issues addressed by the IT SA along with the operation of the SA as such. Still, the SA has been working ceaselessly in a 'smart working' mode (see paras. 25.3 and 25.5) and only onsite inspection activities were unavoidably dropped (see Chapter 18). In fact, the activities by the SA skyrocketed especially in all areas that were somehow related to the health emergency including the activities within the European Data Protection Board (see para. 21.1) and in all supranational forums (see para. 21.3). From the very beginning of the pandemic, the Garante was 'captured' – and held in a grip that has not yet relented – by the multi-pronged strategy implemented by government to tackle the effects of the pandemic from a healthcare (Chapter 5) and economic and social (paras. 4.1 and 4.2) perspective. That strategy revolves largely on the (massive) processing of personal information, including highly sensitive data.

1.2. Se, in questa prospettiva, la punta dell'*iceberg* è stata rappresentata dal processo di "costruzione" (e co-produzione con le autorità sanitarie) del sistema di allerta Covid-19 (cd. *app* Immuni) (par. 5.1) – che nella volontarietà dell'adesione individuale ha avuto uno dei suoi tratti caratterizzanti, comune agli ordinamenti europei (e, in generale, alle democrazie occidentali) (cfr. par. 21.1) –, invero ogni istante della vita della nostra comunità, nella sua quotidianità vieppiù "dislocata" (e poi forzatamente rinserrata) su piattaforme digitali, ha sollevato questioni (di libertà) rispetto alle quali il Garante è stato chiamato a pronunciarsi. La migrazione forzata di larga parte delle nostre vite dalla dimensione materiale allo spazio virtuale (non meno reale), fenomeno già marcato nell'era pre-Covid, ha segnato un (forse irreversibile) punto di svolta: la virtualizzazione delle vite dei nostri giovani – riversate sui *social network* e scandite dalla didattica a distanza in scuole, di ogni ordine e grado, ed università (par. 4.3) – e di parte significativa del mondo del lavoro, con la generalizzazione, ovunque possibile, del cd. lavoro agile (par. 13.2), l'alimentazione dei (sempre più) numerosi e interconnessi *database* gestiti dal Sistema sanitario nazionale, come pure di quelli che raccolgono i destinatari delle più varie provvidenze economiche (cfr. par. 4.2) e dei benefici fiscali (par. 4.1) – nonché sovente dei rispettivi nuclei familiari –, hanno imposto una risposta pronta e scandita dal trattamento elettronico dei dati. Informazioni, spesso confluite in archivi fattisi massivi e soggetti a sempre più insidiosi *data breach* (cfr. cap. 16), che richiedono da parte di tutti gli attori una vigilanza attenta rispetto alle implicazioni sui diritti individuali.

1.2. The tip of the iceberg was made up of the process intended to 'build up' (and deploy jointly with health care authorities) the COVID-19 alert system – i.e., the so-called 'Immuni' app (see para. 5.1). One of the key features of that system was the voluntary nature of its enrolment mechanism, which actually applies across the EU and, generally speaking, in all Western democracies (see para. 21.1). However, the freedom dimension was challenged by every moment of our lives, which were already increasingly 'de-located' to digital platforms and ended up being forcibly kept within the boundaries of those platforms – and the Garante was called upon to have its voice heard on all of this. The forced migration of a substantial part of our lives from the material to the virtual dimension – which is however no less real – marked what is likely to be a final turning point in a process that was already on its way in the pre-COVID age. Youths' lives have become virtual on social networks and ended up being regulated by the distance learning and teaching relied upon by schools at all levels as well as by universities (see para. 4.3); in the employment sector, smart working and teleworking have been implemented to a significant degree whenever possible (see para. 13.2); an increasing number of interconnected databases handled by the National Health Service have been accumulating information including data on the recipients of multifarious benefits and allowances (see para. 4.2) also in the field of taxation (see para. 4.1), at times involving whole families. All of this has required taking steps and measures promptly, leveraging on the electronic processing of data that have often fed hefty filing systems, which in turn have been the subject of increasingly malicious data breaches (see Chapter 16) such as to require careful surveillance by all the stakeholders on account of the impact caused on the rights of individuals.

1.3. Entro questa cornice, la corretta configurazione dei sistemi informativi approntati (o potenziati) per far fronte agli interventi (di varia natura) posti in essere per contrastare la pandemia o attenuarne gli effetti (anche economici) è stata la chiave di volta dell'intervento del Garante. Principi di minimizzazione e finalità, principi della *privacy by design* e della *privacy by default*, valutazione di impatto e misure di sicurezza – parole chiave introdotte, ma più spesso solo rinverdite, dal RGPD –, lungi dall'essere riducibili ad una sorta di litania di adempimenti percepiti o "contrabbandati" come puramente burocratici, si sono confermati quali architravi per la corretta edificazione, rimessa anzitutto ai titolari del trattamento (sotto le insegne del principio di responsabilizzazione), di qualunque infrastruttura informativa, e certo di quelle messe in campo dal legislatore per accompagnare la risposta istituzionale agli effetti della pandemia.

Nella convinta consapevolezza che il "diritto alla protezione dei dati personali non appare […] come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale" (cfr. Corte di giustizia, 9 novembre 2010, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke e Eifert, punto 48; Corte di giustizia, 5 maggio 2011, C-543/09, Deutsche Telekom, punto 51), non devono allora essere buttate alle ortiche le ragioni fondative della protezione dei dati personali rievocate, nella loro semplicità, nel monito di Giovanni Buttarelli: "Dati uguale potere. […] È un potere nelle mani di una cerchia relativamente ristretta. La protezione dei dati serve a imbrigliare questo potere così da metterlo al servizio del diritto di ciascuno al libero sviluppo della personalità: il diritto di pensare liberamente, di avere segreti, di dire quello che si vuole, di stringere e mantenere rapporti" (Privacy 2030. Una nuova visione per l'Europa, 2020, p. 12, doc. web n. 9457003).

1.3. Against this backdrop, the focus of the Garante's action has been on the appropriate configuration of the information systems that have been implemented or enhanced as part of the efforts to tackle the pandemic and mitigate its effects also from the economic perspective. The principles of data minimization and purpose limitation, the principles of privacy by design and by default, data protection impact assessment and security measures are key notions that were introduced, but most often revamped, by the GDPR. They are far from being a sort of string of requirements to be regarded or passed off as merely bureaucratic in nature. In fact, they have been confirmed to be the foundations on which controllers should build up – in line with the accountability principle – any data processing infrastructure and most certainly any infrastructure to be deployed in order to support the public efforts in countering the effects of the pandemic.

Starting from the assumption that 'The right to the protection of personal data is not […] an absolute right, but must be considered in relation to its function in society' (see Court of Justice of the EU, 9 November 2010, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke and Eifert, point 48; Court of Justice of the EU, 5 May 2011, case C-543/09, Deutsche Telekom, point 51), one should refrain from throwing the basic rationale of data protection out of the window – as recalled by Giovanni Buttarelli in his writing: 'Data means power. […] Relatively few wield this power. Data protection aims to constrain it to serve the rights of people to develop their own personalities, have free space to think, keep secrets, speak freely, and form and maintain relationships.' (Privacy 2030. A New Vision for Europe, 2020, p. 12, web doc No 9457003).

1.4. Pur nel farsi di un nuovo capitolo del diritto dell'emergenza, oggi quella sanitaria, a tali principi ha fatto costantemente riferimento il Garante, rinnovatosi nella sua composizione con l'insediamento del Collegio eletto dal Parlamento il 14 luglio 2020. La stella polare che ha guidato le scelte dell'Autorità (e le indicazioni dalla stessa fornite) è rimasta quella della (faticosa) ricerca della salvaguardia dei diritti fondamentali delle persone, in particolare della dignità, della riservatezza e del diritto alla protezione dei dati personali, rifiutando (come già in passato rispetto ad altre "emergenze") di cadere nella trappola di sbrigativi aut-aut. Nel seguire (doverosamente) questa traiettoria, l'atteggiamento tenuto dall'Autorità è stato improntato ad una costante, leale e sollecita cooperazione istituzionale: lo attesta, se mai fosse necessario comprovarlo, l'intensa interlocuzione informale nei tavoli di lavoro (pur virtuali) e la serrata attività consultiva (con un elevato numero di pareri richiesti e non di rado ottenuti in tempi strettissimi, se non *ad horas*) rispetto ai più svariati interventi, in larga misura funzionali al contrasto degli effetti della pandemia (cfr. par. 3.1 e parte IV, tab. 2 e 3). Con soddisfazione, in relazione alla funzione "consulenziale" propria dell'Autorità nelle materie che incidono sulla protezione dei dati personali, si è registrata una più intesa interlocuzione nella fase di adozione di disposizioni rilevanti, anche di rango primario – in linea con la disciplina, sul punto innovativa, contenuta nel Regolamento generale in materia di protezione dei dati (cfr. artt. 36, par. 4, 57, par. 1, lett. *c*) e 58, par. 3, lett. *b*), del RGPD) –, ancorché non siano mancati casi nei quali l'interlocuzione con l'Autorità non è stata invece ricercata (profilo già evidenziato nella Relazione 2019, p. 6 e che torna quest'anno: cfr. par. 4.2.2, in relazione al tema dei *bonus* sociali, e par. 4.8, in materia di digitalizzazione della p.a.), taluni dei quali particolarmente significativi: si pensi, da ultimo,

1.4. Whilst writing a new chapter of state of emergency laws – currently sparked by a health emergency – the Garante has relied consistently on those principles. A new board of commissioners took the helm after being elected by Parliament on 14 July 2020. The compass used in all the decisions made by the Authority as well as in the guidance and measures it has been issuing has remained set on the (demanding) search for safeguards of the fundamental rights of individuals – in particular dignity, privacy and the right to the protection of personal data. As it was the case in the past on account of other types of 'emergency', the Garante took care not to fall a prey to the logic of irreconcilable dilemmas. In following this path, the stance taken by the Authority was one of unrelenting, fair, prompt cooperation with other public authorities. This is shown – suffice it to say here – by the in-depth informal exchanges that took place via numberless (virtual) meetings along with the multiple consultative activities that led to a high number of opinions rendered in many cases shortly after being requested – indeed in a few hours' time – regarding the most diverse measures, which were devised largely to counter the effects of the pandemic (see para. 3.1 and Part IV, Tables 2 and 3). It should be pointed out that the Garante was consulted more regularly and consistently prior to the issuing of substantial measures, including primary legislation, as part of the consultative role it is tasked with in all areas that relate to personal data protection. This is in line with the requirements laid down in the EU GDPR (see Articles 36(4), 57(1)(c), and 58(3)(b) thereof). However, there were cases where the Garante was actually not consulted – a shortcoming that was highlighted in the 2019 Annual Report as well, p. 6; regarding this year's Report, please see para. 4.2.2. as for the regulations granting social allowances and para. 4.8 as for the digitalisation of public administrative activities. In a

alla disciplina della certificazione verde per Covid-19 (cd. *green pass*) delineata dal decreto-legge del 22 aprile 2021, n. 52, che, in assenza di interventi correttivi, può determinare la violazione di rilevanti disposizioni del Regolamento (agli artt. 5, 6, par. 3, lett. *b*), 9, 13, 14, 25 e 32), come evidenziato dal Garante nel provvedimento di avvertimento del 3 maggio 2021, n. 104 (doc. web n. 9578184). Criticità, quelle evidenziate in questo caso, che oltre a risultare in violazione della legge, da un punto di vista formale, producono altresì l'effetto, sostanziale, di esporre a pregiudizio i diritti dei singoli, incardinando su basi normative malferme (sovente oggetto di successivi, dispendiosi, interventi correttivi) la conseguente azione amministrativa o lo sviluppo dell'iniziativa economica.

A questo riguardo è allora necessario individuare (ma in molti casi semplicemente affinare), dal punto di vista procedimentale, strumenti e modalità efficaci (con tempistiche appropriate) che consentano a Parlamento e Governo, ogni qual volta chiamati ad intervenire in ambiti che possano toccare (specie se su larga scala o con effetti significativi sulle libertà individuali) il diritto alla protezione dei dati personali, di trarre pieno vantaggio dalla cooperazione istituzionale con l'Autorità.

few cases, such shortcomings were especially remarkable: reference can be made to the recent regulations governing the so-called COVID-19 green pass as set out in decree No 52 of 22 April 2021. Without the amendments requested by the Garante, those regulations may ultimately be found to be in breach of the GDPR – in particular, of Articles 5, 6(3) (b), 9, 13, 14, 25 and 32 thereof – as emphasized by the Garante in its warning decision of 3 May 2021 (web doc No 9578184). On top of violating the provisions made in the law, the regulations in question would give rise substantively to violations of the rights of individuals and would undermine both administrative activities and entrepreneurial initiatives on account of their unsound foundations – which might require costly remedial measures to be implemented subsequently.

From this standpoint, there is a need to identify – or, in many cases, to fine-tune – effective procedural tools and mechanisms that can allow Parliament and Government to fully and timely benefit from the cooperation with the Garante whenever they are called upon to take measures that may impinge on the right to the protection of personal data – especially if those measures are wide-ranging in nature or can significantly impact the freedom of individuals.

1.5. La dimensione globale (quantomeno delle questioni legate al trattamento delle informazioni personali) è, da tempo ormai, l'habitat naturale delle autorità di protezione dei dati. Se il "confinamento" imposto dalla pandemia ha portato all'azzeramento delle missioni internazionali, l'attività del Garante non è però rimasta neanche per un istante confinata all'ambito nazionale. Le restrizioni per contenere la diffusione della pandemia hanno portato infatti ad una sorta di "normalizzazione" dell'uso massivo delle piattaforme di comunica-

1.5. The global dimension has long been the province of data protection authorities at least in connection with the issues related to the processing of personal information. The forced lockdown caused by the pandemic all but wiped out international missions, however the Garante's activities have not remained home-bound for a single moment. Indeed, the restrictions aimed at containing the spread of the pandemic brought about a sort of 'normalisation' of the massive use of remote communication platforms, which turned cooper-

zione da remoto con un'attività di cooperazione che, specie con riferimento ai lavori svolti nell'ambito del Comitato, da puntiforme si è trasformata in confronto costante, con una moltiplicazione (senza precedenti) delle occasioni di scambio (e di crescita) tra rappresentanti delle autorità di protezione dei dati (cfr. parte IV, tab. 19). Tale intensa attività trova riscontro nella copiosa documentazione attraverso la quale il Comitato ha continuato a fornire indicazioni per un'attuazione coerente del RGPD, sia con riguardo ai suoi più 'tradizionali' ambiti di intervento (cfr. par. 21.1), sia con riferimento alle eccezionali misure prese, a livello nazionale ed europeo, per la lotta alla pandemia, sottolineando più volte che qualunque misura anche restrittiva delle libertà adottata in un contesto eccezionale come quello in corso, debba essere proporzionata e limitata al periodo dell'emergenza. In questo novero vanno inserite le linee guida in materia di titolare e responsabile del trattamento e sulla nozione di consenso, i numerosi pareri resi sui requisiti di accreditamento degli organismi di monitoraggio dei codici di condotta e degli organismi di certificazione predisposti da diverse autorità di controllo (tra cui la nostra) e quelli necessari per l'approvazione, da parte delle medesime, delle regole vincolanti di impresa (Bcr).

E proprio in tema di trasferimenti di dati all'estero, non può non passare inosservata l'attenzione dedicata dal Comitato agli effetti sulle regole contenute nel Capo V del RGPD prodotti dalla sentenza Schrems II – con cui la Corte di giustizia ha confermato la validità delle clausole contrattuali tipo per il trasferimento di dati personali a responsabili del trattamento stabiliti in Paesi terzi, ma ha invalidato la decisione di adeguatezza della protezione offerta dal regime dello scudo UE-USA per la *privacy* – sull'utilizzo degli strumenti ivi previsti e lo sforzo volto a fornire indicazioni chiare in ordine alle misure supplementari da adottare, ove gli ordinamenti dei

ation activities from well-spaced events into a continuous dialogue especially within the framework of the European Data Protection Board. Thus, there was an (unprecedented) multiplication of the opportunities for exchanging (and acquiring) information among representatives from data protection authorities (see Part IV, Table 19). Such intensive exchanges are mirrored by the many documents through which the EDPB continued to provide guidance aimed at ensuring the consistent enforcement of the GDPR – both in respect of the exceptional measures implemented at domestic and EU level to counter the pandemic and with regard to more 'traditional' areas of activity (see para. 21.1). As to the former, the EDPB underlined repeatedly that any such measure, including those limiting the freedom of individuals, must be proportionate and limited to the duration of the emergency period even when adopted under exceptional circumstances. As to the latter, reference should be made to the guidelines on controllers and processors and on the notion of consent, to the many opinions rendered on the accreditation requirements of code of conduct monitoring bodies and the additional accreditation requirements for certification bodies as well as to the opinions the EPDB was required to give with a view to the approval of binding corporate rules by the competent supervisory authorities.

Still regarding data transfers to third countries, one cannot but highlight the attention paid by the EDPB to the effects that the Schrems II judgment produced on the rules in Chapter V of the GDPR regarding the transfer tools as envisaged therein. By the said judgment, the Court of Justice of the EU confirmed that the standard contractual clauses for the transfer of personal data to controllers in third countries retained their validity, however it invalidated the Commission's decision on the adequate protection afforded by the EU-US Pri-

Paesi terzi destinatari impongano agli importatori restrizioni tali da impedire il rispetto delle garanzie contenute negli strumenti stessi (parr. 17 e 21.1).

1.6. Sarebbe però limitativo (se non fuorviante) ritrarre l'impressione della pandemia (e delle questioni che intorno ad essa hanno ruotato) quale catalizzatore unico dell'attività del Garante e (tragico) "mattatore" nell'*annus horribilis* che abbiamo alle spalle. Ormai superata la prima fase della sperimentazione dei nuovi istituti introdotti con il RGPD, le risorse dell'Autorità sono assorbite in modo crescente nell'ambito della cooperazione europea, anzitutto attraverso la piattaforma IMI (cfr. parr. 12.9, 14.6 e 21.1 nonché, per indicatori numerici, la parte IV, tab. 10-12) tenuto anche conto del moltiplicarsi dei casi di rilevanza transfrontaliera e dei trattamenti effettuati dalle (poche e gigantesche) piattaforme e reti sociali che dominano la scena, con criticità che vanno via via emergendo: si pensi alla questione dell'accertamento dell'età *online*, oggetto dell'iniziativa del Garante nei confronti del colosso cinese TikTok (cfr. par. 9.4), alla tematica delle *fake news* (parr. 3.2 e 12.8) e agli interventi, ancora numerosi, in materia di deindicizzazione (par. 9.5).

In ambito economico, come già in passato (cfr. da ultimo Relazione 2019, p. 8), si sono evidenziate le (persistenti) forti criticità rispetto ai trattamenti effettuati per finalità di (tele)*marketing* – con la correlativa irrogazione di sanzioni amministrative pecuniarie particolarmente severe nel settore telefonico ed energetico (se ne dà conto, rispettivamente, ai parr. 11.1.1 e 11.1.2) – e si segnala, a conforto dell'azione da tempo intrapresa dall'Autorità (per una più ampia panoramica sul contenzioso giurisdizionale si rinvia al cap. 20), la recente autorevole

vacy Shield. The EDPB endeavoured to provide clear-cut guidance on the supplementary measures to be implemented if the legal systems of the data importers' third countries envisage limitations such as to prevent compliance with the safeguards set forth in the transfer tools at issue (see paras 17 and 21.1).

1.6. Still, it would be a very incomplete (or downright misleading) view of the Garante's work one that would depict the pandemic and the related issues as the sole catalyst of that work – making up the lion's share of the *annus horribilis* behind us. Having progressed past the initial testing of the new tools introduced by the GDPR, the Authority has been gaining momentum in developing cooperation at EU level – first and foremost, through the IMI platform (see paras. 12.9, 14.6 and 21.1 as well as the figures in Part IV, Table 10-12). Account should also be taken in this respect of the growing number of cross-border processing cases and the impact due to the processing activities performed by the giant IT platforms and social networks that are increasingly under the limelight along with all the attending criticalities. Reference can be made to the issue of online age verification, which was the subject of measures adopted by the Garante vis-à-vis TikTok (see para. 9.4); to fake news (see paras. 3.2 and 12.8); and to the many de-listing requests that are still being received (see para. 9.5).

Looking at business and entrepreneurial activities, there remained (like in the past – see the 2019 Annual Report, p. 8) major criticalities affecting telemarketing-related processing; indeed, hefty administrative fines were imposed on companies from the telecom and utilities sectors (see paras. 11.1.1 and 11.1.2, respectively). The actions the Garante has been waging since long were supported – see Chapter 20, for additional information on the relevant

conferma dell'illiceità delle campagne telefoniche di cd. "recupero consenso" da parte della Corte Suprema di cassazione (cfr. Sez. I, ord. 26 aprile 2021, n. 11019, che ha confermato l'impugnata sentenza del Tribunale di Milano del 5 maggio 2017, n. 5022 e il provv. 22 giugno 2016, n. 275, doc. web 5255159), come pure delle conseguenze sanzionatorie derivanti dall'abusiva attivazione di schede telefoniche all'insaputa degli interessati (cfr. Cass. civ., Sez. II, ord. 20 aprile 2021, n. 10368, confermativa dell'ordinanza-ingiunzione 18 aprile 2013, n. 204, doc. web n. 2691090).

Con riguardo alla materia, assai rilevante, dei codici di condotta, a compimento di un *iter* procedimentale articolato (comprensivo del parere favorevole del Comitato) è stato adottato il provvedimento contenente i requisiti per l'accreditamento a livello nazionale degli organismi di monitoraggio (strumento indispensabile per assicurare il corretto funzionamento dei codici di condotta, con procedimento definito nel settore delle informazioni commerciali e in prossimità di arrivo rispetto ai Sic) (par. 14.3). Nella prospettiva della cd. *accountability*, merita altresì ricordare l'adozione dei requisiti aggiuntivi per l'accreditamento (da parte di Accredia) degli organismi di certificazione, previo parere favorevole del Comitato (par. 14.7).

judicial cases – by the recent decision of the Italian Court of Cassation (No 11019 of 26 April 2021), which upheld the judgment by the Milan Court No 5022 of 5 May 2017 and the Garante's order No 275 of 22 June 2016 (web doc No 5255159) whereby the so-called 'consent recovery' campaigns implemented for telemarketing purposes had been found to be unlawful. The same applies to the judgment of the Italian Court of Cassation No 10368 of 20 April 2021, which upheld the Garante's order (No 204 of 18 April 2013) to pay the fine imposed on account of the unauthorised activation of telephone paycards without informing data subjects.

Regarding the important issue of codes of conduct, a complex procedural sequence was completed when the Garante's decision was adopted (upon the favourable opinion by the EDPB) approving the requirements for accreditation of monitoring bodies – which are indispensable in order to ensure the proper operation of codes of conduct. The adoption of a code of conduct in the business information sector was finalised and the code of conduct for credit bureaus is about to be released as well – see para 14.3.

Reference should also be made from the accountability perspective to the adoption of the additional requirements for the accreditation (by ACCREDIA) of certification bodies, further to the favourable opinion given by the EDPB (see para. 14.7).

1.7. La digitalizzazione crescente della società (cui la pandemia ha impresso un'accelerazione formidabile) e il programma di azione verso la trasformazione digitale – uno dei pilastri dell'azione politica già in essere a livello europeo (v. la Comunicazione della Commissione europea, *2030 Digital Compass: the European way for the Digital Decade*, Brussels, 9.3.2021, COM(2021) 118 final) e nazionale (con il Piano nazionale di ripresa e resilienza) – presuppone una

1.7. The fast-pace digitalisation of society was expedited forcibly by the pandemic and the action programme towards digital transformation is one of the pillars of the political initiatives at EU level – see the European Commission's Communication called '2030 Digital Compass: The European Way for the Digital Decade', Brussels, 09.03.2021, COM(2021)118-final - as well as at domestic level – see the National Recovery and Resilience Plan. A

solida educazione (al) digitale e, al contempo, una consapevolezza piena e diffusa (a livello individuale e sociale) dei "diritti digitali" della persona: tra questi una posizione centrale spetta al diritto alla protezione dei dati personali (sulla scorta dell'art. 8 della Carta dei diritti fondamentali), oggetto di significativi interventi da parte della Corte di giustizia, da ultimo (nuovamente) con una serie di sentenze (richiamate al cap. 24) in materia di dati di traffico (che tornano ad interrogare anche la tenuta del quadro ordinamentale nazionale), oltre alla più volte ricordata pronuncia che ha invalidato il *Privacy Shield* (cd. Schrems II).

E proprio per favorire un'accresciuta consapevolezza della dimensione dei diritti nella società tecnologica, l'Autorità, in varie forme, ha dato nuovo impulso alla propria comunicazione istituzionale (cfr. cap. 23) e continua ad investire (nei limiti delle risorse disponibili) su divulgazione e formazione (cfr. parr. 23.4 e 21.5). Ma il Garante pure richiede uno sforzo (responsabile) in capo ai titolari del trattamento, ribadendo l'importanza della figura del responsabile per la protezione dei dati (cfr. par. 4.6) e spingendosi a sollecitare con i propri provvedimenti, ove se ne siano ravvisati gli estremi, la promozione di adeguate iniziative formative da parte degli stessi titolari del trattamento: ciò è accaduto, ad esempio, nei confronti del Ministero dell'interno in relazione al personale, anche periferico, della Polizia di Stato, per assicurare, in un settore tanto delicato per la dinamica democratica (e oggetto della recente disciplina nazionale di recepimento della direttiva 680/2016), il puntuale rispetto dei diritti delle persone (cfr. par. 8.2). Nelle forme più opportune, un ampio coinvolgimento di scuole ed università (in relazione a queste ultime anche con riguardo alle facoltà tecnico-scientifiche) si fa sempre più urgente.

1.8. Il processo in atto – che si è provato a tratteggiare e che, quanto alle

key precondition for all of this is a robust education initiative focusing (and based) on digital technology along with the full awareness at both public and individual level of the 'digital rights' of individuals. A key role among those rights is played by the right to the protection of personal data as enshrined in Article 8 of the Charter of Fundamental Rights of the EU, which was the subject of authoritative decisions by the Court of Justice of the EU. Reference can be made in this regard to a few judgments (see Chapter 24) concerning traffic data – which actually question, once again, the soundness of the Italian legal framework in this respect – as well as to the aforementioned judgment invalidating the EU-US Privacy Shield, i.e., the so-called Schrems-II judgment.

It was exactly with a view to fostering awareness of the rights dimension in the technological society that the Garante revamped, in many ways, its media outreach activities (see Chapter 23) and continued to invest (the available) resources into dissemination and training (see paragraphs 23.4 and 21.5). At the same time, the Garante called upon controllers to act responsibly and reaffirmed the importance of data protection officers (see para. 4.6) – indeed, the Garante went so far as to urge controllers to implement suitable training activities in certain specific cases. This happened, for instance, with the Ministry of the Interior and the training of police officials in order to ensure full compliance with the rights of individuals in an area that is key for the functioning of democracy – also in the light of the legislation that was recently enacted to transpose directive 2016/680 (see para. 8.2). The wide-ranging involvement of schools and the academia in such awareness-raising initiatives – including technical and scientific departments at universities – is becoming increasingly urgent.

1.8. The ongoing developments as outlined here and detailed in the Annu-

attività realizzate, trova una dettagliata descrizione nella Relazione – richiede, sia consentito sottolinearlo, una cornice istituzionale solida e dotata di risorse strumentali e personali all'altezza della sfida: solo a queste condizioni il Garante (e, più in generale, le autorità di protezione dei dati) possono recare un contributo nell'interesse generale. Lo ribadisce, da ultimo, la Risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP)), nella quale si invitano espressamente "gli Stati membri a rispettare il loro obbligo giuridico a norma dell'articolo 52, paragrafo 4, di dotare le loro autorità di protezione dei dati di risorse sufficienti per consentire loro di svolgere il proprio lavoro nel miglior modo possibile e assicurare parità di condizioni a livello europeo nell'attuazione del GDPR" (punto 17).

Illusorio (se non pericoloso per una convivenza sociale democraticamente ordinata, prima ancora che per i diritti dei singoli) pensare alle sfide della cd. società dei dati – dei *big data*, oggetto di una (originale) prima indagine conoscitiva portata a termine nel 2020 dal Garante unitamente ad Agcm e Agcom (doc. web n. 9264297), e dell'intelligenza artificiale – prescindendo dal sistema valoriale sul quale, tra molte difficoltà e resistenze, l'Unione europea (e le Istituzioni nazionali con essa operanti) ha cercato di coniugare progresso tecno-scientifico e sociale e sviluppo integrale della persona.

al Report require – this must be pointed out – a sound organisational framework along with human and financial resources that can tackle the many challenges before us. Only if these conditions are fulfilled will the Garante – and all supervisory authorities in general – be in a position to contribute to the public interest. This was recently reaffirmed by the European Parliament's Resolution of 25 March 2021 on the Commission Evaluation Report on implementation of the GDPR two years after its application (2020/2717(RSP)), which explicitly called 'on Member States, therefore, to comply with their legal obligation under Article 52(4) to allocate sufficient funds to their DPAs to allow them to carry out their work in the best way possible and to ensure a European level playing field for the enforcement of the GDPR'.

One should not delude oneself into imagining that the challenges of the data society – from big data, which were the subject of an (innovative) fact-finding survey carried out in 2020 by the Garante along with the Italian Antitrust and Communications Safeguards Authorities, up to artificial intelligence – can be addressed without taking account of the framework of values through which the European Union (and the national authorities working under its aegis) have been endeavouring to reconcile technological, scientific and social advancements with the full-fledged, unimpaired development of individuals. Indeed, such a delusion would be putting at risk the democratic foundations of our social order even apart from and beyond endangering the rights of individuals.

2 Il quadro normativo in materia di protezione dei dati personali

Numerosi i provvedimenti normativi con riflessi sulla protezione dei dati personali approvati nel 2020: fra questi, al fine di offrirne una ricognizione sintetica ma tale da rendere conto dell'ampiezza e dell'eterogeneità delle materie che rientrano nell'area di interesse dell'Autorità e che sono comunque suscettibili di incidere sulla materia della protezione dei dati personali, si menzionano in particolare quelli di seguito indicati.

2.1. *Le leggi e i decreti-legge*

Per quanto riguarda le leggi e i decreti-legge, ci si riferisce ai seguenti:

Legge di bilancio 2021

1) la legge 30 dicembre 2020, n. 178, recante il bilancio di previsione dello Stato per l'anno finanziario 2021 e il bilancio pluriennale per il triennio 2021-2023, delle cui disposizioni si segnalano, in particolare:

a) i commi 227 e 228 dell'art. 1 che, mediante l'aggiunta del comma 3-*bis* all'art. 4, d.lgs. 5 agosto 2015, n. 127 (Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni), prevedono che l'Agenzia delle entrate metta a disposizione dei contribuenti una piattaforma telematica dedicata alla compensazione di crediti e debiti derivanti da transazioni commerciali, in modo tale da produrre i medesimi effetti dell'estinzione dell'obbligazione ai sensi del codice civile, demandando l'individuazione delle modalità di attuazione e delle condizioni di servizio di tale sistema a un decreto del Ministro della giustizia, da adottarsi sentito il Garante;

b) il comma 621, secondo il quale, nell'ottica della continuità della gestione del sistema di allerta Covid-19 (cd. *app* Immuni), le attività dirette a garantire lo sviluppo, l'implementazione e il funzionamento della relativa piattaforma (di cui all'art. 6, d.l. 30 aprile 2020, n. 28, su cui v. *infra* par. 5.1) nel 2021 saranno realizzate dalla competente struttura per l'innovazione tecnologica e l'innovazione della Presidenza del Consiglio dei ministri;

c) il comma 623 che, al fine di ridurre il divario digitale e favorire la fruizione della didattica a distanza, prevede l'assegnazione in comodato gratuito di un dispositivo elettronico dotato di connettività per un anno o un *bonus* di equivalente valore da utilizzare per le medesime finalità ai soggetti appartenenti a nuclei familiari con un reddito Isee non superiore a 20.000 euro annui, con almeno uno dei componenti iscritti a un ciclo di istruzione scolastico o universitario non titolari di un contratto di connessione internet o di un contratto di telefonia mobile, che si dotino del Sistema pubblico di identità digitale (Spid);

d) il comma 1097, concernente il cd. *cashback*, secondo il quale, modificando il comma 288 dell'art. 1, l. 27 dicembre 2019, n. 160 (legge di bilancio 2019), i rimborsi attribuiti per gli acquisti con strumenti di pagamento elettronici non concorrono a formare il reddito del percipiente. Il Garante è stato consultato dal Mef sullo schema di regolamento recante la disciplina di tale programma di rimborso e incentivo all'utilizzo di pagamenti elettronici, il cui testo era stato aggiornato, rispetto alla versione originariamente trasmessa, per recepire le indicazioni fornite dall'Autorità nel corso di interlocuzioni intercorse con rappresentanti del Dicastero, di PagoPA

s.p.a. e di Consap s.p.a., al fine di conformare il regolamento alle garanzie previste dalla normativa europea e nazionale di protezione dati (cfr. parr. 3.1.4 e 4.1.4);

e) i commi 957 e 958 i quali, nell'ambito delle misure finalizzate alla prevenzione dell'assenteismo dei dipendenti pubblici, prevedono rispettivamente, il primo, che vengano attribuite alla Presidenza del Consiglio dei ministri le risorse disponibili in conto residui attualmente destinate per tale azione di contrasto e, il secondo, l'abrogazione dei commi da 1 a 4 dell'art. 2, l. n. 56/2019 (cd. Concretezza). I due commi abrogati prevedevano l'introduzione di sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi per i dipendenti delle amministrazioni pubbliche ai fini della verifica dell'osservanza dell'orario di lavoro, ad esclusione del personale in regime di diritto pubblico, dei dipendenti titolari di un rapporto di lavoro agile nonché del personale degli istituti scolastici ed educativi.

Il decreto-legge cd. Ristori

2) Il decreto-legge 28 ottobre 2020, n. 137, recante ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da Covid-19 (cd. Ristori), convertito dalla legge 18 dicembre 2020, n. 176. Nel provvedimento sono confluiti anche i successivi decreti-legge Ristori-*bis* (d.l. 9 novembre 2020, n. 149), Ristori-*ter* (d.l. 23 novembre 2020, n. 154) e Ristori-*quater* (d.l. 30 novembre 2020, n. 157). Fra le disposizioni del decreto – per lo più volte a riconoscere contributi a fondo perduto per imprese e altri soggetti la cui attività è stata fortemente compromessa dalla crisi connessa alla pandemia – risultano di particolare interesse gli artt. 18, 19 e 20, in materia di salute e sicurezza, che si illustrano brevemente di seguito. Premesso che l'art. 18 ha consentito l'esecuzione di tamponi antigenici rapidi anche da parte dei medici di medicina generale e dei pediatri di libera scelta, l'art. 19 autorizza i professionisti a raccogliere le informazioni (per ciascun assistito) sui tamponi effettuati e i relativi esiti sul referto elettronico, rendendoli immediatamente disponibili attraverso il Sistema tessera sanitaria sia all'assistito (in caso di esito positivo o negativo), anche mediante il Fascicolo sanitario elettronico (Fse), sia alle Asl di competenza (in caso di solo esito positivo). Sul referto elettronico sono presenti in chiaro i dati di contatto, imprescindibili per adottare i provvedimenti di sanità pubblica (isolamento e quarantena) nonché per mettere in atto le operazioni di tracciamento dei relativi contatti. La disposizione prevedeva che dovesse essere acquisito il parere del Garante in merito alle modalità attuative delle predette disposizioni, da adottarsi di concerto tra Mef e Ministero della salute; il Garante ha reso parere favorevole sul relativo schema di decreto, poi adottato il 3 novembre 2020 e pubblicato nella G.U. n. 276 del 5 novembre 2020 (parere 3 novembre 2020, n. 215, doc. web n. 9563445: cfr. par. 5.4). L'art. 20 prevede, invece, che il Ministero della salute attivi un servizio nazionale di supporto telefonico e telematico alle persone risultate positive al virus Covid-19, che hanno avuto contatti stretti o casuali con soggetti risultati positivi o che hanno ricevuto una notifica di allerta attraverso l'applicazione Immuni (cfr. *infra*), i cui dati sono resi accessibili per caricare il codice chiave in presenza di un caso di positività. A tal fine, i dati relativi ai casi diagnosticati di positività al virus sono resi disponibili al menzionato servizio nazionale, anche attraverso il Sistema tessera sanitaria ovvero tramite sistemi di interoperabilità. Il servizio nazionale di risposta telefonica è stato istituito con ordinanza del 19 dicembre 2020, n. 34 del Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19, sul cui schema il Garante ha reso parere favorevole (provv. 17 dicembre 2020, n. 273, doc. web n. 9516719: cfr. par. 5.1.4). Il decreto introduce, inoltre, specifiche misure per il settore giustizia (cfr. artt. 23-27). In tali disposizioni si prevede l'utilizzo di strumenti processuali telematici che consentano, per quanto possibile, l'esercizio della giurisdizione pena-

le, amministrativa e tributaria senza rischi per tutti gli operatori interessati, con la previsione di istituti idonei a consentire una gestione più flessibile anche nell'ambito penitenziario. Si segnalano, infine: l'art. 30 (cd. Svuota carceri) che, nel caso di detenzione domiciliare, prevede che debba essere sempre disposta "l'applicazione di procedure di controllo mediante mezzi elettronici o altri strumenti tecnici" (cd. braccialetti elettronici) per prevenire il rischio concreto di fughe e di reiterazione di condotte delittuose; l'art. 31, che detta apposite disposizioni per consentire lo svolgimento delle elezioni degli organi territoriali e nazionali degli ordini professionali vigilati dal Ministero della giustizia con modalità telematiche da remoto.

Misure di contrasto all'utilizzo distorto della rete

3) Il decreto-legge 21 ottobre 2020, n. 130, recante disposizioni urgenti in materia di immigrazione e protezione internazionale, nonché misure di contrasto all'utilizzo distorto del web e di disciplina del Garante nazionale dei diritti delle persone private della libertà personale (cd. Sicurezza), convertito dalla legge 18 dicembre 2020, n. 173. Di particolare interesse risulta l'art. 12, per il quale, al fine di rafforzare la prevenzione e il contrasto dei reati in materia di traffico e altre condotte aventi ad oggetto sostanze stupefacenti, l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'art. 14, comma 2, l. 3 agosto 1998, n. 269, forma un elenco, da tenere costantemente aggiornato, dei siti web che possono essere utilizzati per commettere uno o più di tali reati con l'impiego di sistemi informatici o mezzi di comunicazione telematica ovvero attraverso reti di telecomunicazione disponibili al pubblico. Tale elenco è notificato ai fornitori di connettività alla rete internet (cd. *provider*) affinché impediscano l'accesso agli stessi. A garanzia dell'osservanza dell'obbligo gravante sui fornitori di rete di inibire entro sette giorni l'accesso ai siti web segnalati dai competenti organi di polizia, il comma 2 della disposizione introduce una sanzione amministrativa pecuniaria, alla cui irrogazione provvede il Mise.

Norme di semplificazione e digitalizzazione dei procedimenti amministrativi

4) Il decreto-legge 16 luglio 2020, n. 76, recante misure urgenti per la semplificazione e l'innovazione digitale (cd. Semplificazioni), convertito con la legge 11 settembre 2020, n. 120, adottato dal Governo in chiave di ausilio alla ripresa del Paese e volto alla semplificazione dei procedimenti amministrativi, alla digitalizzazione della p.a. nonché al sostegno all'economia verde e all'attività di impresa. Tra le disposizioni di interesse si segnalano, in particolare, le seguenti:

a) l'art. 12, che prevede modifiche alla l. 7 agosto 1990, n. 241, per rendere effettivi alcuni istituti, perseguire talune finalità già insite nella legge e ridurre i tempi dei procedimenti. In primo luogo, viene integrato l'art. 1, l. n. 241/1990, disponendo che i rapporti tra cittadini e p.a. siano improntati al principio della collaborazione e della buona fede, con l'obbligo per le p.a. statali di ridurre i termini dei procedimenti di rispettiva competenza. Al fine di incentivare il rispetto dei termini procedimentali nonché di garantire la piena operatività dei meccanismi di silenzio assenso, con il nuovo comma 8-*bis* dell'art. 2, l. n. 241/1990, viene stabilita l'inefficacia di alcuni provvedimenti adottati fuori termine. Un secondo gruppo di disposizioni introduce misure atte a favorire la partecipazione di singoli e imprese al procedimento amministrativo telematico, consentendosi, in sostanza, l'accesso agli atti e l'esercizio dei diritti tramite il punto di accesso telematico gestito da PagoPA attraverso una particolare applicazione denominata APP IO. Con ulteriori novelle alla legge n. 241/1990 in materia di attività consultiva delle pubbliche amministrazioni si prevede che, in caso di decorrenza del termine senza che sia stato comunicato il parere, ancorché si tratti di un parere obbligatorio, l'amministrazione richiedente procede indipendentemente dallo stesso. Infine, con le modifiche all'art. 18, l. n. 241/1990 si prevede che le dichiarazioni di cui agli artt. 46 e 47, d.P.R. n. 445/2000, ovvero l'acquisizione d'ufficio di dati e documenti da parte delle pubbliche amministrazioni,

sostituiscano ogni tipo di documentazione comprovante tutti i requisiti soggettivi ed oggettivi richiesti dalla normativa di riferimento, fatto comunque salvo il rispetto delle disposizioni antimafia e delle misure di prevenzione di cui al decreto legislativo 6 settembre 2011, n. 159;

b) l'art. 17-*bis*, il quale novella la disciplina concernente l'accesso alle informazioni presenti nell'Anagrafe tributaria da parte degli enti locali e dei soggetti affidatari del servizio di riscossione. In base a tale disposizione gli enti e i soggetti in parola possono accedere anche ai dati di cui all'art. 7, comma 6, d.P.R. n. 605/1973, registrati nel cd. Archivio dei rapporti finanziari (Arf). Si tratta dei dati identificativi (compreso il codice fiscale) di ogni soggetto che intrattenga qualsiasi rapporto o effettui – anche per conto o a nome di terzi – qualunque operazione di natura finanziaria (ad eccezione dei bollettini di conto corrente postale di importo unitario inferiore a 1.500 euro) con operatori finanziari, quali banche, Poste italiane, intermediari finanziari, imprese di investimento, organismi di investimento collettivo del risparmio e società di gestione del risparmio;

c) l'art. 24, in materia di cittadinanza digitale e accesso ai servizi digitali della pubblica amministrazione, che apporta modifiche al Cad in tema di identità, domicilio digitale e accesso ai servizi digitali. In particolare, la disposizione estende la possibilità di utilizzare i servizi pubblici erogati in rete tramite la propria identità digitale, precisando – quale misura di semplificazione – che l'accesso al domicilio digitale avvenga tramite dispositivi mobili anche attraverso il punto di accesso telematico previsto dall'art. 64-*bis* del Cad. Tali modifiche mirano a consolidare la funzione di punto di accesso telematico ai servizi pubblici dell'APP IO, applicazione gestita da PagoPA, società interamente partecipata dal Mef, prevedendo che le p.a. rendano i propri servizi fruibili in rete su dispositivi mobili anche attraverso tale applicazione. Ai fini dell'esposizione di tutti i servizi su APP IO, si aggiunge al citato art. 64-*bis*, il comma 1-*quater*, che impone ai soggetti di cui all'art. 2, comma 2, lett. *a*), del Cad (e quindi anche alle autorità indipendenti ivi indicate) di avviare i progetti di trasformazione digitale entro il 28 febbraio 2021. Di interesse in materia di protezione dei dati personali risultano poi le modifiche all'art. 6-*quinquies* del Cad, sul fenomeno dell'invio di comunicazioni indesiderate. La norma sostituisce l'attuale divieto di utilizzo degli indirizzi per finalità "diverse da quelle aventi valore legale" ovvero estranee alla finalità di erogazione di servizi pubblici, con il divieto di utilizzo dei medesimi per l'invio di comunicazioni commerciali come definite dall'art. 2, comma 1, lett. *f*), d.lgs. n. 70/2003. In pratica, tale modifica comporta che il divieto dell'uso del domicilio digitale senza il preventivo consenso del destinatario si riferisce non solo ai soggetti cui si applica il Cad, ma a qualunque mittente. Si chiarisce altresì che il divieto attiene appunto all'invio, senza il consenso dei destinatari, di comunicazioni commerciali di carattere promozionale e di materiale pubblicitario estraneo alle finalità istituzionali del mittente. Le conseguenze sanzionatorie per il caso di violazione del divieto dell'uso del domicilio digitale senza consenso sono disciplinate dal medesimo decreto legislativo n. 70/2003 nonché dal RGPD. Con il comma 3 dell'articolo, infine, si prevede che al sistema Scipafi (Sistema centralizzato informatico di prevenzione amministrativa del furto di identità) di cui al decreto legislativo 13 agosto 2010, n. 141, possano aderire anche i gestori dell'identità digitale di cui all'art. 64 del Cad, al fine di effettuare le verifiche propedeutiche al rilascio delle credenziali di accesso relative al sistema Spid;

d) l'art. 26, che definisce le modalità di funzionamento della piattaforma digitale con le quali le pubbliche amministrazioni possono notificare i propri atti, provvedimenti, avvisi e comunicazioni a singoli e imprese. L'autenticazione alla piattaforma ai fini dell'accesso (anche tramite l'APP IO) avviene tramite le piattaforme abilitanti

già sviluppate: lo Spid e la Carta d'identità elettronica (Cie). La definizione di tutti gli aspetti di dettaglio relativi al funzionamento della piattaforma è rimessa ad uno o più decreti del Presidente del Consiglio dei ministri, o del Ministro delegato per l'innovazione tecnologica e la digitalizzazione, sentito il Garante;

e) l'art. 29, che apporta ulteriori modifiche alla legge 9 gennaio 2004, n. 4, recante disposizioni per favorire l'accesso delle persone con disabilità agli strumenti informatici. Di particolare interesse è la realizzazione di una piattaforma unica nazionale informatica di targhe associate a permessi di circolazione dei titolari di contrassegni, istituita presso il Ministero delle infrastrutture e dei trasporti, nell'ambito dell'archivio nazionale dei veicoli previsto dall'art. 226 del codice della strada (d.lgs. 30 aprile 1992, n. 285) per consentire la verifica delle targhe associate ai permessi di circolazione rilasciati ai sensi dell'art. 381, comma 2, d.P.R. 16 dicembre 1992, n. 495. Detta disposizione è in larga parte frutto della collaborazione del Garante con i competenti uffici del Ministero. Dal punto di vista attuativo, si precisa che nella piattaforma confluiranno informazioni che sono già detenute dai comuni che rilasciano i permessi di sosta e di transito nelle zone a traffico limitato per le persone con disabilità. Si demanda a un decreto del Ministro delle infrastrutture e dei trasporti l'individuazione delle procedure per la gestione della piattaforma, previo parere del Garante e nel rispetto delle prescrizioni adottate dall'Autorità ai sensi dell'art. 2-*quinquiesdecies* del Codice;

f) l'art. 30, che interviene in materia anagrafica introducendo misure di semplificazione volte ad accelerare l'attuazione dell'Agenda digitale e la trasformazione digitale del Paese. A tal fine, vengono apportate modifiche all'art. 62 del Cad e al regolamento anagrafico della popolazione residente (d.P.R. 30 maggio 1989, n. 223), prevedendo la realizzazione di un servizio, offerto tramite l'Anagrafe nazionale della popolazione residente (Anpr), che consenta la produzione dei certificati anagrafici in modalità telematica. Tale sistema garantisce, tramite il sigillo elettronico qualificato, la certezza dell'Anpr quale sorgente autoritativa emanante i certificati anagrafici. Viene inoltre prevista l'attribuzione di un codice identificativo unico in Anpr al fine di contraddistinguere ogni soggetto registrato e facilitare l'interoperabilità e l'integrazione dell'Anagrafe con le banche dati delle p.a. e dei gestori di servizi pubblici. Il nuovo comma 6-*bis* dell'art. 62 del Cad prevede che con uno o più decreti del Ministro dell'interno, sentito il Garante, sia assicurato l'adeguamento tecnico ed evolutivo della piattaforma di funzionamento dell'Anpr, anche rispetto al piano per il graduale subentro dell'Anpr alle anagrafi della popolazione residente (d.P.C.M. 10 novembre 2014, n. 194);

g) l'art. 34, che sostituisce il vigente art. 50-*ter* del Cad, concernente la piattaforma digitale nazionale, affidando la gestione della stessa non più al Commissario straordinario per l'Agenda digitale, ma alla Presidenza del Consiglio dei ministri. L'intervento normativo è volto a favorire la condivisione di dati e informazioni prevedendo la messa a disposizione e l'utilizzo, da parte dei soggetti accreditati, di interfacce di programmazione delle applicazioni (Api). Le pubbliche amministrazioni e gli altri soggetti di cui all'art. 2, comma 2, del Cad, sono tenuti ad accreditarsi alla piattaforma, a sviluppare le interfacce e a rendere disponibili le proprie banche dati senza nuovi o maggiori oneri per la finanza pubblica. Sulla struttura e sul funzionamento di tale piattaforma l'Autorità aveva espresso a suo tempo forti perplessità per le rilevanti ricadute in punto di protezione dati (cfr. nota del Garante al Presidente del Consiglio dei ministri 22 gennaio 2018, doc. web n. 8456134, e parere 22 maggio 2018 reso sullo schema di decreto legislativo di "attuazione" del regolamento (UE) 679/2016, poi d.lgs. n. 101/2018, doc. web n. 9163359). Nonostante le modifiche apportate alla disposizione normativa in parola, non possono che confermar-

si le perplessità circa la concentrazione di una siffatta quantità di dati in capo ad un unico soggetto (PagoPA) e comunque sulla genericità della prevista condivisione di dati fra le diverse amministrazioni coinvolte nella piattaforma. La norma rimette poi ad AgID, sentito il Garante, l'adozione di linee guida per definire gli standard tecnologici e i criteri di sicurezza, di accessibilità, di disponibilità e di interoperabilità per la gestione della piattaforma, e demanda ad un decreto di natura non regolamentare adottato dal Presidente del Consiglio dei ministri, sentito il Garante, la fissazione della strategia nazionale dati, con l'individuazione delle tipologie, dei limiti, delle finalità e delle modalità di messa a disposizione della Presidenza del Consiglio dei dati aggregati e anonimizzati detenuti dai titolari del trattamento.

Il decreto-legge Rilancio

5) Il decreto-legge 19 maggio 2020, n. 34, recante misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da Covid-19 (cd. Rilancio), convertito dalla legge 17 luglio 2020, n. 77, che interviene, in modo trasversale, prevedendo misure volte alla tutela delle famiglie e dei lavoratori, nonché alla salvaguardia e al sostegno delle imprese e dei liberi professionisti. Le disposizioni di maggior interesse sotto il profilo della protezione dei dati personali sono contenute nel Titolo I dedicato alla salute e alla sicurezza delle persone. Esse sono, peraltro, il frutto di una serie di interlocuzioni dell'Autorità con i competenti uffici del Ministero della salute, dell'Istituto superiore di sanità e dell'Istat che hanno portato a condividere i testi poi presentati in Consiglio dei ministri (cfr. par 3.1.2). In particolare, in materia di sanità si segnalano:

a) l'art. 7, concernente le metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione, per il quale il Ministero della salute, nell'ambito dei compiti e delle funzioni relative a indirizzi generali e di coordinamento in materia di prevenzione e cura delle malattie, nonché di programmazione tecnico sanitaria, può trattare, ai sensi dell'art. 2-*sexies*, comma 2, lett. *v*), del Codice e nel rispetto del RGPD, dati personali, anche relativi alla salute degli assistiti, raccolti nei sistemi informativi del Ssn (nonché, nell'originaria formulazione, poi venuta meno, dei dati reddituali riferiti all'interessato e al suo nucleo familiare) per lo sviluppo di metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione (cfr. par. 5.12.1);

b) l'art. 11, recante modifiche all'art. 12, d.l. n. 179/2012, istitutivo del Fse, al fine di velocizzare e snellire le procedure per l'adozione, su tutto il territorio nazionale, di tale importante strumento, che viene ulteriormente potenziato, senza alcun arretramento in termini di garanzie per i pazienti;

c) l'art. 12, recante disposizioni per facilitare e accelerare il flusso informativo dei dati su nascite e decessi (di cui all'art. 62, comma 6, lett. *c*), del Cad), il quale stabilisce che le strutture sanitarie, i medici, i medici necroscopi o altri sanitari delegati, inviino con modalità telematica (anziché con modulistica cartacea) al Sistema tessera sanitaria del Mef i dati relativi ai suddetti eventi (avviso di decesso; certificato necroscopico; denuncia della causa di morte; attestazione di nascita; dichiarazione di nascita);

d) l'art. 13, finalizzato a consentire all'Istat di effettuare rilevazioni statistiche nel Programma statistico nazionale e disporre così di dati affidabili e completi sul sistema economico e produttivo nazionale e sui fenomeni sociali, epidemiologici e ambientali, anche a supporto degli interventi di contrasto all'emergenza sanitaria nonché di quelli finalizzati alla gestione della fase di ripresa (a titolo esemplificativo: per valutare il senso di isolamento degli anziani, l'interruzione delle cure su malattie croniche per paura del contagio, i disturbi del sonno, la "reazione" di soggetti in regime di detenzione, ecc.).

Il menzionato decreto n. 34/2020 reca inoltre disposizioni che prevedono misure

di sostegno alle imprese e alle persone fisiche e altre norme in materia di digitalizzazione di funzioni pubbliche e di servizi, tra le quali si segnalano in particolare:

e) l'art. 82, che introduce il Reddito di emergenza (Rem), quale misura di sostegno al reddito per i nuclei familiari in conseguenza dell'emergenza epidemiologica da Covid-19, erogato dall'Inps;

f) l'art. 83, che impone ai datori di lavoro pubblici e privati – fino alla data di cessazione dello stato di emergenza – di assicurare la sorveglianza sanitaria eccezionale dei lavoratori maggiormente esposti a rischio di contagio, in ragione dell'età o della condizione di rischio derivante da immunodepressione, anche da patologia Covid-19 o da esiti di gravi patologie o dallo svolgimento di terapie salvavita;

g) l'art. 99, che al fine di monitorare gli effetti sul mercato del lavoro dell'emergenza epidemiologica e delle misure di contenimento adottate, istituisce presso il Ministero del lavoro e delle politiche sociali l'Osservatorio nazionale per il mercato del lavoro, con il compito di studiare ed elaborare i dati relativi all'occupazione, definire i fabbisogni generati dalle trasformazioni del mercato del lavoro e individuare le azioni e gli interventi da adottare. L'articolo demanda ad un decreto del Ministro, sentito il Garante, il compito di individuare i dati, anche individuali, che potranno essere trattati e le amministrazioni titolari del trattamento (i dati così individuati potranno essere utilizzati dal Ministero al solo fine di elaborazione statistica);

h) l'art. 135, che reca disposizioni in materia di giustizia tributaria sostituendo integralmente l'art. 16, comma 4, d.l. n. 119/2019, relativo alle procedure da seguire per lo svolgimento dell'udienza a distanza, sia pubblica sia in camera di consiglio. La disposizione prevede che le regole tecniche e l'individuazione delle Commissioni tributarie presso le quali è possibile attivare l'udienza a distanza sono demandate ad un decreto direttoriale del Dipartimento delle finanze sul quale, come previsto, il Garante ha reso parere (provv. 15 ottobre 2020, n. 186, doc. web n. 9471537: cfr. par. 3.1.4);

i) l'art. 148, che modifica la disciplina degli indici sintetici di affidabilità fiscale (Isa) prevedendo che, per l'applicazione degli stessi, la competente società a partecipazione pubblica definisca specifiche metodologie basate su analisi ed elaborazioni utilizzando, anche attraverso l'interconnessione e la pseudonimizzazione, direttamente le banche dati già disponibili per l'Amministrazione finanziaria, l'Inps, l'Ispettorato nazionale del lavoro e l'Istat nonché i dati e gli elementi acquisibili presso istituti ed enti specializzati nella ricerca e nell'analisi economica. È altresì previsto che potranno essere individuati ulteriori dati e informazioni necessari per migliorare la valutazione dello stato di crisi individuale;

l) l'art. 176, che riconosce il cd. *bonus* vacanze, rimettendone le modalità attuative ad un provvedimento del Direttore dell'Agenzia delle entrate, sentito l'Inps e previo parere del Garante (cfr. par. 4.1.3);

m) l'art. 234, in materia di istruzione, il quale prevede lo stanziamento di fondi da impiegare per la realizzazione di un sistema informativo integrato per il supporto alle decisioni nel settore dell'istruzione scolastica, per la raccolta, la sistematizzazione e l'analisi multidimensionale dei relativi dati, nonché per il supporto alla gestione giuridica ed economica del personale, anche attraverso le tecnologie dell'intelligenza artificiale, nonché per la didattica a distanza;

n) l'art. 263, che, al fine di assicurare la continuità dell'azione amministrativa e la celere conclusione dei procedimenti avviati su istanza o segnalazioni dei privati, impone alle amministrazioni pubbliche di adeguare le misure sul lavoro agile previste dall'art. 87, comma 1, lett. *a*), d.l. 17 marzo 2020, n. 18 (cd. Cura Italia), alle esigenze della progressiva riapertura di tutti gli uffici pubblici e a quelle dei singoli e delle imprese, organizzando il lavoro dei propri dipendenti e l'erogazione dei servizi

attraverso una maggiore flessibilità dell'orario di lavoro, rivedendone l'articolazione giornaliera e settimanale, introducendo modalità di interlocuzione programmata con l'utenza, anche attraverso soluzioni digitali e non in presenza, quindi per telefono o videoconferenza o (semplicemente) per mezzo di *e-mail* e Pec.

Indagine di sieroprevalenza

6) Il decreto-legge 10 maggio 2020, n. 30, recante misure urgenti in materia di studi epidemiologici e statistiche sul Sars-Cov-2, convertito dalla legge 2 luglio 2020, n. 72. Il decreto, composto da un unico articolo, al fine di disporre con urgenza di studi epidemiologici e di statistiche affidabili e complete sullo stato immunitario della popolazione, "autorizza" il trattamento di dati personali, anche genetici e relativi alla salute, per fini statistici e di studi scientifici nel settore della sanità pubblica, nell'ambito di un'indagine di sieroprevalenza condotta congiuntamente dai competenti uffici del Ministero della salute e dall'Istat in qualità di titolari del trattamento. A questo scopo tali Enti si avvalgono di un'apposita piattaforma informatica istituita presso il Ministero. La base giuridica del trattamento è individuata negli artt. 9, par. 2, lett. *g*) e *j*), e 89 del RGPD, nonché nell'art. 2-*sexies*, comma 2, lett. *cc*), del Codice. In tale quadro è consentito all'Istat di individuare i campioni casuali di individui da sottoporre a indagine, i cui dati anagrafici e il cui codice fiscale saranno trasmessi alla piattaforma. Il Ministero è, a sua volta, abilitato a richiedere ai fornitori dei servizi telefonici, che sono tenuti a dare riscontro, i recapiti degli utenti che dovessero rientrare nei campioni. Si prevedono le regole per la raccolta e le modalità di conservazione dei campioni, oltre che i tempi della loro conservazione, e viene individuata quale banca biologica "depositaria" quella dell'Inmi (Spallanzani), parte dei *network* nazionali ed internazionali dei Centri risorse biologiche e riconosciuta all'interno delle biobanche Irccs dal Ministero della salute. Tale Dicastero viene indicato quale titolare del trattamento dei dati relativi ai campioni biologici conservati nella banca. L'accesso ai dati sarà effettuato esclusivamente per il perseguimento delle finalità di ricerca individuate dal decreto-legge, nell'ambito di progetti congiunti con il Ministero. Sullo schema della disposizione normativa, presumibilmente diverso da quello approvato dal Consiglio dei ministri, il Garante ha reso parere in data 4 maggio 2020, n. 82 (cfr. parr. 3.1.2 e 5.3) e, in seguito ad esso, sono state avviate interlocuzioni tra gli uffici del Ministero, dell'Istat, della Protezione civile e dell'Autorità che hanno consentito una riformulazione della disposizione al fine di superare i rilievi evidenziati.

***App* Immuni**

7) Il decreto-legge 30 aprile 2020, n. 28, recante misure urgenti in materia di intercettazioni di conversazioni e comunicazioni, di ordinamento penitenziario e di giustizia civile, amministrativa e contabile, nonché per l'introduzione del sistema di allerta Covid-19, convertito dalla legge 25 giugno 2020, n. 70 (cd. decreto Giustizia). In particolare, l'art. 6 (inserito nel Capo II recante misure urgenti per l'introduzione del sistema di allerta Covid-19), rubricato "Sistema di allerta Covid-19", è volto a disciplinare il trattamento di dati personali nel contesto dell'emergenza sanitaria determinata dalla diffusione del Covid-19 per finalità di allertamento delle persone che possono avere avuto contatti ravvicinati con altri soggetti positivi al virus. Il trattamento dei dati riguarda il tracciamento effettuato tramite l'utilizzo di un'applicazione, installata su base volontaria e destinata alla registrazione dei soli contatti tra soggetti che la abbiano "scaricata", al fine di adottare le adeguate misure di informazione e prevenzione sanitaria nel caso di soggetti entrati in contatto con utenti che risultino, all'esito di test o diagnosi medica, contagiati. Si prevede che il Ministero della salute (titolare del trattamento) si coordini con i soggetti operanti nel Servizio nazionale della protezione civile e i soggetti cd. attuatori di cui all'art. 1 dell'ordinanza del Capo del Dipartimento della protezione civile del 3 febbraio 2020, n. 630, nonché con l'Istituto superiore di sanità e con le strutture pubbliche

e private accreditate che operano nell'ambito del Ssn, nel rispetto delle relative competenze istituzionali. Si chiarisce, al riguardo, che la modalità di tracciamento dei contatti tramite la piattaforma informatica è complementare alle ordinarie modalità di tracciamento in uso nell'ambito del Ssn. Di particolare importanza è il comma 2, in base al quale il Ministero della salute, all'esito di una valutazione di impatto (da adottarsi sentito il Garante ai sensi dell'art. 36 del RGPD e dell'art. 2-*quinquiesdecies* del Codice), dovrà porre in essere misure tecniche e organizzative volte ad assicurare un elevato livello di garanzie e di sicurezza, prevedendo, in particolare, la raccolta, per impostazione predefinita, dei soli dati necessari ad avvisare gli utenti di rientrare fra i contatti stretti e che il trattamento abbia ad oggetto dati di prossimità dei dispositivi resi anonimi o, se ciò non sia possibile, pseudonimizzati (cfr. par. 5.1.2, anche in relazione al provv. 1° giugno 2020, n. 95, doc. web n. 9356568). Di interesse risultano anche il comma 3 della disposizione – che codifica in concreto il principio di finalità, limitando il trattamento dei dati agli scopi descritti, salvo l'utilizzo degli stessi in forma aggregata o comunque anonima ai soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica – e il comma 6, in base al quale ogni trattamento di dati personali dovrà cessare al termine del periodo di emergenza secondo la tempistica espressamente indicata, con conseguente cancellazione dei dati.

La norma, che tiene conto di molte delle indicazioni fornite dal Presidente dell'Autorità nell'audizione tenuta in data 8 aprile 2020 presso la Commissione trasporti e comunicazioni della Camera (cfr. parr. 3.1.1 e 5.1.1), è stata sottoposta al vaglio formale del Garante, il quale si è espresso con il parere di competenza in data 29 aprile 2020, n. 79 (cfr. parr. 3.1.2; 5.1.1). Essa è stata modificata (ai commi 1 e 6) dall'art. 2, d.l. 7 ottobre 2020, n. 125 (recante misure urgenti connesse con la proroga della dichiarazione dello stato di emergenza epidemiologica da Covid-19 e per la continuità operativa del sistema di allerta Covid) per consentire l'utilizzo del sistema di allerta anche oltre frontiera e, quindi, come parte di una strategia europea di controllo del contagio e, per altro verso, di tutela della popolazione rispetto al diffondersi del virus su scala transnazionale. In quest'ottica, viene consentita l'interoperabilità con le piattaforme che operano, con le medesime finalità, nel territorio dell'Unione europea. Come noto, infatti, nel contesto della lotta al coronavirus, la maggior parte degli Stati membri ha adottato un'applicazione nazionale di tracciamento dei contatti e allerta. La modifica prevede esplicitamente che l'attuazione dell'interoperabilità dovrà essere preceduta da una valutazione di impatto del trattamento ai sensi dell'art. 35 del RGPD. Con il medesimo art. 2 si è altresì previsto che il sistema di allerta Covid-19 operi sino alla cessazione delle esigenze di protezione e prevenzione della sanità pubblica legate alla diffusione del Covid-19 anche a carattere transfrontaliero, individuate con d.P.C.M., e non oltre il 31 dicembre 2021. Il testo dell'art. 2 è il frutto di interlocuzioni intercorse fra l'Autorità e la Presidenza del Consiglio dei ministri (cfr. par. 3.1.2).

Il trattamento dei dati nel periodo emergenziale

8) 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 la legge 24 aprile 2020, n. 27, presenta diverse disposizioni di interesse di seguito indicate:

a) l'art. 17-*bis* (già art. 14, d.l. n. 14/2020, confluito nel decreto Cura Italia), che reca disposizioni sul trattamento dei dati personali nel contesto emergenziale. La norma è volta a garantire l'efficacia delle misure di protezione dall'emergenza sanitaria nonché ad assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del Ssn. Il comma 1, ai sensi dell'art. 9, par. 2, lett. *g*), *h*) e *i*), del RGPD e dell'art. 2-*sexies*, comma 2, lett. *t*) e *u*), del Codice, consente a tutti i

soggetti incaricati nella gestione dell'emergenza, per motivi di sanità pubblica, di effettuare i trattamenti di dati personali anche sensibili o giudiziari (di cui agli artt. 9 e 10 del RGPD), se del caso mediante reciproco scambio di informazioni che risultino necessarie per l'espletamento delle relative funzioni (ci si riferisce, in particolare, ai soggetti operanti nel Servizio di protezione civile e ai soggetti attuatori di cui all'art. 1 dell'ordinanza del Capo del Dipartimento della protezione civile del 3 febbraio 2020, n. 630; agli uffici del Ministero della salute e dell'Istituto superiore di sanità e alle strutture pubbliche e private che operano nell'ambito del Ssn). In considerazione del contesto emergenziale, allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, è altresì consentita la comunicazione dei dati personali a soggetti pubblici e privati diversi da quelli citati nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del RGPD nei casi in cui ciò risulti indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto. Tale disposizione dovrebbe quindi consentire la comunicazione dei dati personali comuni ai dirigenti degli uffici pubblici, compresi quelli giudiziari, nonché ai dirigenti scolastici e ai dirigenti delle aziende private e, in generale, a tutti coloro i quali, ricoprendo il ruolo di datori di lavoro, hanno il dovere di adottare ogni misura di sorveglianza o precauzionale all'interno delle strutture o degli uffici di cui sono responsabili. I trattamenti di dati personali in questione devono essere effettuati nel rispetto dei principi di cui all'art. 5 del RGPD, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati. Inoltre, nel bilanciamento tra l'interesse della salute pubblica e di gestione dell'emergenza sanitaria, da un lato, e l'esigenza di salvaguardare la riservatezza degli interessati, dall'altro, i soggetti coinvolti possono conferire le autorizzazioni al trattamento dei dati al proprio personale (ai sensi dell'art. 2-*quaterdecies* del Codice) con modalità semplificate, anche oralmente, e possono omettere l'informativa di cui all'art. 13 del RGPD o fornire un'informativa semplificata, previa comunicazione orale agli interessati della limitazione effettuata. Infine, la norma precisa che, al termine dello stato di emergenza, i medesimi soggetti adotteranno misure idonee a ricondurre i trattamenti di dati personali effettuati nel contesto dell'emergenza nell'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali. Il descritto regime normativo troverà applicazione fino alla data di cessazione dello stato di emergenza;

Proroga delle funzioni del Garante

b) l'art. 118, il quale reca la proroga delle funzioni del Garante dal 31 marzo 2020 fino ai 60 giorni successivi alla cessazione dello stato di emergenza epidemiologica da Covid-19, termine entro il quale il Garante è legittimato ad esercitare le proprie funzioni limitatamente agli atti di ordinaria amministrazione e a quelli indifferibili e urgenti, ferma restando la cessazione da tali funzioni al momento dell'insediamento del nuovo Collegio. Ciò, come si legge nella relazione illustrativa, "in considerazione dell'evolversi dell'epidemia da Covid-19, dichiarata dall'Organizzazione mondiale della sanità (Oms) un'emergenza di sanità pubblica di rilevanza internazionale" e al fine di "evitare che le procedure di nomina debbano svolgersi in un periodo caratterizzato da una possibile limitazione dell'attività delle Camere, chiamate a partecipare, in diversa misura, al rinnovo degli stessi organi";

Sospensione dei termini dei procedimenti amministrativi

c) l'art. 103, che reca disposizioni per il "congelamento" dei termini dei procedimenti amministrativi e gli effetti degli atti amministrativi in scadenza durante il periodo dell'emergenza. In particolare tale disposizione fissava al 15 aprile 2020 – termine poi differito al successivo 15 maggio dall'art. 37, d.l. 8 aprile 2020, n. 23 (cd. Liquidità), convertito dalla l. 5 giugno 2020, n. 40 – la sospensione di tutti i termini relativi ai procedimenti amministrativi pendenti alla data del 23 febbraio 2020 o il cui decorso fosse iniziato successivamente a tale data, al fine di prevenire

il verificarsi di ritardi o la formazione del silenzio significativo nell'arco temporale dedicato alla riorganizzazione dell'attività lavorativa in ragione del sopravvenuto stato emergenziale. Rispetto a tale previsione, il Garante ha stabilito che il periodo di sospensione dei termini di cui alle menzionate disposizioni non avrebbe trovato applicazione ai procedimenti innanzi all'Autorità connessi all'emergenza sanitaria ovvero in presenza di condizioni tali da configurare un pregiudizio imminente ed irreparabile per gli interessati o, ancora, nei casi in cui il carattere di estrema urgenza sia riconosciuto anche sulla base di motivata istanza delle parti (provv. 30 aprile 2020, n. 80, doc. web n. 9333182);

d) l'art. 87, che reca misure straordinarie in materia di lavoro agile e di esenzione dal servizio, stabilendo che per il periodo dello stato di emergenza il lavoro agile costituisce la modalità ordinaria di svolgimento della prestazione lavorativa presso le pubbliche amministrazioni e le autorità amministrative indipendenti, le quali limiteranno la presenza dei dipendenti sul posto di lavoro esclusivamente per assicurare le attività indifferibili e non altrimenti erogabili;

Lavoro agile

e) l'art. 75, che consente anche alle autorità indipendenti di approvvigionarsi di strumenti idonei a favorire il lavoro agile con modalità semplificate. In particolare si consente alle amministrazioni aggiudicatrici, come definite dall'art. 3, d.lgs. 18 aprile 2016, n. 50, nonché alle autorità amministrative indipendenti, fino al 31 dicembre 2020, il ricorso alla procedura negoziata senza previa pubblicazione di un bando di gara;

f) l'art. 73, che individua talune semplificazioni utilizzabili dagli organi collegiali per svolgere le proprie attività. In particolare si consente, per tutto il permanere dello stato di emergenza, lo svolgimento in videoconferenza delle sedute delle giunte comunali, dei consigli dei comuni, delle province, delle città metropolitane e degli organi collegiali degli enti pubblici nazionali, anche articolati su base territoriale, pure nel caso in cui non sia stata regolamentata tale modalità di svolgimento. Tale possibilità viene estesa agli organi collegiali degli enti pubblici nazionali, a condizione che sia garantita la certezza nell'identificazione dei partecipanti e la sicurezza delle comunicazioni (comma 2), alle associazioni private anche non riconosciute e alle fondazioni, nel rispetto di criteri di trasparenza e tracciabilità previamente fissati, purché siano individuati sistemi che consentano di identificare con certezza i partecipanti nonché adeguata pubblicità delle sedute, ove previsto, secondo le modalità individuate da ciascun ente.

Funzionamento degli organi collegiali di enti locali e nazionali

9) La legge 10 febbraio 2020, n. 10, recante disposizioni in materia di donazione del corpo *post mortem* e di utilizzo dei cadaveri a fini di studio, di ricerca scientifica e di formazione. La legge mira a disciplinare gli atti di disposizione del proprio corpo e dei tessuti *post mortem* a fini di studio, di formazione e di ricerca scientifica da parte di soggetti che hanno espresso in vita il loro consenso. In sintesi, essa prevede che la dichiarazione di consenso alla donazione *post mortem* del proprio corpo o dei tessuti per fini di ricerca, debba essere redatta, in analogia con la legge n. 219/2017 sul consenso informato e sulle disposizioni anticipate di trattamento (Dat), nelle forme previste per queste ultime. Inoltre, la dichiarazione di consenso deve essere consegnata alla Asl di appartenenza, cui spetta il compito di conservarla e di trasmetterla telematicamente alla banca dati Dat. La revoca del consenso può essere effettuata in qualsiasi momento e con le medesime modalità. A differenza della legge n. 219/2017, che prevede la possibilità di indicare nelle Dat un fiduciario chiamato a rappresentare il disponente nelle relazioni con il medico e con le strutture sanitarie, nella dichiarazione di consenso alla donazione *post mortem* deve essere obbligatoriamente indicato un fiduciario (ed eventualmente di un sostituto) al quale spetta l'onere di comunicare l'esistenza del consenso al medico che accerta il decesso.

Donazione del corpo *post mortem*

L'art. 5 del disegno di legge dispone l'istituzione, presso il Ministero della salute, dell'elenco nazionale dei centri di riferimento per la conservazione e l'utilizzazione dei corpi dei defunti.

2.2. *I decreti legislativi*

In relazione ai decreti legislativi, ci si riferisce ai seguenti:

Archivio nazionale lavoratori esposti a radiazioni ionizzanti

1) il decreto legislativo 31 luglio 2020, n. 101, recante l'attuazione della direttiva 2013/59/Euratom, che stabilisce norme fondamentali di sicurezza relative alla protezione contro i pericoli derivanti dall'esposizione alle radiazioni ionizzanti. Il decreto detta disposizioni applicabili a tutte le situazioni che comportino un rischio da esposizione a radiazioni ionizzanti non trascurabile per la protezione della salute umana e, ancor più, per quella dei lavoratori. Il titolo XI del provvedimento (artt. 106-146) riproduce e aggiorna le corrispondenti norme di cui al titolo VIII del decreto legislativo n. 230/1995, volte a tutelare i lavoratori – inclusi quelli addetti ad attività esercitate dallo Stato, dagli enti pubblici, territoriali e non territoriali, dagli organi del Ssn, dagli istituti di istruzione, dalle università e dai laboratori di ricerca – rispetto ai rischi derivanti dall'esposizione alle radiazioni ionizzanti. Di particolare interesse è l'art. 126 che prevede l'istituzione presso il Ministero del lavoro di un Archivio nazionale dei lavoratori esposti, le cui modalità e i criteri di costituzione, alimentazione, gestione e di accesso vengono demandate ad un decreto del Ministro del lavoro da adottare sentito il Garante.

Registrazione delle persone a bordo delle navi passeggeri

2) Il decreto legislativo 11 maggio 2020, n. 38, recante attuazione della direttiva (UE) 2017/2109 del Parlamento europeo e del Consiglio, del 15 novembre 2017, che modifica la direttiva 98/41/CE, relativa alla registrazione delle persone a bordo delle navi da passeggeri che effettuano viaggi da e verso i porti degli Stati membri e la direttiva 2010/65/UE, relativa alle formalità di dichiarazione delle navi in arrivo e/o in partenza da porti degli Stati membri. Il decreto si propone di aggiornare, chiarire e semplificare gli attuali requisiti per il conteggio e la registrazione dei passeggeri e dei membri dell'equipaggio a bordo delle navi da passeggeri, rafforzando, al contempo, il livello di sicurezza della navigazione. Come viene infatti espressamente previsto dall'art. 1, la raccolta di dati effettuata a bordo delle navi è finalizzata a "migliorare il livello di sicurezza e accrescere la possibilità di salvataggio dei passeggeri e dei membri dell'equipaggio […] nonché a garantire una gestione più efficace delle operazioni di ricerca e soccorso" anche nell'ottica di sfruttare le potenzialità della digitalizzazione nell'ambito della registrazione, trasmissione, disponibilità e protezione dei dati. Tra le disposizioni di particolare interesse si segnalano gli artt. 4 e 5, i quali prevedono che prima della partenza della nave, a cura dell'addetto alla registrazione dei passeggeri, vengano registrate nell'interfaccia unica nazionale, oltre al conteggio delle persone a bordo (art. 4), anche le loro generalità e le informazioni riguardanti i passeggeri che hanno dichiarato di avere bisogno di cure o assistenza speciali (art. 5). L'art. 6 prevede inoltre specifici obblighi in capo alle società di gestione di navi da passeggeri, tra i quali quelli di rendere disponibili i dati sulle persone e di designare un addetto alla registrazione dei passeggeri responsabile per l'inserimento delle informazioni nell'interfaccia unica nazionale o nel sistema di identificazione automatica. Si prevede venga fornita ai passeggeri una specifica informativa tramite il biglietto o direttamente dalla società che assume l'esercizio della nave; in tal modo il passeggero è informato sui motivi posti alla base della raccolta dei dati (finalità) e sulla facoltà di indicare eventuali informazioni utili per particolari cure o assistenza in caso di emergenza, nonché in merito alla circostanza

che i dati personali sono conservati solo per il tempo strettamente necessario (art. 9). L'art. 11 prevede che, in caso di violazione degli obblighi di riservatezza previsti dal decreto all'art. 12, il funzionario o l'agente addetto alla registrazione dei passeggeri che ha accertato la violazione invii l'informativa al Garante. L'art. 12 del decreto è espressamente dedicato al trattamento dei dati personali, disponendo che quelli raccolti ai sensi dell'art. 5 siano conservati dalla società solo per il tempo necessario al raggiungimento delle finalità previste e, in ogni caso, fino al momento in cui il viaggio sia terminato (in sicurezza) oppure, in caso di emergenza o in seguito a un incidente, fino al completamento dell'indagine o del procedimento giudiziario. Si prevede inoltre che nel rispetto delle previsioni del Codice e del decreto legislativo 18 maggio 2018, n. 51, le informazioni che non sono più necessarie siano cancellate automaticamente e senza ritardo. Sempre al medesimo articolo, al comma 4, è stabilito che i dati personali raccolti per le finalità di cui all'art. 1, siano "altresì, utilizzati per i controlli di frontiera di cui al regolamento (UE) 2016/399 del 9 marzo 2016, che istituisce un codice unionale relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen)". Sullo schema di decreto il Garante ha espresso parere favorevole (provv. 23 gennaio 2020, n. 9, doc. web n. 9277100), con osservazioni volte a rendere il provvedimento pienamente conforme ai principi e alle norme del RGPD, poi pressoché integralmente recepite dall'Amministrazione (cfr. par 3.1.2). In particolare, l'Autorità aveva espresso perplessità relativamente all'attribuzione della competenza a ricevere il rapporto di cui all'art. 17, l. 24 novembre 1981, n. 689, al capo del compartimento marittimo prevista dall'art. 11 dello schema, alla luce della disciplina sulle sanzioni amministrative pecuniarie derivanti da violazioni inerenti al diritto alla protezione di dati personali contenuta nel RGPD, che attribuisce la relativa competenza alle autorità nazionali di controllo. Il Garante aveva inoltre rilevato che l'art. 5 dello schema, nell'individuare la tipologia dei dati personali raccolti a bordo della nave, aveva compreso tra quelli obbligatori cognome, nome, genere, nazionalità e data di nascita, mentre rimetteva ad una specifica iniziativa del passeggero il rilascio di ulteriori informazioni riferite alla necessità di cure o assistenza in situazioni di emergenza, nonché di eventuali numeri da contattare in tali eventualità. Trattandosi di particolari categorie di dati personali (relativi alla salute degli interessati), si richiamava l'attenzione dell'amministrazione sull'opportunità che, nell'informativa da fornire al passeggero ai sensi dell'art. 13 del RGPD, lo stesso fosse reso edotto non solo della prevista possibilità di comunicare i propri dati sanitari, ma anche dell'inserimento degli stessi nell'interfaccia e della loro trasmissione al comandante prima della partenza della nave (art. 6, comma 5). L'Autorità aveva inoltre espresso perplessità sulla compatibilità delle disposizioni di cui ai commi 4 e 5 dell'art. 12 dello schema, che prevedevano l'utilizzo dei dati raccolti anche per i controlli di frontiera, con le finalità perseguite dalla direttiva oggetto di attuazione, alla luce del quadro normativo europeo e nazionale di garanzie previste a tutela del diritto alla protezione dei dati personali. La XIV Commissione politiche dell'Unione europea della Camera, nell'esprimere il 4 marzo del 2020 parere favorevole sullo schema di decreto, ha richiesto al Governo di valutare l'opportunità di recepire i rilievi contenuti nel parere del Garante; il Governo ha recepito pressoché integralmente tali osservazioni.

Ciononostante l'art. 12, comma 4, d.lgs. n. 36/2020 prevede che "I dati raccolti ai sensi dell'articolo 5 sono, altresì, utilizzati per i controlli di frontiera di cui al Regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio del 9 marzo 2016, che istituisce un codice unionale relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen). A tal fine, i dati sono trasferiti al Dipartimento della pubblica sicurezza del Ministero dell'interno,

mediante modalità tecniche concordate con il Ministero delle infrastrutture e dei trasporti".

Scambio automatico di informazioni nel settore fiscale

3) Il decreto legislativo 30 luglio 2020, n. 100, volto a dare attuazione alla direttiva (UE) 2018/822 del Consiglio, del 25 maggio 2018 (cd. DAC6), recante modifica della direttiva 2011/16/UE in materia di scambio automatico obbligatorio di informazioni nel settore fiscale. Il decreto – anche al fine di rafforzare gli strumenti di contrasto all'evasione e all'elusione fiscale – modifica le norme e le procedure relative allo scambio automatico obbligatorio di informazioni nel settore fiscale relativamente ai meccanismi soggetti all'obbligo di comunicazione all'Agenzia delle entrate da parte degli intermediari e dei contribuenti con le altre autorità competenti degli Stati membri e con altre giurisdizioni. Il meccanismo transfrontaliero rappresenta uno schema, accordo o progetto riguardante l'Italia e una o più giurisdizioni estere. Le informazioni oggetto di comunicazione riguardano, in particolare: l'identificazione degli intermediari e dei contribuenti interessati (nome, data e luogo di nascita ovvero denominazione o ragione sociale, indirizzo, residenza ai fini fiscali, numero di identificazione fiscale), nonché dei soggetti che costituiscono imprese associate di tali contribuenti; gli elementi distintivi presenti nel meccanismo transfrontaliero che lo rendono oggetto di comunicazione e una sintesi del suo contenuto; la data di avvio dell'attuazione del suddetto meccanismo e le disposizioni nazionali che ne stabiliscono l'obbligo; l'identificazione delle giurisdizioni di residenza fiscale dei contribuenti interessati, nonché delle eventuali altre giurisdizioni potenzialmente interessate dal meccanismo transfrontaliero oggetto dell'obbligo di comunicazione; l'identificazione di qualunque altro soggetto potenzialmente interessato dal meccanismo.

2.3. *Norme di rango secondario*

Sono stati inoltre pubblicati i seguenti atti di rango secondario aventi impatto sulla protezione dei dati personali, sui cui schemi, peraltro, il Garante ha reso a suo tempo parere:

- d.P.C.M. 19 giugno 2020, n. 110, recante il regolamento sulle modalità e criteri di attivazione e gestione del servizio IT-*Alert* per finalità di protezione civile (parere 17 ottobre 2019, n. 193, doc. web n. 9207188);
- decreto 24 novembre 2020, n. 156 del Ministro dell'economia e delle finanze, recante il regolamento sulle condizioni e criteri per l'attribuzione delle misure premiali per l'utilizzo degli strumenti di pagamento elettronici (cd. *cashback*) (parere 13 ottobre 2020, n. 179, doc. web n. 9466707: cfr. parr. 3.1.4 e 4.1.4);
- decreto 12 gennaio 2021, n. 33 del Ministro della giustizia, recante il regolamento di modifica del decreto 7 novembre 2001, n. 458, in materia di funzionamento dell'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento (parere 1° ottobre 2020, n. 178, doc. web n. 9483571: cfr. par. 3.1.4);
- decreto 22 dicembre 2020, n. 192, recante modifiche al decreto 24 dicembre 2019, n. 177, concernente i criteri e le modalità di attribuzione e di utilizzo della Carta elettronica, prevista dall'art. 1, comma 604, l. 30 dicembre 2018, n. 145 (cd. *bonus* cultura o 18*app*) (parere 26 novembre 2020, n. 234, doc. web n. 9505279) (cfr. parr. 3.1.4 e 4.2.5).

2.4. *Raccolta di disposizioni correlate all'epidemia da Covid-19*

È dato di esperienza comune, e le pagine precedenti lo attestano, che la diffusione dell'epidemia da Covid-19 ha portato il Parlamento, il Governo e le altre Istituzioni competenti ad adottare un corposo numero di atti volti a contenere l'emergenza sanitaria, causando un'imponente stratificazione di fonti (di vario livello) e una continua evoluzione della disciplina.

Dato che parte significativa di tali interventi normativi/regolatori hanno un impatto significativo sulla disciplina in materia di protezione dei dati personali, è stata curata dall'Autorità un'opera di sistematizzazione e classificazione di tali disposizioni, riunendone gli estratti in un documento pubblicato sul sito web dell'Autorità al fine di agevolarne l'individuazione da parte agli operatori del diritto interessati all'applicazione della disciplina di protezione dei dati, a partire da titolari e responsabili del trattamento. Il documento in questione, aggiornato settimanalmente, costituisce una raccolta di disposizioni di testi normativi e amministrativi generali, applicabili sull'intero territorio nazionale, emanati in relazione all'emergenza scaturita dalla diffusione dell'epidemia da Covid-19, a partire dall'inizio del 2020, che presentano profili di interesse sul piano della protezione dei dati personali.

3 I rapporti con il Parlamento e le altre Istituzioni

3.1. *L'attività consultiva del Garante*

Innovando rispetto alla cornice normativa preesistente, il RGPD 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. n. 96 del RGPD; art. 28, par. 2, direttiva (UE) 2016/680; art. 24, comma 2, d.lgs. n. 51/2018). Ciò ha incrementato notevolmente l'attività consultiva dell'Autorità – in precedenza interessata solo dalla normativa di carattere secondario (regolamenti) o da atti amministrativi generali "suscettibili di incidere sulle materie disciplinate" dal Codice (così l'art. 154, comma 4, del Codice, poi abrogato) – non di rado svolta in tempi brevissimi (specie nelle tematiche aventi ad oggetto la situazione di emergenza sanitaria), ben lontani dai termini previsti dalla normativa di riferimento (45 giorni: cfr. art. 154, comma 5, Codice).

Sotto questo profilo non aiuta la mancanza di procedure definite o comunque sufficientemente sperimentate, né il dettato dell'art. 36, par. 4, del RGPD il quale si limita a stabilire che la consultazione avvenga "durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali", senza alcuna indicazione della tempistica.

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

Alla luce del quadro normativo sopra esposto, consolidando una prassi già avviata nel 2019, il Parlamento ha "consultato" il Garante, richiedendone l'audizione presso le competenti Commissioni nel corso dell'esame di proposte o disegni di legge aventi rilevanza sotto il profilo della protezione dei dati, oppure, in altri casi, sollecitando l'inoltro di memorie scritte su eventuali profili di criticità delle disposizioni normative in discussione.

Ciò è avvenuto nel corso dei lavori su progetti normativi o disegni di legge di conversione di provvedimenti d'urgenza del Governo relativi a temi di rilevanza primaria, che spaziano dal trattamento dei dati personali effettuato nella situazione di emergenza sanitaria, anche mediante strumenti elettronici (si pensi all'utilizzo del sistema di allerta istituito a fini di tracciamento delle persone colpite dal virus, mediante la *app* Immuni), alla sempre più diffusa circolazione, sui *social network* o comunque in rete, di informazioni false (cd. *fake news*), come pure alla disciplina delle intercettazioni di comunicazioni.

Al di là delle forme prescelte per consultare l'Autorità, il Parlamento ha in tal modo dimostrato una forte sensibilità sui temi aventi impatto sul diritto alla protezione dei dati personali, coinvolgendo il Garante nel corso del procedimento legislativo. Sotto questo specifico profilo, le audizioni o le memorie scritte hanno riguardato i seguenti progetti di legge:

- memoria alla Commissione Affari costituzionali del Senato, nell'ambito dell'esame del disegno di legge di conversione del decreto-legge 7 ottobre 2020, n.

125, recante misure urgenti connesse con la proroga della dichiarazione dello stato di emergenza epidemiologica da Covid-19 e per la continuità operativa del sistema di allerta Covid (19 ottobre 2020, doc. web n. 9468919: cfr. par. 2.1);
- audizione presso le Commissioni riunite trasporti e cultura della Camera dei deputati nell'ambito dell'esame di alcune proposte di legge recanti istituzione di una Commissione parlamentare di inchiesta sulla diffusione intenzionale, seriale e massiva di informazioni false (cd. *fake news*) (3 marzo 2020, doc. web n. 9283850: cfr. par. 12.8);
- audizione presso la Commissione giustizia del Senato sul disegno di legge di conversione del decreto-legge 30 dicembre 2019, n. 161, recante modifiche alla disciplina delle intercettazioni di conversazioni o comunicazioni (4 febbraio 2020, doc. web n. 9260158).

Più in generale, il Parlamento ha coinvolto l'Autorità richiedendo audizioni o memorie scritte anche su altri temi di interesse approfonditi nelle competenti Commissioni nell'ambito di indagini conoscitive o specifici dibattiti, come nei seguenti casi:
- audizione presso la Commissione parlamentare per l'infanzia e l'adolescenza, nell'ambito dell'indagine conoscitiva sulle forme di violenza fra i minori e ai danni di bambini e adolescenti (8 luglio 2020, doc. web n. 9434094);
- audizione presso la Commissione parlamentare per la semplificazione, nell'ambito dell'indagine conoscitiva in materia di semplificazione dell'accesso ai servizi erogati dal Servizio sanitario nazionale (25 maggio 2020, doc. web n. 9351203);
- audizione presso la Commissione lavoro pubblico e privato, previdenza sociale del Senato sull'affare (atto n. 453) relativo al tema di ricadute occupazionali dell'epidemia da Covid-19, azioni idonee a fronteggiare le situazioni di crisi e necessità di garantire la sicurezza sanitaria nei luoghi di lavoro (13 maggio 2020, doc. web n. 9341993);
- audizione presso la Commissione trasporti e comunicazioni della Camera dei deputati sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Covid-19 (8 aprile 2020, doc. web n. 9308774).

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

Intensa è stata la collaborazione con il Governo e, in particolare, con le amministrazioni più interessate ai temi connessi all'esigenza di fronteggiare l'emergenza epidemiologica sul piano della sanità pubblica e degli interventi economici (Ministero della salute e Mef) nell'ambito dei procedimenti di elaborazione di norme destinate a divenire oggetto di provvedimenti d'urgenza o di proposte di emendamento nel corso dei lavori parlamentari.

In tale quadro, il Garante ha reso parere formale, ai sensi dell'art. 36, par. 4, del RGPD, in due occasioni, rispetto a:
- una proposta normativa predisposta dal Ministero della salute concernente l'utilizzo di una "applicazione" volta a realizzare il tracciamento dei contagi da Covid-19, poi confluita nell'art. 6, decreto-legge 30 aprile 2020, n. 28, convertito dalla legge 25 giugno 2020, n. 70 (parere 29 aprile 2020, n. 79, doc. web n. 9328050) (cfr. parr. 2.1 e 5.1.1). La norma prevede che l'*app* possa essere utilizzata esclusivamente su base facoltativa e che i dati personali forniti dagli interessati siano trattati esclusivamente per rendere edotti gli utenti dell'applicazione di rientrare tra i contatti stretti di soggetti risultati positivi al Covid-19. Circa gli scopi di tale utilizzo, nella disposizione si pre-

cisa che i dati raccolti attraverso l'applicazione non possono essere utilizzati per finalità diverse da quelle del corretto ed efficace funzionamento dell'*app*, vale a dire al fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione, fatta salva, comunque, la possibilità di utilizzo "in forma aggregata o comunque anonima", per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica, nel rispetto del diritto europeo (commi 1 e 3). L'allertamento avviene attraverso l'utilizzo della tecnologia *bluetooth* e senza che siano trattati dati di localizzazione degli individui. Il Garante, nel parere reso, preso atto che la norma proposta teneva conto di molte delle indicazioni fornite nel corso dell'audizione tenuta in data 8 aprile 2020 presso la Commissione trasporti e comunicazioni della Camera (cfr. par. 3.1.1), l'ha ritenuta conforme, nelle sue linee generali, ai criteri indicati dalle linee guida del Cepd del 21 aprile 2020 a proposito dei sistemi di *contact tracing* (doc. web n. 9321621), ovvero alla: volontarietà, per cui la mancata adesione al sistema non deve comportare svantaggi o comunque conseguenze pregiudizievoli, né rappresentare la condizione per l'esercizio di diritti (cfr. art. 6, comma 4); previsione normativa, quale base giuridica adeguata in termini di garanzie, in conformità ai dettami del RGPD e del Codice; trasparenza (cfr. art. 6, comma 2, lett. *a*), che assicura agli interessati un'idonea informazione sul trattamento); determinatezza ed esclusività dello scopo (il tracciamento deve essere finalizzato esclusivamente al contenimento dei contagi, escludendo fini ulteriori); selettività e minimizzazione dei dati; non esclusività del processo algoritmico e possibilità di esercitare in ogni momento i diritti di cui agli artt. da 15 a 22 del RGPD; reciprocità di anonimato tra gli utenti dell'*app*, i quali devono peraltro non essere identificabili dal titolare del trattamento, dovendo l'identificazione ammettersi al limitato fine dell'individuazione dei contagiati. Il Garante, in sostanza, nell'esprimere parere favorevole all'approvazione della norma, ha ritenuto che il sistema di *contact tracing* prefigurato non contrasti con i principi di protezione dei dati personali in quanto: previsto da una norma di legge sufficientemente dettagliata quanto ad articolazione del trattamento, tipologia di dati raccolti, garanzie accordate agli interessati e temporaneità della misura; fondato sull'adesione volontaria dell'interessato, con esclusione di ogni forma di condizionamento individuale e, quindi, di disparità di trattamento basata sulla scelta effettuata; preordinato al perseguimento di fini di interesse pubblico indicati con sufficiente chiarezza, con esclusione del trattamento secondario dei dati così raccolti per fini diversi, salva la possibilità (nei termini generali previsti dal RGPD) di utilizzo, in forma anonima o aggregata, a fini statistici o di ricerca scientifica; conforme ai principi di minimizzazione e ai criteri di *privacy by design* e *by default*, nella misura in cui prevede la raccolta dei soli dati di prossimità dei dispositivi, il loro trattamento in forma pseudonima, sempre che non sia possibile in forma del tutto anonima, con esclusione del ricorso a dati di geolocalizzazione e limitandone la conservazione al tempo strettamente necessario ai fini del perseguimento dello scopo indicato, con cancellazione automatica alla scadenza del termine di conservazione; conforme al principio di trasparenza nei confronti dell'interessato, cui è fornita adeguata informazione; suscettibile di essere perfezionato con l'ulteriore precisazione delle caratteristiche di dettaglio del trattamento e delle misure di sicurezza da parte del Ministero della salute, anche mediante un provvedimento del Garante da adottarsi ai sensi dell'art. 2-*quinquiesdecies* del Codice;

- una proposta normativa del Ministero della salute finalizzata a consentire indagini di sieroprevalenza sul Sars-Cov-2 da parte del medesimo Dicastero e dell'Istat per finalità epidemiologiche e statistiche, successivamente approvata quale art. 1, d.l. 10 maggio 2020, n. 30, convertito dalla legge 2 luglio 2020 n. 72 (parere 4 maggio 2020, n. 82, doc. web n. 9340513) (cfr. parr. 2.1 e 5.3); la norma consente il trattamento di dati personali, anche genetici e relativi alla salute, per fini statistici e di studi scientifici svolti nel settore della sanità pubblica, nell'ambito di un'indagine di sieroprevalenza condotta congiuntamente dai competenti uffici del Ministero della salute e dall'Istat in qualità di titolari del trattamento. Essa prevede l'istituzione di una piattaforma tecnologica, la realizzazione di studi epidemiologici e statistici da parte del predetto Dicastero e dell'Istat sullo stato immunitario della popolazione, indispensabili per contrastare l'emergenza epidemiologica da Covid-19. Il Garante, con il menzionato parere, si è espresso sullo schema evidenziando lacune e criticità correlate, in particolare, all'applicazione della disciplina relativa ai trattamenti di dati personali per fini statistici e di ricerca scientifica, che impone il divieto di utilizzo dei dati trattati a tali scopi per l'assunzione di decisioni o provvedimenti individuali o comunque per fini diversi. È stato ritenuto eccessivo l'accesso da parte delle regioni e delle province autonome, per finalità di analisi e programmazione nell'ambito dell'emergenza epidemiologica, ai dati identificativi trasmessi dall'Istat all'apposita piattaforma del Ministero della salute, integrati da quelli sulla salute e genetici, suscettibili peraltro di interconnessione con ulteriori – non meglio precisati – dati personali presenti in banche dati dell'Istat e del medesimo Dicastero. Parimenti problematica è stata considerata la previsione dell'interconnessione dei dati sulla salute e genetici raccolti nell'ambito dell'indagine di sieroprevalenza tra numerosissimi soggetti cui sono attribuite differenti competenze e funzioni, quali il Ministero della salute, l'Istat, la Croce rossa italiana, le regioni, le province autonome, i laboratori che effettuano il prelievo, le università e i centri di ricerca, nonché l'Istituto superiore di sanità. Si è ritenuto che anche l'impiego del sistema informativo sanitario del Ministero per consentire l'interconnessione con i sistemi informativi regionali a fini di programmazione e controllo dell'assistenza sanitaria presentasse profili di criticità. Su tali basi il Garante ha ritenuto necessario che, nell'ambito dei sistemi informativi del Ministero della salute e delle regioni, fosse previsto il trattamento di dati aggregati risultanti dall'indagine di sieroprevalenza. A seguito della adozione del parere, sono state avviate proficue interlocuzioni tra gli uffici del Ministero, dell'Istat, della Protezione civile e dell'Autorità che hanno consentito di riformulare la disposizione in modo da superare le criticità evidenziate.

Nell'ambito di una serie di interlocuzioni, anche informali, fra l'Autorità e gli uffici dei ministeri interessati, è stato curato l'esame di ulteriori proposte normative di rango primario su temi di particolare interesse, poi confluite anch'esse in provvedimenti normativi del Governo. Il riferimento va, in particolare, ad alcune disposizioni in materia di Fse (sul quale v. *amplius* par. 5.11.1), metodologie mediche predittive, indagini in materia di ricerca scientifica e statistica, gestione dei registri delle nascite e delle morti – inserite successivamente nel decreto-legge 19 maggio 2020, n. 34 (cd. Rilancio), convertito dalla legge 17 luglio 2020, n. 77 (artt. 7, 11, 12 e 13: cfr. par. 2.1) –, nonché ad una disposizione volta a favorire l'interoperabilità dell'*app* Immuni con le analoghe applicazioni degli altri Paesi europei in chiave di prevenzione comune e coordinata del contagio e a prorogare l'impiego dello strumento di allerta e il relativo monitoraggio dei dati, considerato il persistente stato

di emergenza epidemiologica. Tale ultima disposizione è stata poi approvata come art. 2, d.l. 7 ottobre 2020, n. 125, convertito dalla legge 27 novembre 2020, n. 159 (nel quadro dei lavori di approvazione del relativo disegno di legge di conversione, il Garante ha fornito ulteriori elementi di valutazione su richiesta della competente commissione del Senato: cfr. parr. 2.1, n. 7 e 3.1.1).

Infine, è stato reso il parere di competenza su uno schema di decreto legislativo, recante norme di attuazione della direttiva (UE) 2017/2109, che modifica la direttiva (CE) 98/41 relativa alla registrazione delle persone a bordo delle navi da passeggeri che effettuano viaggi da e verso i porti degli Stati membri e la direttiva (UE) 2010/65 relativa alle formalità di dichiarazione delle navi in arrivo e/o in partenza da porti degli Stati membri (parere 23 gennaio 2020, n. 9, doc. web n. 9277100) (cfr. par. 2.2).

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

Il Garante ha reso il proprio parere su alcuni progetti di legge e altri atti normativi in ambito regionale o delle province autonome, riferiti in particolare ai seguenti ambiti:

- proposte normative della Provincia autonoma di Trento in materia, in particolare, di anagrafe provinciale degli assistiti, da inserire nel "Collegato 2020" (parere 23 gennaio 2020, n. 11, doc. web n. 9266796);
- schema di regolamento della Provincia autonoma di Trento concernente l'attuazione della legge provinciale 31 maggio 2012, n. 10, in materia di trattamento dei dati personali nell'ambito del Registro unico dei controlli provinciali (RUCP) (parere 5 marzo 2020, n. 51, doc. web n. 9309418);
- schema di regolamento della Provincia autonoma di Trento recante disciplina del trattamento dei dati personali nell'ambito del Registro tumori, realizzato in attuazione dell'art. 14, commi 5-*bis* e 5-*ter* della legge provinciale 23 luglio 2010, n. 16 (parere 26 marzo 2020, n. 63, doc. web n. 9344651);
- disegno di legge della Provincia autonoma di Trento concernente misure di sostegno per le famiglie, i lavoratori e i settori economici connesse all'emergenza epidemiologica da Covid-19 (parere 8 maggio 2020, n. 84, doc. web n. 9344635: cfr. par. 5.12.2);
- schema di regolamento della Provincia autonoma di Trento concernente la medicina di iniziativa nel Servizio sanitario provinciale, in attuazione dell'art. 4, comma 1-*ter* della legge provinciale n. 16 del 2010 (parere 1° ottobre 2020, n. 175, doc. web n. 9469372: cfr. par. 5.12.2);
- schema di norma predisposta dalla Provincia autonoma di Trento in materia di trattamenti che implicano decisioni integralmente automatizzate (parere 15 ottobre 2020, n. 191, doc. web n. 9480921);
- proposta di emendamento della Regione Piemonte alla legge regionale 7 aprile 2000, n. 43, recante disposizioni per la tutela dell'ambiente in materia di inquinamento atmosferico e per la prima attuazione del Piano regionale per il risanamento e la tutela della qualità dell'aria (parere 15 ottobre 2020, n. 184, doc. web n. 9480905).

3.1.4. La consultazione del Garante sugli atti del Governo aventi natura regolamentare

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 sui sottoindicati schemi di decreto aventi natura regolamentare:

- schema di d.P.C.M. di attuazione dell'art. 19-*bis*, d.lgs. 18 agosto 2015, n. 142 (introdotto dall'art. 5, legge 7 aprile 2017, n. 47), recante le modalità di svolgimento del colloquio che il minore straniero non accompagnato deve effettuare al momento dell'ingresso nelle strutture di prima accoglienza (parere 9 aprile 2020, n. 67, doc. web n. 9343058);
- schema di decreto interministeriale di natura regolamentare recante disposizioni sul cd. *bonus* mobilità, attuativo dell'art. 2, comma 1, d.l. 14 ottobre 2019, n. 111, convertito con modificazioni dalla legge 12 dicembre 2019, n. 141 e modificato dal decreto-legge 19 maggio 2020, n. 34 (parere 9 luglio 2020, n. 135, doc. web n. 9439976);
- schema di decreto interministeriale avente natura regolamentare recante adeguamenti normativi sulle modalità di rilascio delle carte tachigrafiche e per la tenuta dei registri, ai sensi dell'art. 3, comma 8, del decreto ministeriale 31 ottobre 2003, n. 361 (parere 17 settembre 2020, n. 157, doc. web n. 9468728);
- schema di regolamento del Ministro della giustizia di modifica del decreto 7 novembre 2001, n. 458, recante disposizioni sul funzionamento dell'archivio informatizzato degli assegni bancari e postali (parere 1° ottobre 2020, n. 178, doc. web n. 9483571);
- schema di decreto del Ministro dell'economia e finanze recante regolamento in materia di condizioni e criteri per l'attribuzione delle misure premiali per utilizzo degli strumenti di pagamento elettronici ai sensi dell'art. 1, commi da 288 a 290, della legge 27 dicembre 2019, n. 160, cd. *cashback* (parere 13 ottobre 2020, n. 179, doc. web n. 9466707: cfr. par. 4.1.4);
- schema di regolamento recante modifiche al d.P.R. 26 luglio 1976, n. 752, di attuazione dello Statuto speciale della Regione Trentino Alto Adige, in materia di proporzionale negli uffici statali siti nella Provincia di Bolzano e di conoscenza delle due lingue nel pubblico impiego (parere 29 ottobre 2020, n. 199, doc. web n. 9487448);
- schema di decreto del Ministro dell'ambiente, del territorio e del mare di natura regolamentare concernente il riconoscimento di un contributo a favore di imprese che svolgono attività in campo di guida escursionistica e tutela ambientale, in conseguenza dell'emergenza Covid-19 (parere 29 ottobre 2020, n. 211, doc. web n. 9487962);
- schema di decreto interministeriale avente natura regolamentare volto a definire le modalità e i termini per l'ottenimento e l'erogazione del beneficio economico di cui al Programma sperimentale buono mobilità per il 2021, cd. *bonus* rottamazione (parere 26 novembre 2020, n. 233, doc. web n. 9519436);
- schema di regolamento del Ministero per i beni e le attività culturali e per il turismo, concernente le regole sull'attribuzione e l'utilizzo della Carta elettronica per i diciottenni del 2020 (cd. *bonus* cultura o anche 18*app*) (parere 26 novembre 2020, n. 234, doc. web n. 9505279: cfr. par. 4.2.5);
- schema di regolamento del Ministro dello sviluppo economico che sostituisce il d.P.R. n. 178/2010 in materia di Registro pubblico delle opposizioni (Rpo) alle comunicazioni pubblicitarie indesiderate (parere 10 dicembre 2020, n. 260, doc. web n. 9517462: cfr. par. 11.1).

3.1.5. La consultazione del Garante sui provvedimenti di altre Istituzioni

Il Garante si è inoltre espresso su una pluralità di atti e provvedimenti di Istituzioni diverse rispetto al Governo, delle quali si potrà dare più ampiamente conto nel corpo della Relazione e tra i quali si segnalano:

- schema di decreto del Presidente del Consiglio di Stato recante le regole tecni-

co-operative per l'attuazione del processo amministrativo telematico, nonché per la sperimentazione e la graduale applicazione dei relativi aggiornamenti, ai sensi dell'articolo 4, comma 2, del decreto-legge 30 aprile 2020, n. 28 (parere 19 maggio 2020, n. 88, doc. web n. 9347280);
- schema di provvedimento della Banca d'Italia recante modifiche al regolamento del Governatore della Banca d'Italia del 29 gennaio 2002, come modificato il 31 luglio 2018, recante il funzionamento dell'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento (Centrale di allarme interbancaria - Cai) (parere 10 giugno 2020, n. 97, doc. web n. 9433428);
- schema di determinazione del Direttore dell'Agenzia delle dogane e dei monopoli, d'intesa con il Direttore dell'Agenzia delle entrate, di modifica della determinazione attuativa della lotteria dei corrispettivi (cd. decreto *cashless*) (provv. 1° ottobre 2020, n. 172, doc. web n. 9466165).

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 aspetti di interesse in materia di protezione dei dati.

In un caso sono stati richiesti al Garante elementi informativi da parte del Governo (Ministero dello sviluppo economico) per poter corrispondere agli atti in questione, rispetto all'interrogazione a risposta scritta n. 4-03135, presentata dall'on. De Bonis in materia di *fake news*, in relazione alla quale l'Autorità ha inoltrato le osservazioni di competenza (nota 6 maggio 2020, par. 12.8). L'interrogazione verteva su un sistema di *fact checking* al fine di contrastare il fenomeno delle *fake news* riguardanti il Covid-19. Il progetto, denominato FACTA, permetterebbe ad un utente di Whatsapp, servizio di messaggistica di proprietà di Facebook, di inviare messaggi ricevuti da altri utenti a Pagella Politica srls (titolare del sito www.pagellapolitica.it) al fine di ottenere un controllo di veridicità dei contenuti riportati nei messaggi medesimi. All'esito di tali verifiche, qualora si ritenesse falso il contenuto (della notizia), il messaggio verrebbe inserito in una lista, appositamente creata e pubblicata sul web. Il progetto, nato dall'esigenza di dare certezze nell'attuale situazione emergenziale legata all'epidemia da Covid-19, sarebbe tuttavia destinato a rimanere in uso anche dopo la cessazione di questa fase, quale servizio aggiuntivo di contrasto alle *fake news.*

Nella nota inviata al Ministero, l'Autorità, nel prendere atto della delicatezza della materia e dei diversi profili coinvolti, il cui equilibrio assume particolare importanza in uno Stato democratico (protezione dei dati personali, libertà di espressione del pensiero e utilizzo efficace, ma proporzionato delle più moderne tecnologie), ha rimarcato la necessità che in tale ambito – dove è labile il confine tra notizie smaccatamente false, volte ad esempio a disorientare volontariamente chi le riceve, e altre invece più "semplicemente" oggetto di possibile diversa interpretazione – ogni trattamento di dati sia improntato alla più rigorosa correttezza e abbia ad oggetto informazioni esatte ed aggiornate, segnatamente nei casi in cui dati personali riferiti a persone identificate o identificabili siano contenuti nei messaggi sottoposti a verifica (cfr. art. 5, par. 1, lett. *a*) e *d*), del RGPD) (si pensi, ad es., per rimanere in un ambito strettamente correlato al Covid-19, alle notizie sulle origini dell'epidemia o sulla necessità dell'uso dei dispositivi di protezione, oggetto di dibattito anche nell'ambito della comunità scientifica). L'Autorità ha poi ricordato come le implicazioni di ordine individuale e collettivo che possono derivare da una "malainformazione", anche quale possibile minaccia per la democrazia e la sovranità di un Paese (si pensi al caso

Cambridge Analytica), erano state sottolineate dal Presidente del Garante nell'audizione informale tenuta il 3 marzo 2020 presso le Commissioni riunite Trasporti e Cultura della Camera, nell'ambito dei lavori per l'approvazione di alcune proposte di legge (AC 1056 e abb.) recanti l'istituzione di una Commissione parlamentare di inchiesta sulla diffusione intenzionale, seriale e massiva di informazioni false (cfr. par. 3.1.1).

Per quanto riguarda la struttura del progetto, pur ritenendo meritevole di considerazione l'adozione di sistemi e strumenti che si propongano quale fine generale di contenere la divulgazione e la circolazione di *fake news*, specie rispetto a scorrette e pericolose prassi sanitarie, l'Autorità ha riferito di non essere in possesso di elementi sufficienti per valutarne la conformità ai principi, alle regole e al quadro di garanzie previste per il trattamento dei dati personali dalla normativa europea e nazionale di riferimento. A tal riguardo, il Garante ha informato il Ministero di avere avviato le opportune interlocuzioni con Agcom – che ha sottoposto a monitoraggio l'iniziativa quale possibile progetto pilota – al fine di realizzare un comune approfondimento ad ampio spettro del tema, avente profili la cui tutela è affidata, *pro quota*, a ciascuna delle due Autorità. All'esito di tali interlocuzioni è stato così istituito tra le due Autorità un tavolo tecnico congiunto ove approfondire la tematica della disinformazione *online* (cfr. par. 12.8).

Nella risposta scritta fornita all'interrogante dal competente Ministero dello sviluppo economico in data 14 settembre 2020 si è preso atto di quanto riportato dall'Autorità circa l'indisponibilità, allo stato, di sufficienti elementi di valutazione del progetto e si sono riportati gli elementi forniti da Agcom, che pure era stata interpellata sul merito dell'atto di sindacato ispettivo riguardante, prevalentemente, i rischi legati alla libertà di espressione.

Numerosi, inoltre, sono stati gli atti di sindacato presentati in Parlamento su temi di interesse per l'Autorità, alcuni dei quali, conclusi con la risposta del rappresentante del Governo. In particolare, si segnalano:

- tre interrogazioni a risposta scritta (nn. 4-03145, Buratti, 4-03678, Andreuzza, 4/04215, Licatini), presentate nella seconda metà del 2019 in materia di *telemarketing* e Registro delle opposizioni (Rpo), cui il Mise ha fornito riscontro con un unico atto in data 25 febbraio 2020. Tutte e tre vertevano, infatti, sulla stessa materia, vale a dire l'applicazione delle norme contenute nella legge n. 5/2018 recante nuove disposizioni in materia di iscrizione e funzionamento del registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato. Gli interroganti, nel rilevare la mancata adozione del regolamento previsto dall'art. 1, comma 15, della citata legge, destinato ad apportare modifiche a quello vigente (d.P.R. n. 178/2010), sottolineavano la necessità di recepire le osservazioni formulate sul relativo schema dal Garante nel parere del 30 aprile 2019, n. 109 (doc. web n. 9109315; cfr. Relazione 2019, p. 37), con particolare riferimento alla prospettata applicazione delle nuove disposizioni a specifiche categorie merceologiche rispetto alle quali rifiutare specificatamente le telefonate pubblicitarie e alla possibilità di dare il consenso alla ricezione di telefonate per un certo tipo di prodotti e negarlo per altri. Gli interroganti hanno ricordato che, nel parere, il Garante ha evidenziato che questa scelta è "di difficile esecuzione pratica" perché ci sono aziende che trattano prodotti di diverse categorie merceologiche, suggerendo pertanto di eliminare la distinzione per categorie. Nella risposta fornita, il Ministro dello sviluppo economico pro tempore, con riferimento all'*iter* di approvazione del suddetto regolamento, nel precisare che il provvedimento era stato approvato,

in via preliminare, dal Consiglio dei ministri del 17 gennaio 2020 e doveva essere sottoposto ai pareri del Consiglio di Stato e delle competenti Commissioni parlamentari, ha rilevato che si era dovuto attendere l'emanazione del d.P.R. 8 novembre 2018, n. 149, con il quale il Registro pubblico delle opposizioni è stato esteso agli indirizzi postali riportati negli elenchi telefonici. Nel frattempo il Ministero aveva istituito un tavolo tecnico con rappresentanti del Garante, dell'Agcom, della Fondazione Ugo Bordoni, dell'Istat e delle associazioni di categoria maggiormente rappresentative del settore del *telemarketing* per dirimere alcune questioni tecnico-giuridiche discendenti dal tenore letterale di talune disposizioni della legge n. 5/2018. Quanto alla possibilità di circoscrivere l'applicazione delle nuove disposizioni a specifiche categorie merceologiche, il Ministro ha affermato che lo schema di regolamento approvato in via preliminare ha recepito l'indicazione del Garante di eliminare tale riferimento, concludendo che con l'estensione del Registro alle numerazioni non presenti negli elenchi telefonici pubblici, in accordo alla legge n. 5/2018, si offrirà una soluzione contro il *telemarketing* aggressivo, garantendo un maggiore controllo del trattamento dei dati personali per finalità pubblicitarie (in tema di Registro pubblico delle opposizioni, si veda al par. 3.1.3 il riferimento all'ulteriore parere reso dal Garante il 10 dicembre 2020, n. 260, doc. web n. 9517462, sullo schema di regolamento in questione, come modificato dal Ministero sulla scorta dei pareri resi dal Consiglio di Stato, dall'Agcom e dal Garante stesso nel 2019; cfr. anche par. 11.1);

- interrogazione a risposta scritta n. 4-02517 (Muroni) presentata il 18 marzo 2019 alla Camera e indirizzata ai Ministri dell'interno e dello sviluppo economico, concernente una vicenda relativa alla diffusione, sui *social network*, di video tratti da telecamere pubbliche di videosorveglianza. Nel caso di specie, in seguito all'affissione di alcuni volantini di protesta in relazione alle politiche di un ente locale sugli asili nido, il sindaco del comune aveva pubblicato sul proprio profilo ospitato da un *social network* i volti di almeno quattro delle persone che avrebbero compiuto l'attacchinaggio ripresi dalle telecamere di sicurezza del comune. Secondo l'interpellante, tale comportamento andava stigmatizzato integrando una violazione della *privacy* delle persone coinvolte, anche in spregio al divieto di utilizzo delle immagini registrate dalle telecamere per fini estranei alle indagini, codificato nel regolamento del comune sulla videosorveglianza, in base al quale il comune può disporre l'installazione degli impianti di videosorveglianza esclusivamente a fini di prevenzione e repressione di fatti delittuosi mettendo i dati raccolti a disposizione delle sole Forze dell'ordine. Rispondendo all'interrogazione in data 25 febbraio 2020, il Sottosegretario di Stato per l'interno, nel confermare i fatti riportati e informare sugli sviluppi amministrativi della vicenda, ha ricordato la normativa in materia di videosorveglianza e protezione dei dati personali, a partire dal RGPD e dal d.lgs. n. 51/2018, fino al decreto-legge 23 febbraio 2009, n. 11, che costituisce la base giuridica del trattamento dei dati personali mediante strumenti di videosorveglianza, consentito esclusivamente (con le dovute garanzie) ai fini di tutela della sicurezza urbana. A tal riguardo, ha rilevato infine come la predetta normativa sia stata oggetto di chiarimento da parte del Garante con il provvedimento in materia di videosorveglianza dell'8 aprile 2010, che contiene prescrizioni vincolanti per tutti i soggetti pubblici e privati che intendano avvalersi di siffatti sistemi;
- interrogazione a risposta immediata in Commissione Affari costituzionali della Camera n. 5-03482 (Ceccanti-Sensi) riguardante l'utilizzo da parte delle

Forze di polizia italiane di sistemi informatici per il riconoscimento facciale. In particolare gli interroganti chiedevano informazioni sul Sistema automatico di riconoscimento delle immagini (SARI) in grado di identificare un soggetto ignoto confrontandone il volto tramite ricerche nella banca dati denominata Sistema automatizzato di identificazione delle impronte (*Automated Fingerprint Identification System* - AFIS) anche per i possibili riflessi sulla protezione dei dati delle persone (in concreto, inserendo nel SARI la fotografia di un sospettato, il sistema andrebbe a cercare i fotosegnalati che gli somigliano, precedentemente inseriti nel *database* AFIS). Nella risposta resa, il Sottosegretario all'interno Sibilia ha riferito che il Sistema automatico di riconoscimento immagini (SARI *Enterprise*) è gestito dalla Polizia di Stato e consente di risalire all'identità di un individuo mediante il confronto di volti su una lista di candidati selezionati dal sistema tra tutte le foto segnaletiche presenti nella banca dati AFIS, al momento riferite a 17.592.769 cartellini corrispondenti a 9.882.490 individui diversi, di cui 2.090.064 cittadini italiani. Viceversa, il SARI, essendo un *software* e non una banca dati, non contiene alcun dato. Il Sottosegretario ha precisato che le immagini utilizzate per effettuare le ricerche con il SARI sono acquisite dagli uffici di polizia operanti nell'ambito di indagini relative ad un procedimento penale e trasmesse dal Servizio per la cooperazione internazionale di polizia (Scip) della Direzione centrale della Polizia criminale nell'alveo delle attività di specifica competenza. Infine, il citato *software* sarebbe utilizzabile esclusivamente da parte di operatori appartenenti alla Polizia di Stato e all'Arma dei Carabinieri, previa formazione e abilitazione al suo impiego.

Al riguardo, può aggiungersi che il Garante ebbe ad esprimersi sul sistema SARI *Enterprise* con il provvedimento del 26 luglio 2018, n. 440 (doc. web n. 9040256), non riscontrandovi criticità sotto il profilo della protezione dati. Diversa valutazione è stata invece riservata al distinto sistema SARI *Real-time* – allo stato non ancora attivo – che consentirebbe, attraverso una serie di telecamere installate in un'area geografica delimitata, di analizzare in tempo reale i volti dei soggetti ivi ripresi, confrontandoli con una banca dati predefinita (denominata *watch list*): rispetto a tale sistema, ritenuto privo di una base giuridica che legittimi il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza e suscettibile di realizzare, per come è progettato, una forma di sorveglianza indiscriminata, il Garante ha espresso parere non favorevole (provv. 25 marzo 2021, n. 127, doc. web n. 9575877).

Più atti di sindacato ispettivo hanno impegnato il Governo a rispondere sugli aspetti applicativi del sistema di allerta per il tracciamento delle persone affette da Covid-19 (cd. *contact tracing*), mediante l'applicazione Immuni. Ci si riferisce in particolare ai seguenti:

- interrogazione a risposta scritta 4-03475 (Rauti ed altri), presentata il 19 maggio 2020 alla Camera dei deputati, concernente i criteri di selezione della *app* di *contact tracing* prescelta e i limiti del suo funzionamento. L'interrogante, premesso che il Gruppo di lavoro *data-driven* istituito per l'emergenza Covid-19 aveva selezionato, tra le 319 proposte pervenute, la *app* Immuni, peraltro non ancora realizzata, né disponibile; che il 29 aprile il Consiglio dei ministri aveva approvato un decreto-legge che ha previsto l'installazione, presso il Ministero della salute, di una piattaforma per il *contact tracing* e la pseudonimizzazione dei dati, anziché l'anonimizzazione, ossia una procedura che consentirebbe a chi dispone della chiave per associare le informazioni di risalire a quelle originarie; che il previsto tracciamento tramite *bluetooth*

poteva compromettere l'efficacia stessa dell'*app*, mentre la centralizzazione della base dati porrebbe seri problemi di sicurezza, l'interrogante chiedeva di sapere: quali fossero stati i criteri di selezione che avevano portato alla scelta della società poi selezionata; come si ritenesse di garantire, da un lato, la sicurezza delle applicazioni e dei *server* (conservazione sicura dei dati memorizzati, scambi tra le *app* e il *server* remoto, ecc.) in relazione alla tutela delle libertà e dei diritti costituzionali e, dall'altro, il rispetto del principio di minimizzazione dei dati previsto dal RGPD, evitando la reidentificazione dei soggetti che avrebbero scaricato l'*app*; per quale ragione il citato decreto-legge avesse previsto l'utilizzo dei dati per scopi ulteriori rispetto alla gestione della crisi sanitaria e come si intendesse garantire la distruzione definitiva dei dati fissata per il 31 dicembre 2020. All'interrogazione ha risposto, in data 16 giugno 2020, la Ministra per l'innovazione tecnologica e la digitalizzazione pro tempore la quale, rispetto ai profili aventi impatto sulla protezione dei dati, ha precisato che: a) per quanto attiene alla procedura di selezione ed assegnazione della soluzione tecnologica di *contact tracing*, sulla base di una relazione del citato Gruppo di lavoro, l'*app* Immuni era risultata la più idonea come base per la realizzazione del sistema nazionale di *contact tracing* digitale e il successivo contratto stipulato con la società sviluppatrice dell'*app* ha avuto il solo scopo di assicurare al Governo un suo contributo a fronteggiare l'emergenza da Covid-19, vale a dire la licenza d'uso aperta, gratuita, perpetua e irrevocabile del codice sorgente e di tutte le componenti dell'*app* Immuni, con l'impegno a completare gli sviluppi *software* necessari per la messa in esercizio del sistema nazionale di *contact tracing*. In sostanza, si trattava dell'inizio di un percorso funzionale a successive verifiche e adattamenti tecnici volti a garantire sia l'ottenimento della massima efficacia possibile del sistema individuato, sia l'aderenza del medesimo sistema e delle sue modalità di funzionamento alle normative italiane ed europee sul rispetto della *privacy* in un quadro di sicurezza; b) con riferimento al necessario rispetto del principio di minimizzazione nel trattamento dei dati al fine di escludere la reidentificazione dei soggetti, la necessità del rinvio alle specifiche tecniche di cui è stata promossa la pubblicazione; c) l'*app* non raccoglie alcun dato di geolocalizzazione degli utenti, ma registra esclusivamente i codici randomici inviati dai dispositivi di altri utenti dell'*app* mediante la tecnologia *bluetooth low energy*. L'applicazione può essere scaricata gratuitamente e volontariamente su telefoni con sistema operativo iOS e Android, non accede alla rubrica, non invia sms e non chiede il numero di telefono all'utente. Una volta attivata, l'*app* scambia con altri dispositivi che l'hanno installata codici, generati randomicamente (e che cambiano frequentemente), che non permettono di risalire all'identità dell'utente. Lo scambio è bidirezionale: ogni *smartphone* invia il proprio codice randomico e riceve i codici randomici degli *smartphone* nelle vicinanze, salvandoli nella propria memoria interna; d) la distruzione definitiva dei dati viene assicurata mediante cancellazione di quelli raccolti nel *database* e nelle copie di *backup* e, comunque, in caso di disinstallazione dell'*app;* e) ancora, nell'ottica di garantire la massima sicurezza e trasparenza, è stata inserita nell'ambito del decreto-legge 30 aprile 2020, n. 28, la disciplina del sistema di allerta Covid-19, al fine di assicurare un modello efficiente, solido anche dal punto di vista della *privacy*, capace al contempo di assicurare la più opportuna condivisione di informazioni epidemiologiche (art. 6, sul cui schema il Garante ha reso parere in data 29 aprile 2020, n. 79: cfr. parr. 3.1.2 e 5.1.1); f) in conformità alla raccomandazione della Commissione europea dell'8 aprile 2020 e ai principi

generali indicati dalla Commissione nel pacchetto di strumenti (*toolbox of practical measure*), il tracciamento dei contatti è fondato sul trattamento di dati di sola prossimità dei dispositivi, resi anonimi, oppure, ove ciò non sia possibile, pseudonimizzati. I dati relativi ai contatti stretti saranno conservati, anche nei dispositivi mobili degli utenti, per il periodo, stabilito dal Ministero della salute, strettamente necessario al tracciamento, e alla scadenza del termine cancellati in modo automatico. La Ministra ha infine precisato che nessun dato sarebbe raccolto da Apple e Google, che sono solo in grado di sapere che l'*app* di *contact tracing* è stata "scaricata", ma, per quanto dichiarato, non avrebbero accesso ad alcun dato dell'applicazione medesima;

- interrogazione a risposta immediata in Assemblea alla Camera n. 3-01808 (Lollobrigida ed altri), presentata in data 13 ottobre 2020, con la quale l'interrogante chiedeva la percentuale di cittadini che avessero scaricato l'*app* Immuni e le relative conseguenze in termini di efficacia dello strumento adottato a fini di tracciamento e di prevenzione, nonché le misure previste per rendere l'*app* accessibile a tutte le fasce della popolazione, perfezionando il rapporto con la medicina del territorio. Nella risposta resa il 14 ottobre 2020, la Ministra per l'innovazione tecnologica e la digitalizzazione ha riferito che l'*app* Immuni ha ricevuto una valutazione favorevole da un rapporto del Consiglio d'Europa nel quale si è sottolineata l'importanza di aver emanato in Italia una legge specifica nel rispetto dei diritti fondamentali della persona, come base e sviluppo dell'applicazione. Dopo aver riferito i numeri delle persone che allo stato risultavano dotate dell'applicazione, la Ministra ha ricordato che con il decreto-legge 7 ottobre 2020, n. 125 si è reso possibile l'utilizzo di Immuni anche "a livello europeo", grazie alla prevista interoperabilità con le piattaforme che operano, con le medesime finalità, nel territorio dell'Unione europea (su uno schema di tale norma l'Autorità ha avuto modo di interloquire con i competenti uffici del Ministero fornendo indicazioni utili a conformarla ai principi e alle regole di protezione dati e, successivamente, di fornire elementi di valutazione al Parlamento a richiesta della Commissione del Senato competente ad esaminare il disegno di legge di conversione del decreto: cfr., rispettivamente, parr. 3.1.1 e 3.1.2). Nel dibattito in Aula che ha fatto seguito all'intervento della Ministra è stata sottolineata l'importanza di rispettare, durante il periodo di emergenza sanitaria, le prescrizioni fornite in materia di *app* Immuni dal Garante al Ministero della salute con il provvedimento del 1° giugno 2020, n. 95 (doc. web n. 9356568: cfr. par. 5.1.2);
- interrogazione a risposta immediata in Assemblea alla Camera n. 3-01862 (Volpi) presentata il 3 novembre 2020, concernente l'istituzione del servizio nazionale di risposta telefonica per la sorveglianza sanitaria, con particolare attenzione all'attribuzione delle competenze per l'efficace funzionamento dell'*app* Immuni e all'adeguata formazione di tutti gli operatori coinvolti. L'interrogante lamentava, in base ai dati sui *download* dell'*app* e ai tracciamenti effettuati grazie a Immuni, che il sistema di tracciamento non procedesse con efficienza, principalmente a causa della mancata immissione nel sistema, ad opera di gran parte delle Asl, del nominativo delle persone che autorizzano il trattamento dei loro dati, chiedendo quindi al Governo di chiarire tempestivamente in capo a chi fosse radicato il compito di eseguire le procedure per il "caricamento" dei dati e l'invio delle notifiche, nonché per garantire un'adeguata formazione e informazione a tutti gli operatori coinvolti nei *call center* e nelle Asl, inclusi i medici di medicina generale. Rispondendo all'interrogante, in data 14 ottobre 2020, la Ministra ha fatto riferimento all'art. 20, d.l. 28

febbraio 2020, n. 137 (cd. Ristori) che ha previsto l'integrazione tra il sistema di tracciamento regionale sull'*app* Immuni con il servizio nazionale di supporto telefonico e telematico. Gli operatori di questo sistema potranno caricare il codice chiave in caso di positività; quindi, rispetto alla fase precedente, in cui questa funzione era esclusivamente riservata al personale dei dipartimenti di prevenzione delle aziende sanitarie regionali, si è previsto un altro punto di accesso per l'inserimento dei codici chiave; con il d.P.C.M. 18 ottobre 2020 tale adempimento è divenuto obbligatorio per il personale dell'azienda sanitaria. Per quanto riguarda il servizio nazionale di supporto telematico e telefonico, ha informato l'Aula di aver delegato la disciplina dell'organizzazione e del funzionamento del servizio al Commissario straordinario, secondo quanto previsto dal comma 3 del menzionato articolo 20 (sullo schema di ordinanza del Commissario, successivamente adottata il 19 dicembre 2020, n. 34, l'Autorità ha reso parere il 17 dicembre 2020, n. 273, doc. web n. 9516719: cfr. par. 5.1.4).

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

L'attività svolta dal Garante

RELAZIONE ANNUALE
2020

II - L'attività svolta dal Garante

4 Il Garante e le amministrazioni pubbliche

4.1. *L'attività fiscale e tributaria*

4.1.1. La cd. dichiarazione dei redditi precompilata

In più occasioni il Garante si è pronunciato con riguardo alla realizzazione della cd. dichiarazione dei redditi precompilata: in particolare, in relazione agli schemi di decreto del Mef e con riguardo a schemi di provvedimento dell'Agenzia delle entrate, adottati ai sensi dell'art. 3, commi 4 e 5, d.lgs. 21 novembre 2014, n. 175.

Adeguamento del tracciato del Sistema TS

Con un decreto, il Ministero ha inteso estendere il novero delle informazioni da trasmettere telematicamente all'Agenzia delle entrate sì da ricomprendere quelle concernenti le spese di istruzione scolastica da parte dei soggetti costituenti il sistema nazionale di istruzione. In relazione ad esso il Garante ha espresso parere favorevole, avendolo ritenuto conforme alla normativa in materia di protezione dei dati personali e alle garanzie già approntate nell'ambito della raccolta dei dati necessari all'elaborazione della dichiarazione precompilata (provv. 6 febbraio 2020, n. 25, doc. web n. 9283865).

In attuazione di tale decreto è stato sottoposto al Garante lo schema di provvedimento del Direttore dell'Agenzia delle entrate volto a definire le specifiche tecniche della trasmissione dei dati sulle spese di istruzione scolastica all'Anagrafe tributaria. Tenendo in considerazione le indicazioni fornite dall'Ufficio, tale schema ha introdotto ulteriori garanzie, con particolare riferimento ai dati relativi alle erogazioni liberali a favore degli istituti scolastici non deliberate dagli organi scolastici, in quanto suscettibili di implicare il trattamento di categorie particolari di dati personali, stabilendone la tempestiva e integrale cancellazione dall'archivio in caso di esercizio dell'opposizione da parte dell'interessato o di mancato accesso alla dichiarazione precompilata entro la data in cui viene resa disponibile la dichiarazione precompilata relativa all'anno successivo.

Trattandosi di garanzie analoghe a quelle già previste per le erogazioni liberali agli enti del terzo settore e rilevato che i canali di trasmissione dei dati da parte dei soggetti obbligati nonché le relative misure di sicurezza risultavano essere già stati favorevolmente valutati dall'Autorità, il Garante ha espresso parere favorevole (provv. 15 ottobre 2020, n. 182, doc. web n. 9483510).

Accesso alla dichiarazione precompilata

Il Garante si è espresso nuovamente anche sullo schema di provvedimento del Direttore dell'Agenzia delle entrate che individua le modalità tecniche per consentire al contribuente o agli altri soggetti autorizzati di accedere alla dichiarazione precompilata resa disponibile in via telematica. In particolare, l'Autorità ha valutato gli esiti della sperimentazione avviata nel 2018 che ha consentito ad alcuni Caf (espressamente individuati) di accedere, "in cooperazione applicativa con cornice di sicu-

rezza", alle dichiarazioni dei redditi precompilate e alle informazioni attinenti alla dichiarazione 730 precompilata disponibili presso l'Agenzia delle entrate. In esito a tale sperimentazione è emersa l'efficacia dell'utilizzo del codice *hash* quale misura di sicurezza calcolato sul *file* PDF composto dalla delega rilasciata dal contribuente e dal documento di riconoscimento. Al fine di semplificare gli adempimenti per i Caf, l'Agenzia ha proposto di imporre (a partire dal 2020) il calcolo del predetto codice *hash* sulla sola delega e non anche sul documento di identità del delegante, anche considerato che le specifiche tecniche per lo scarico puntuale della dichiarazione 730 precompilata prevedono, tra l'altro, il numero e la data della delega, il tipo di documento del contribuente (carta identità, patente, passaporto o altro), il numero di documento di identità del contribuente delegante, e che, in sede di verifica, su richiesta dell'Agenzia, il Caf è comunque tenuto a esibire il documento di riconoscimento del contribuente indicato in sede di scarico puntuale e la delega che ha generato il codice.

Anche in questo caso il Garante ha espresso parere favorevole, ritenendo in ogni caso necessario che l'Agenzia delle entrate prosegua la propria attività di controllo a campione sulla legittimità degli accessi alla cd. precompilata effettuati in generale dai Caf nel corso del 2020, tenendo altresì conto delle modalità che disciplinano l'assistenza fiscale a distanza introdotta in considerazione dell'emergenza epidemiologica da Covid-19; gli esiti di tali controlli dovranno essere trasmessi al Garante (provv. 23 aprile 2020, n. 77, doc. web n. 9347298).

Spese di istruzione scolastica

Con l'art. 1, commi 679 e 680, l. 27 dicembre 2019, n. 160 (legge di bilancio 2020) il legislatore ha previsto che, per ottenere la detrazione fiscale di alcune tipologie di spesa, sia necessario avvalersi di mezzi di pagamento elettronici, versamenti bancari o postali ovvero di altri sistemi che assicurano la tracciabilità, specificando al contempo che tale limitazione non trova applicazione in relazione alle spese sostenute per l'acquisto di medicinali e di dispositivi medici nonché per prestazioni sanitarie rese dalle strutture pubbliche o da strutture private accreditate al Ssn. Sono state inoltre approvate modifiche alla disciplina in materia di fatturazione elettronica per gli operatori sanitari e di memorizzazione elettronica e trasmissione telematica dei corrispettivi giornalieri (cfr. art. 15, d.l. 26 ottobre 2019, n. 124).

Per effetto di tali novelle legislative, la Ragioneria generale dello Stato ha sottoposto al Garante uno schema di decreto del Mef per l'adeguamento del tracciato del Sistema tessera sanitaria (Sistema TS) ai fini della trasmissione dei dati relativi alle spese sanitarie e veterinarie per la dichiarazione precompilata, includendo tra questi la modalità di pagamento, il tipo di documento fiscale e l'aliquota ovvero la natura della singola operazione ai fini Iva, con esclusione delle casistiche di spese sanitarie e veterinarie indicate dalla legge.

Il Garante ha reso parere favorevole sullo schema di decreto nel quale, anche sulla base delle indicazioni fornite dall'Ufficio, si sono individuate garanzie per dare attuazione ai principi in materia di protezione dei dati personali; è stata esclusa, infatti, la trasmissione all'Agenzia, a fini della fatturazione elettronica, dei codici fiscali degli assistiti; la raccolta del codice fiscale dell'interessato da parte del Sistema TS in relazione alle spese che non danno diritto alla detrazione è prevista al solo fine di consentire eventuali rettifiche dei dati erroneamente trasmessi, che verranno cancellati una volta scaduti i termini previsti per la presentazione della dichiarazione dei redditi. Rimane esclusa la trasmissione del codice fiscale in caso di opposizione da parte dell'assistito alla messa a disposizione dei dati all'Agenzia per la predisposizione della dichiarazione dei redditi precompilata, come anche la trasmissione all'Agenzia del codice fiscale degli assistiti con riferimento alle fatture emesse in relazione a prestazioni sanitarie relative ai periodi d'imposta interessati (provv. 9 luglio 2020, n. 132, doc. web n. 9441223).

Il Garante è stato quindi chiamato a esprimersi anche su due schemi di provvedimento del Direttore dell'Agenzia delle entrate che hanno dato attuazione al decreto sopra illustrato; sugli stessi non sono stati sollevati rilievi in quanto, da una parte, le specifiche tecniche per la trasmissione dei dati sulle spese sanitarie e veterinarie al Sistema TS erano già definite (da ultimo) dal citato schema di decreto ministeriale; dall'altra, con riferimento agli altri oneri detraibili, non sono state definite nuove specifiche tecniche rispetto a quelle già previste, rimaste invariate rispetto all'impianto precedente (provv. 1° ottobre 2020, n. 177, doc. web n. 9478015).

4.1.2. La fatturazione elettronica

Il Garante è stato chiamato nuovamente ad esprimersi sulla questione della fatturazione elettronica in relazione all'attuazione dell'art. 14, d.l. 26 ottobre 2019, n. 124, convertito dalla legge 19 dicembre 2019, n. 157, che introduce la memorizzazione dei *file* XML delle fatture.

Rilievi critici erano stati espressi dal Presidente dell'Autorità con la memoria inviata alla Commissione VI Finanze della Camera dei deputati in relazione al disegno di legge di conversione C. 2220 del 5 novembre 2019 (doc. web n. 9178137), in linea con quanto già rilevato dall'Autorità nei provvedimenti del 15 novembre 2018, n. 481 (doc. web n. 9059949) e del 20 dicembre 2018, n. 511 (doc. web n. 9069072), nei quali si era ritenuta sproporzionata la memorizzazione di dati non fiscalmente rilevanti e inerenti alla descrizione delle prestazioni fornite.

In particolare, l'Agenzia ha trasmesso all'Autorità un nuovo schema di provvedimento del Direttore volto ad attuare il predetto articolo, disciplinando la memorizzazione e l'utilizzo dei *file* XML delle fatture elettroniche e prevedendo, rispetto al quadro vigente individuato sulla base del menzionato provvedimento del 20 dicembre 2018, la memorizzazione dei cd. dati fattura integrati con le informazioni relative a natura, qualità e quantità dei beni e dei servizi oggetto dell'operazione (ovvero la descrizione dell'oggetto della fattura), nonché la memorizzazione integrale dei *file* XML delle fatture, utilizzabili da parte del personale centrale e delle strutture territoriali dell'Agenzia delle entrate specificatamente autorizzato nell'ambito di alcune attività istruttorie. È stata prevista, inoltre, la stipula di una convenzione con la Guardia di finanza per la messa a disposizione dei *file* delle fatture elettroniche e dei dati fattura integrati per le attività di polizia economica e finanziaria ai sensi dell'art. 1, comma 5-*bis*, d.lgs. n. 127/2015.

Nel parere, il Garante ha osservato che l'Agenzia, nel dare attuazione alla disposizione, ha previsto la memorizzazione e l'utilizzo dei *file* delle fatture elettroniche che contengono i dati inerenti alla natura, qualità e quantità dei beni e servizi oggetto dell'operazione economica, estendendo così tanto l'oggetto della memorizzazione, quanto l'ambito di utilizzazione dei dati presenti nella fattura elettronica. Ciò senza nemmeno escludere alcune tipologie di dati, quali quelli non rilevanti a fini fiscali o relativi alla descrizione delle prestazioni fornite, suscettibili di comprendere anche dati appartenenti a categorie particolari o l'eventuale sottoposizione dell'interessato a procedimenti penali – si pensi alle fatture relative a prestazioni in ambito forense (cfr. artt. 9 e 10 del RGPD) –, né i codici fiscali dei consumatori (quantomeno per fatture relative a spese non detraibili).

Il Garante ha rilevato che la previsione della memorizzazione e dell'utilizzazione, senza distinzione alcuna, dell'insieme dei dati personali contenuti nei *file* delle fatture elettroniche, anche laddove si assicurino elevati livelli di sicurezza e accessi selettivi, risulta sproporzionata in uno stato democratico, per quantità e qualità delle informazioni oggetto di trattamento, rispetto al perseguimento del legittimo obiettivo di interesse pubblico di contrasto all'evasione fiscale; ciò pur tenendo conto che,

allo stato, le spese sanitarie trasmesse attraverso il Sistema TS sono escluse da tale previsione. L'Autorità aveva già invitato il legislatore a selezionare opportunamente le tipologie di informazioni trattate, che dovevano essere oggetto di specifica valutazione rispetto alle esigenze in concreto perseguite, al fine di non violare il principio di proporzionalità del trattamento dei dati sancito dal RGPD e assurto a parametro di legittimità in materia nella giurisprudenza della CGUE, della CEDU e della Corte costituzionale (cfr. sentenza n. 20/2019).

Nel parere, pertanto, il Garante ha ritenuto che lo schema di provvedimento introducesse un trattamento di dati in violazione degli artt. 5, par. 1, lett. *a*), 6, par. 3, 9, 10, 24 e 25 del RGPD, riguardante, peraltro senza distinzione alcuna tra tipologie di informazioni o categorie di interessati e dati personali di dettaglio, anche dati ulteriori rispetto a quelli necessari a fini fiscali, relativi alla totalità della popolazione, non proporzionato all'obiettivo di interesse pubblico (pur legittimo) perseguito, e senza che venissero individuate, in ossequio ai principi di *privacy by design* e *by default*, adeguate misure di garanzia per assicurare la protezione dei dati, anche in relazione a quelli di cui agli artt. 9 e 10 del RGPD (provv. 9 luglio 2020, n. 133, doc. web n. 9434785).

Con un successivo provvedimento, l'Autorità ha quindi preso atto della volontà dell'Agenzia di trasmettere una nuova bozza del provvedimento attuativo dell'art. 14, d.l. n. 124/2019, sostitutiva del precedente, e della conseguente esigenza di prorogare al 1° marzo 2021 il termine per l'adesione al servizio di consultazione dei *file* XML delle fatture elettroniche allo stato memorizzate e, correlativamente, per l'eventuale cancellazione dei *file* XML in caso di mancata adesione da parte degli operatori economici e dei consumatori (provv. 7 agosto 2020, n. 151, doc. web n. 9451049).

4.1.3. Bonus *vacanze*

L'art. 176, d.l. 19 maggio 2020, n. 34, ha stabilito che, per il periodo d'imposta 2020, è riconosciuto un credito in favore dei nuclei familiari con Isee in corso di validità non superiore a 40.000 euro, utilizzabile dal 1° luglio al 31 dicembre 2020 per il pagamento di servizi offerti dalle imprese turistico ricettive, dagli agriturismi e dai *bed and breakfast*. Tale credito (cd. *bonus* vacanze) era utilizzabile da un solo componente per nucleo familiare e veniva riconosciuto a condizione che, tra l'altro, le spese fossero sostenute in un'unica soluzione e il totale del corrispettivo fosse documentato da fattura elettronica o documento commerciale da trasmettersi telematicamente all'Agenzia delle entrate, recante il codice fiscale del soggetto che intendeva fruire del credito. Ai sensi dell'art. 5, comma 6, d.l. 28 ottobre 2020, n. 137, il *bonus* vacanze è diventato utilizzabile fino al 30 giugno 2021, purché richiesto entro il 31 dicembre 2020.

L'attuazione di questa misura era rimessa ad un provvedimento del Direttore dell'Agenzia delle entrate, da adottare sentito l'Inps con riferimento agli aspetti concernenti la verifica della sussistenza di una Dsu in corso di validità per Isee non superiore a 40.000 euro. Lo schema di provvedimento in questione – secondo il quale la richiesta dell'agevolazione poteva essere effettuata da uno qualunque dei componenti del nucleo familiare esclusivamente mediante l'*app* per dispositivi mobili denominata "IO" (APP IO), resa disponibile da PagoPA e accessibile tramite Spid o Carta di identità elettronica (Cie) – è stato poi sottoposto al Garante per il prescritto parere.

In questa sede, pur rilevando il recepimento di alcune indicazioni fornite dall'Ufficio nel corso delle riunioni tecniche, il Garante ha comunque riscontrato la permanenza di alcuni profili di criticità, a partire dai rapporti con PagoPA (quale responsabile del trattamento) e in relazione ai tempi di conservazione dei dati. Soprattutto,

i principali rilievi hanno riguardato l'utilizzo dell'APP IO (sulla quale v. *infra* par. 4.1.4), che costituisce punto di accesso telematico in rete della p.a. ai sensi dell'art. 64-*bis*, d.lgs. 7 marzo 2005, n. 82, attivato in via sperimentale e la cui autorizzazione è sottoposta ad approfondimenti da parte dell'Autorità. In particolare, il Garante ha evidenziato che: le modalità di autenticazione informatica da parte dell'utente dovevano avvenire in conformità ai paradigmi e protocolli previsti da AgID con riferimento all'utilizzo di Spid; le notifiche *push*, previa adeguata informazione, dovevano essere disattivabili dall'utente e, comunque, non dovevano fornire indicazioni di dettaglio relative al mittente e al contenuto del messaggio oggetto della notifica (limitandosi a rinviarlo all'*app* stessa); non doveva essere prevista l'adesione automatica a tutti i servizi già disponibili sull'APP IO, assicurando agli utenti la facoltà di scegliere gli enti da cui ricevere la predetta messaggistica (cd. modalità *opt-in*); occorreva adottare adeguate garanzie, anche in termini di trasparenza, con riferimento al trasferimento di dati personali verso Paesi terzi, alla luce della sentenza della Corte di giustizia (Grande Sezione) del 16 luglio 2020, C-311/18, Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems (cd. Schrems II).

In ragione di tutto ciò, il Garante ha espresso parere favorevole sullo schema di provvedimento del Direttore dell'Agenzia delle entrate ed ha autorizzato l'Agenzia ad effettuare il trattamento, finalizzato all'erogazione del *bonus* vacanze, ai sensi dell'art. 58, par. 3, lett. *c*), del RGPD e dell'art. 2-*quinquiesdecies* del Codice, nel rispetto delle citate prescrizioni (provv. 12 giugno 2020, n. 102, doc. web n. 9367375).

4.1.4. Cashback

Il Garante ha espresso parere positivo sulla bozza di regolamento che definisce il funzionamento del programma di rimborso in denaro (cd. *cashback*) a favore dei consumatori che effettuano acquisti con strumenti di pagamento elettronici, nell'ambito del quale dovranno però essere adottate precise misure a garanzia dei dati personali. In base allo schema presentato dal Mef (cfr. par. 3.1.4), i consumatori potranno scegliere di aderire al programma *cashback* tramite l'APP IO o attraverso banche o società che emettono carte di pagamento (*issuer*). In questo modo i dati anagrafici e gli estremi delle carte di pagamento scelte per partecipare al programma saranno comunicati a PagoPA, la società incaricata dal Mef della progettazione e della gestione del sistema informativo *cashback*.

Ogni volta che la carta di pagamento registrata sarà utilizzata dal consumatore per l'acquisto in negozio, i dati necessari (es., data e importo dell'acquisto) saranno trasmessi dalla società che gestisce la transazione (*acquirer*) al sistema *cashback*. Al termine di ogni semestre sarà calcolato il rimborso spettante a ciascun consumatore aderente al programma sulla base degli importi dei pagamenti effettuati. Sono previsti rimborsi speciali, sulla base di una graduatoria, per chi avrà eseguito il maggior numero di transazioni. Sarà Consap (società del Mef) ad occuparsi dell'erogazione dei rimborsi, inclusa la gestione dell'eventuale contenzioso.

Nel corso dell'istruttoria, alla luce dei rischi e delle criticità emerse nell'ambito di un trattamento di dati così massivo, riferibile ad ogni aspetto della vita quotidiana dell'intera popolazione, il Garante ha chiesto di stabilire già nel regolamento stringenti garanzie a tutela delle persone coinvolte. È stato innanzitutto necessario individuare espressamente i ruoli e le singole responsabilità dei numerosi soggetti coinvolti nel trattamento dei dati; sono state introdotte misure per garantire che gli *acquirer* trasmettano al sistema solamente i dati necessari, limitati alle transazioni effettuate attraverso gli strumenti di pagamento registrati dai soggetti aderenti. L'Autorità ha altresì chiesto di precisare le finalità del trattamento delle diverse tipologie di dati raccolti nell'ambito del programma di rimborso, con particolare riguardo ai

dati dell'esercente che potranno essere trattati solo per eventuali reclami; anche i dati raccolti potranno essere conservati solo per il tempo strettamente necessario.

Il Garante ha evidenziato la necessità di valutare in sede attuativa le modalità con cui l'APP IO e i sistemi con i quali gli istituti bancari e le società emittenti carte di pagamento rendono disponibili agli aderenti gli importi dei rimborsi spettanti e la posizione nella graduatoria, in modo che siano conformi al principio di minimizzazione previsto dal RGPD. È stata prevista l'adozione di specifiche misure di sicurezza atte a garantire la protezione, mediante funzioni crittografiche non reversibili, degli identificativi degli strumenti di pagamento elettronici.

L'Autorità si è riservata, infine, di verificare, prima dell'avvio del programma, le misure di sicurezza, le modalità e i tempi di conservazione dei dati che il Ministero dovrà indicare nella valutazione d'impatto (provv. 13 ottobre 2020, n. 179, doc. web n. 9466707), oggetto di valutazione con il parere 26 novembre 2020, n. 232 (doc. web n. 9492345). Tale valutazione, a seguito delle interlocuzioni avvenute con l'Ufficio, è stata integrata con misure volte a prevedere che siano raccolti e trattati, in relazione ad ogni specifica finalità perseguita, esclusivamente i dati necessari, in conformità a quanto previsto dal decreto. Il Garante ha richiesto, in particolare, che nella valutazione fossero descritte accuratamente le operazioni e le modalità di trattamento, con specifico riferimento alla fase di adesione al programma, al censimento degli strumenti di pagamento nell'APP IO e alle verifiche effettuate sull'Iban indicato dall'aderente per il pagamento dei rimborsi. L'Autorità ha inoltre ritenuto necessario che fossero individuati meccanismi volti a garantire che l'aderente possa registrare solamente strumenti di pagamento a lui intestati, impedendo così la visualizzazione di spese effettuate da terzi.

Nella valutazione è stato poi specificato il ruolo assunto dai soggetti coinvolti nei trattamenti di dati personali necessari alla realizzazione del progetto *cashback*, in relazione alle diverse finalità perseguite, anche al fine di assicurare la trasparenza nei confronti degli interessati nonché di consentire una chiara ripartizione degli obblighi e delle responsabilità previste dal RGPD in un trattamento così complesso. Sono state individuate misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento anche attraverso tecniche di segnalazione (*alerting*) e di rilevazione delle anomalie (*anomaly detection*) in relazione alle diverse componenti del sistema *cashback*, sulla base di parametri quantitativi e qualitativi, nonché garantendo l'integrità e la non ripudiabilità dei dati presenti nei *file* oggetto di scambio tra i soggetti coinvolti nel trattamento attraverso la firma digitale degli stessi. È stato altresì richiesto che nella valutazione fossero individuati tempi e modalità di conservazione dei dati, assicurando che gli stessi siano trattati solo per il tempo necessario al conseguimento delle finalità perseguite e prevedendo, per ciascuna di esse, modalità di conservazione differenziate anche in ragione del tempo trascorso dalla loro raccolta. Particolari cautele sono state suggerite per l'individuazione di adeguate garanzie per i trattamenti che comportano il trasferimento dei dati personali verso Paesi terzi, anche tenendo conto della sentenza della Corte di giustizia (Grande Sezione) del 16 luglio 2020, C-311/18, Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems (cd. Schrems II).

Infine, il Ministero si è impegnato a informare il Garante riguardo alle misure che, in accordo con PagoPA, saranno adottate o pianificate per assicurare idonee modalità di verifica dell'intestazione all'aderente degli strumenti di pagamento, nonché a evitare la registrazione di *default* dei suddetti strumenti anche nell'ambito della piattaforma PagoPA.

Come già evidenziato in occasione del *bonus* vacanze (cfr. par. 4.1.3), il Garante si è riservato di esaminare i profili di funzionamento dell'APP IO gestita da PagoPA

in qualità di titolare del trattamento, in relazione ai quali la Società si è impegnata a osservare le misure e gli accorgimenti già prescritti nel menzionato provvedimento del 12 giugno 2020.

4.1.5. La fatturazione automatica

In ambito fiscale l'Autorità si è espressa sullo schema di decreto del Ministro per l'innovazione tecnologica e la digitalizzazione, da adottarsi di concerto con il Ministro dell'economia e delle finanze, volto alla definizione delle regole tecniche del servizio di fatturazione automatica, ai sensi dell'art. 5, comma 2-*septies*, del Cad (provv. 29 ottobre 2020, n. 200, doc. web n. 9487468). Il legislatore ha previsto l'istituzione di tale servizio per facilitare gli operatori economici nell'adempimento dell'obbligo di fatturazione elettronica; la sua realizzazione nell'ambito della piattaforma di cui all'art. 5, comma 2, del Cad (ovvero la piattaforma PagoPA) è affidata alla omonima società che dovrà garantirne la fruizione anche da parte di coloro che effettuano acquisti al di fuori dell'esercizio dell'attività di impresa, di un'arte o di una professione. Il servizio di fatturazione automatica si applica alle operazioni di pagamento effettuate presso Pos presenti sul territorio nazionale mediante l'utilizzo di carte di debito, carte di credito, carte prepagate, ivi inclusi gli strumenti di pagamento, nonché tramite applicazioni che consentono di effettuare bonifici di pagamento o tramite altri sistemi di pagamento messi a disposizione presso punti vendita presenti sul territorio nazionale. L'adesione al servizio è volontaria, sulla base di una registrazione distinta per gli esercenti e per i cessionari: a) gli esercenti si iscrivono al servizio (*una tantum*, con possibilità di modifica o cancellazione), direttamente o tramite soggetti terzi, tra i quali *l'acquirer* o il proprio fornitore di servizi di fatturazione elettronica; b) i cessionari, nell'APP IO o nei sistemi messi a disposizione dal proprio *issuer*, registrano uno o più strumenti di pagamento di cui intendono avvalersi per usufruire del servizio (*una tantum*, con possibilità di modifica o revoca), indicando anche gli estremi della propria partita iva ovvero del proprio codice fiscale.

Lo schema trasmesso al Garante ha tenuto conto delle indicazioni fornite dall'Ufficio nell'ambito delle interlocuzioni informali volte ad assicurare, in particolare, che il trattamento fosse progettato nel rispetto dei principi di proporzionalità e di *privacy by design* e *by default*, limitando la raccolta dei dati a quelli strettamente necessari alla finalità perseguita, senza accentrare, presso la Società, i dati relativi a tutte le transazioni commerciali eseguite con strumenti di pagamento elettronici, a prescindere dall'adesione all'iniziativa da parte dei cessionari e dal fatto che sia stata richiesta l'emissione della fattura all'atto dell'acquisto.

In particolare, il Garante ha posto l'attenzione sulle garanzie da introdurre a tutela dei diritti e delle libertà delle persone fisiche che, in qualità di cessionari, al di fuori dell'esercizio dell'attività di impresa e di un'arte o professione, intendano aderire al servizio di fatturazione automatica, con meccanismi che consentano di rispettare i requisiti del RGPD, attraverso la minimizzazione nella raccolta dei dati relativi alle transazioni rilevanti, la chiara definizione del ruolo assunto dai diversi soggetti coinvolti nel trattamento nonché la corretta individuazione dei flussi di dati necessari alla realizzazione dell'iniziativa per il compito di interesse pubblico. Specifiche cautele sono state previste per il trattamento dei dati relativi agli identificativi degli strumenti di pagamento elettronici indicati dai cessionari all'atto dell'adesione al servizio di fatturazione automatica che devono essere protetti tramite funzioni crittografiche non reversibili.

Il servizio di fatturazione automatica presenta rischi elevati per i diritti e le libertà degli interessati, derivanti dalla raccolta massiva e generalizzata di informazioni di dettaglio, potenzialmente riferibili ad ogni aspetto della vita quotidiana dell'inte-

ra popolazione, che richiedono specifiche valutazioni in ordine alla proporzionalità del trattamento e all'individuazione delle misure da adottare al fine di rispettare i requisiti del RGPD. È stato pertanto previsto che nella valutazione d'impatto da sottoporre all'esame del Garante siano indicate le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento e siano disciplinati i tempi e le modalità di conservazione dei dati trattati ai fini della fatturazione automatica, assicurando, nel rispetto del principio di limitazione della conservazione, che gli stessi siano conservati solo per il tempo necessario all'erogazione del servizio.

Anche in relazione a tale servizio, l'Autorità si è riservata di esaminare le specifiche caratteristiche dell'APP IO, con particolare riferimento alle osservazioni già formulate nel provvedimento del 12 giugno 2020, n. 102 (doc. web n. 9367375) circa il previsto utilizzo di notifiche *push*, l'attivazione automatica di servizi non espressamente richiesti dall'utente nonché il trasferimento di dati personali verso Paesi terzi.

4.1.6. La lotteria dei corrispettivi

Risolte le criticità legate alla riservatezza dei partecipanti, il Garante ha autorizzato l'avvio della cd. lotteria dei corrispettivi, esprimendo parere favorevole sul provvedimento dell'Agenzia delle dogane e dei monopoli, formulato d'intesa con l'Agenzia delle entrate, che ne disciplina lo svolgimento (provv. 13 febbraio 2020, n. 30, doc. web n. 9282901).

Il provvedimento sottoposto all'Autorità tiene conto delle numerose indicazioni fornite dall'Ufficio per rendere conforme al RGPD il trattamento di dati effettuato. Tra i numerosi profili approfonditi, particolare attenzione è stata posta sull'utilizzo del codice lotteria in luogo del codice fiscale; tale misura, attuativa dei principi di *privacy by design* e *by default*, è stata ritenuta infatti efficace per la tutela dei consumatori a fronte di una raccolta massiva e su larga scala di dati presso l'Agenzia delle dogane e dei monopoli, l'Agenzia delle entrate, e, per come è organizzata la lotteria, anche presso gli esercenti. Il codice lotteria, pseudonimo del codice fiscale, consente infatti di rendere le informazioni raccolte non riconducibili al singolo individuo in assenza di informazioni aggiuntive e permette al consumatore di non fornire all'esercente il codice fiscale (dal quale sono ricavabili anche informazioni su sesso, data e luogo di nascita, non necessarie per la partecipazione al concorso). L'Autorità ha ritenuto che le misure tecniche e organizzative individuate nello schema di provvedimento e nelle valutazioni di impatto effettuate dalle Agenzie fossero adeguate al rischio elevato che il concorso a premi comporta. Per partecipare alla lotteria, al momento dell'acquisto il consumatore deve esibire all'esercente il proprio codice lotteria in formato cartaceo o elettronico (ad es., codice a barre). Il codice, ottenuto utilizzando una funzione disponibile nell'area pubblica del "Portale lotteria" dell'Agenzia delle dogane e dei monopoli, generato casualmente, è composto da 8 caratteri alfanumerici e associato in modo univoco al codice fiscale. Ogni consumatore può generare più codici lotteria, tutti ugualmente validi ai fini del concorso. L'Agenzia delle entrate estrapola i dati necessari dai singoli scontrini trasmessi dagli esercenti (partita iva e denominazione dell'esercente, numero dello scontrino, data e ora dell'acquisto, importo, modalità di pagamento, codice lotteria) e li trasmette al "Sistema lotteria" dell'Agenzia delle dogane e dei monopoli, gestito con il supporto di Sogei. L'Agenzia delle dogane e dei monopoli converte in biglietti virtuali della lotteria i dati degli scontrini che, a maggior tutela dei consumatori, sono conservati separatamente dagli abbinamenti tra i codici fiscali e i codici lotteria. Successivamente all'estrazione dei biglietti, personale autorizzato dell'Agenzia delle dogane e dei monopoli può risalire all'identità del consumatore per attribuire e comunicare la vincita. Tutte le operazioni eseguite

devono essere tracciate in appositi *file* di log, conservati per 24 mesi. I dati potranno essere utilizzati solo ai fini della lotteria. Ogni ulteriore trattamento sarebbe, infatti, incompatibile in considerazione del contesto e delle modalità con le quali sono stati raccolti, non essendo prevista l'identificazione del consumatore né al momento della generazione del codice lotteria né in quello dell'acquisto. Il consumatore può accedere alla sezione riservata del Portale Lotteria per consultare gli scontrini e i biglietti virtuali associati, verificare le vincite ed esercitare i propri diritti in modo semplificato. Nella fase di prima applicazione, le prestazioni sanitarie e le fatture elettroniche non entreranno a far parte della lotteria, fino all'adozione di un successivo provvedimento, da adottare sentito il parere del Garante.

Successivamente l'Autorità ha espresso parere favorevole sullo schema di provvedimento, predisposto dall'Agenzia delle dogane e dei monopoli d'intesa con l'Agenzia delle entrate, che completa l'attuazione della lotteria dei corrispettivi, istituendo nuovi premi per i consumatori maggiorenni, residenti in Italia, che acquistano beni o servizi con strumenti di pagamento elettronici (*cashless*), ma anche per gli esercenti che emettono il relativo scontrino (provv. 1° ottobre 2020, n. 172, doc. web n. 9466165). Il nuovo provvedimento aggiorna di conseguenza l'entità, il numero dei premi messi a disposizione, le operazioni di estrazione e le modalità di attribuzione dei premi aggiuntivi per i consumatori che pagano l'intero importo *cashless* (ad es. tramite bancomat o carta di credito) e per i venditori che hanno emesso lo scontrino vincente. Lo schema tiene conto delle indicazioni fornite dal Garante nelle interlocuzioni sul progetto di lotteria avviate con le due Agenzie, così da assicurare la piena conformità al Regolamento anche in relazione alle novità da ultimo introdotte.

Infine, il Garante si è espresso favorevolmente sullo schema di provvedimento del Direttore dell'Agenzia delle entrate recante "Modifiche al provvedimento del Direttore dell'Agenzia delle entrate n. 739122 del 31 ottobre 2019, in tema 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 11 dicembre 2016, n. 232" (provv. 29 ottobre 2020, n. 212, doc. web n. 9489035). Lo schema stabilisce che i registratori telematici possono memorizzare esclusivamente, in via alternativa, il codice fiscale o il codice lotteria nella fase di registrazione dei dati dei corrispettivi della singola operazione commerciale realizzata, in coerenza con quanto disposto dal provvedimento interdirettoriale che disciplina la lotteria, in base al quale non partecipano al concorso gli acquisti per i quali il consumatore richieda all'esercente l'acquisizione del proprio codice fiscale a fini di detrazione o deduzione fiscale. Ad avviso del Garante, l'Agenzia ha così individuato garanzie adeguate per consentire la partecipazione alla lotteria anche ad acquisti effettuati presso esercenti che offrono anche beni e servizi detraibili o deducibili (specialmente farmacie), senza vanificare l'efficacia della prevista pseudonimizzazione del codice fiscale con il codice lotteria, che sarebbe stata compromessa dalla contemporanea presenza – nel registratore telematico e sul documento commerciale – di entrambi i codici, evitando anche disparità di trattamento tra esercenti che vendono uno stesso prodotto.

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

4.2.1. Anticipo Tfr/Tfs

In ambito previdenziale, il Garante si è espresso sullo schema di accordo quadro per l'anticipo del Tfs/Tfr in favore dei dipendenti delle amministrazioni pubbliche e degli enti di ricerca, di cui all'art. 23, comma 2, d.l. 28 gennaio 2019, n. 4, convertito, con modificazioni, dalla l. 28 marzo 2019, n. 26 (provv. 9 luglio 2020, n.

131, doc. web n. 9434908). Lo schema di accordo tra il Mef, il Ministero del lavoro, il Ministero per la pubblica amministrazione e l'Abi, cui possono aderire le banche e/o intermediari finanziari, disciplina le modalità di attuazione delle disposizioni in tema di anticipo del Tfs/Tfr (i termini e le modalità di adesione della banca, le modalità di presentazione della domanda di anticipo del Tfs/Tfr da parte del soggetto finanziato, nonché le modalità di comunicazione tra la banca e l'ente erogatore). L'Autorità ha richiamato la necessità che i titolari del trattamento (la banca e l'ente erogatore) adottino, nel rispetto del principio di *accountability* (artt. 5, par. 2, e 24 del RGPD), misure di sicurezza adeguate ai rischi presentati dal trattamento (art. 32 del RGPD), individuando procedure per la gestione delle violazioni dei dati personali (artt. 33 e 34 del RGPD) e provvedendo a valutare, in relazione alle modalità di trasmissione dei dati, l'adozione di tecniche di cifratura idonee a garantirne la riservatezza e l'integrità, anche laddove vengano previsti sistemi di comunicazione alternativi alla Pec.

4.2.2. Provvidenze

In più occasioni il Garante si è espresso in relazione a trattamenti di dati personali necessari per l'erogazione di benefici economici in favore di categorie di soggetti che si sono trovati in una situazione di disagio economico, soprattutto per effetto delle conseguenze causate dall'emergenza epidemiologica da Covid-19.

Misure di sostegno promosse dalla Regione Campania

Il Garante si è pronunciato favorevolmente, ai sensi dell'art. 2-*ter*, comma 2, del Codice, sul trattamento di dati personali connesso al riconoscimento di misure di sostegno economico nei confronti di persone stabilite nel territorio della Regione Campania. In particolare, anche a seguito delle interlocuzioni intercorse tra l'Ufficio e le Istituzioni interessate volte a evitare l'attivazione di una trasmissione massiva di dati individuali riguardanti i destinatari di prestazioni assistenziali e pensionistiche, l'Inps e la Regione hanno identificato modalità per l'individuazione dei beneficiari, nonché di erogazione, rispettose della protezione dei dati personali, rimettendo la gestione delle prestazioni esclusivamente all'Istituto e limitando le tipologie di informazioni oggetto di trasmissione alla Regione ai soli dati anonimi e aggregati con riferimento ai lavoratori stagionali impiegati in attività alberghiere ed extralberghiere. Per i percettori di pensioni/assegni sociali e di integrazione al trattamento minimo di pensione, è stata ammessa la trasmissione alla Regione di dati pseudonimizzati e, solo laddove necessari per finalità di controllo (e comunque non in forma massiva), anche di dati identificativi riferiti a singoli.

Per queste ragioni è stato necessario formulare rilievi sulla comunicazione di dati personali nei termini descritti, avendola ritenuta necessaria per assicurare (con urgenza) l'attivazione delle misure di sostegno economico a fronte dell'emergenza epidemiologica da Covid-19 e in linea con i principi di limitazione delle finalità e di minimizzazione dei dati, ferma restando l'adozione di adeguate misure per garantire la trasparenza nei confronti degli interessati e la sicurezza del trattamento, rimesse ad un'apposita convenzione tra le parti (provv. 28 aprile 2020, n. 78, doc. web n. 9335112).

Rendicontazione dei pagamenti concernenti la CIG in deroga

Analoga tipologia di comunicazione di dati personali, ai sensi dell'art. 2-*ter*, comma 2, del Codice, è stata sottoposta dall'Inps al Garante, con riferimento alla necessità di trasmettere alle autorità di gestione (cioè regioni e province autonome) informazioni concernenti i pagamenti effettuati dall'Istituto a fini di erogazione della cassa integrazione guadagni in deroga (CIG) (tra le quali i codici fiscali dei beneficiari) attivata per fronteggiare le conseguenze economiche causate dall'emergenza sanitaria da Covid-19. La comunicazione di tali dati si è resa necessaria al fine di portare a rendicontazione, a valere sul Fondo strutturale europeo, le spese per

l'emergenza già anticipate dallo Stato e, conseguentemente, di ottenere dall'UE il relativo rimborso entro il 31 dicembre 2020 (come stabilito dall'art. 242, commi 1 e 2, d.l. 19 maggio 2020, n. 34; cfr. altresì il regolamento (UE) 1303/2013 del 17 dicembre 2013).

Il Garante, pur avendo ricevuto l'istanza in prossimità della scadenza del termine per la conclusione del processo di rendicontazione il cui decorso avrebbe precluso allo Stato di avvalersi dei fondi europei, (in tempi assai ristretti) si è comunque pronunciato favorevolmente sull'assunto che la comunicazione dei dati personali dall'Inps alle autorità di gestione risultasse necessaria per assicurare l'esecuzione del compito di interesse pubblico connesso alle citate esigenze di rendicontazione; al contempo, ha prescritto di valutare l'adozione di tecniche di pseudonimizzazione, anche al fine di assicurare il rispetto dei principi di minimizzazione dei dati e di *privacy by design* e *by default* (provv. 17 dicembre 2020, n. 275, doc. web n. 9519360).

Bonus sociali

Il Garante si è espresso sui trattamenti connessi al cd. *bonus* sociale, misura di sostegno a favore delle famiglie in stato di disagio economico e sociale consistente nell'applicazione di una tariffa agevolata che comporta una compensazione della spesa in relazione alle forniture di energia elettrica, gas naturale e acqua. In questo ambito, l'art. 57-*bis*, comma 5, d.l. 26 ottobre 2019, n. 124 – disposizione non preventivamente sottoposta al parere del Garante – ha stabilito che, a partire dal 1° gennaio 2021, le modalità di fruizione di tale prestazione sociale agevolata sarebbero passate dal previgente meccanismo del riconoscimento a domanda degli interessati a un nuovo meccanismo di riconoscimento automatico sulla base dell'Isee in corso di validità, rimettendo ad Arera la definizione degli aspetti attuativi della misura.

A questo proposito, Arera ha chiesto al Garante il previsto parere sullo schema di delibera concernente le modalità di trasmissione delle informazioni utili ai fini dell'erogazione dei *bonus* sociali da parte dell'Inps al Sistema informativo integrato (SII). Sistema che si incentra su una banca dati dei punti di prelievo e dei dati identificativi degli utenti creata per la gestione dei flussi informativi relativi ai mercati energetici e gestita da Acquirente Unico (e mai sottoposta al vaglio del Garante).

In ragione delle criticità rilevate nello schema di delibera, il Garante ha fissato alcune condizioni per conformare il trattamento alla disciplina in materia di protezione dei dati personali. In primo luogo, ha ritenuto necessaria l'individuazione di Arera quale titolare del trattamento, in coerenza con la disciplina in materia di Isee e di prestazioni sociali agevolate (d.P.C.M. 5 dicembre 2013, n. 159, e d.m. 16 dicembre 2014, n. 206), in quanto soggetto che, nell'individuare le modalità del trattamento, disciplina l'erogazione della prestazione sociale agevolata (ente erogatore) e si avvale del Gestore del SII (Acquirente Unico) quale responsabile del trattamento. Ha poi affermato la necessità di individuare con certezza le "utenze agevolabili" in caso di spettanza dei *bonus*, mediante l'utilizzo di dati esatti già in sede di acquisizione al momento della presentazione della Dsu da parte degli interessati, ma al contempo prevedendo, nelle more delle necessarie modifiche, la trasmissione dall'Inps al SII delle sole tipologie di dati personali strettamente indispensabili ai fini dell'erogazione dei *bonus*. È stata rimarcata la necessità di prevedere la messa a disposizione degli interessati di tutte le informazioni necessarie per consentire una piena comprensione circa il trattamento dei dati presenti nella Dsu a fini di erogazione dei *bonus* sociali. Infine, è stata richiesta la definizione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, con riferimento alla trasmissione dei dati personali dall'Inps al SII e ai successivi trattamenti effettuati presso il SII, sulla base di una valutazione di impatto sulla protezione dei dati dal titolare del trattamento (provv. 17 dicembre 2020, n. 279, doc. web n. 9510819).

4.2.3. Reddito di cittadinanza

Controlli

Il Garante è tornato a occuparsi del reddito di cittadinanza (Rdc) (al riguardo v. già provv. 20 giugno 2019, n. 138, doc. web n. 9122428, concernente il decreto del Ministro del lavoro e delle politiche sociali 2 settembre 2019, che istituiva il Sistema informativo del Rdc, ai sensi dell'art. 6, d.l. 28 gennaio 2019, n. 4). Con un primo parere, il Garante si è pronunciato sullo schema di convenzione da stipularsi tra il Ministero del lavoro e delle politiche sociali, di concerto con il Mef e la Guardia di finanza, che stabilisce le modalità operative per l'accesso, da parte di quest'ultima al Sistema Rdc al fine di consentire i controlli nei confronti dei beneficiari e il monitoraggio delle attività degli enti di formazione (in attuazione dell'art. 6, comma 6, d.l. n. 4/2019 e dell'art. 7, comma 3, d.m. 2 settembre 2019).

L'Autorità si è espressa in senso favorevole in quanto, fermo restando che le categorie di dati accessibili e di interessati a cui i dati si riferiscono sono stati stabiliti direttamente nel citato decreto, le misure individuate – anche a seguito degli approfondimenti effettuati e delle indicazioni formulate dall'Autorità – sono state ritenute adeguate. In particolare, tali misure hanno riguardato: la modalità di accesso al Sistema Rdc, basata sull'identità federata riservata agli utenti della Guardia di finanza, la periodicità delle attività di verifica e revisione della sussistenza delle condizioni per la conservazione dei profili di autorizzazione attribuiti agli utenti della Guardia di finanza, la previsione del divieto di utilizzo di dispositivi automatici (*robot*) che consentano di consultare in forma massiva i dati ivi contenuti, l'introduzione di adeguati limiti al numero di soggetti interrogabili dagli utenti della Guardia di finanza con operazioni di consultazione multipla, sia in relazione a una singola operazione, sia alle operazioni complessivamente effettuate in un giorno. Sono state inoltre individuate le modalità di tracciamento degli accessi e delle operazioni compiute sul Sistema Rdc dagli utenti della Guardia di finanza, i tempi di conservazione delle registrazioni degli accessi e delle operazioni nonché il loro utilizzo a fini di verifica della liceità del trattamento (provv. 19 maggio 2020, n. 89, doc. web n. 9429241).

Verifica dei requisiti

In un'altra occasione il Garante è stato interpellato dall'Inps con riferimento allo schema di provvedimento concernente l'acquisizione delle informazioni pertinenti, disponibili negli archivi delle amministrazioni titolari dei dati, ai fini del riconoscimento del Rdc e della correlata verifica del possesso dei requisiti d'accesso da parte dei richiedenti (in attuazione dell'art. 5, comma 3, d.l. n. 4/2019). In particolare, ai sensi degli artt. 2, comma 1, e 3, comma 13, d.l. n. 4/2019, si tratta dei dati concernenti: l'intestazione o la piena disponibilità di autoveicoli o motoveicoli (detenuti nel Pra, presso l'Aci); il patrimonio immobiliare (detenuti nell'Anagrafe tributaria presso l'Agenzia delle entrate) facente capo all'intero nucleo familiare; la sottoposizione a misure cautelari personali, l'irrogazione di condanne definitive per particolari reati o la sottoposizione ad uno stato di detenzione (detenuti presso il Ministero della giustizia); il ricovero in istituti di cura di lunga degenza o presso altre strutture residenziali a totale carico dello Stato o di altra amministrazione pubblica (detenuti presso regioni e province autonome).

Anche in considerazione dell'accoglimento delle indicazioni fornite dall'Ufficio, incentratesi sulla minimizzazione delle tipologie di dati oggetto di scambio informativo, la limitazione alle finalità previste dalla legge e i tempi di conservazione dei dati acquisiti dall'Inps, il Garante ha espresso il proprio avviso favorevole.

È stata altresì prevista l'adozione, da parte delle amministrazioni destinatarie dei dati personali forniti dall'Istituto, di adeguate misure per assicurarne l'integrità e la riservatezza rispetto a divulgazioni e accessi non autorizzati o illeciti, per cancellarli immediatamente una volta fornito il riscontro richiesto nonché, con riguardo ai flussi informativi, l'adozione di misure tecniche e organizzative in grado di assi-

curare l'integrità, la riservatezza e la non ripudiabilità dei dati (in particolare, la cifratura delle informazioni e la firma digitale). Con il medesimo provvedimento, il Garante ha autorizzato i trattamenti in questione ai sensi dell'art. 58, par. 3, lett. *c*), del RGPD e dell'art. 2-*quinquiesdecies* del Codice, in considerazione del fatto che gli stessi sono effettuati per l'esecuzione di un compito di interesse pubblico e presentano rischi elevati per i diritti e le libertà degli interessati, in quanto prevedono scambi di dati personali, su larga scala e con modalità telematiche, relativi alla salute, alla condizione sociale e alla situazione economica e finanziaria nonché a condanne penali e reati, riferiti principalmente a soggetti vulnerabili, anche minori d'età, che condizionano l'accesso a servizi e prestazioni sociali. Allo stesso tempo, il Garante ha rilevato, con riferimento all'intenzione (rappresentata dall'Inps) di acquisire, con le medesime modalità, anche le informazioni necessarie ai fini dello svolgimento delle successive verifiche sulla permanenza dei requisiti durante il periodo di fruizione del beneficio, che i profili concernenti tali ulteriori controlli dovranno essere esaminati all'esito della valutazione di impatto predisposta al riguardo (provv. 26 novembre 2020, n. 231, doc. web n. 9492971).

4.2.4. Isee

Anche l'Isee ha formato oggetto di rivisitazione; a questo proposito, il Ministero del lavoro e delle politiche sociali ha richiesto il parere del Garante sulla proposta del nuovo modello tipo di attestazione Isee con omissioni o difformità sui saldi e le giacenze del patrimonio mobiliare, come predisposta dall'Inps, "finalizzata ad esporre, con riferimento alle Dichiarazioni sostitutive uniche (Dsu) presentate a decorrere dal 1° gennaio 2020, gli esiti dei controlli sui saldi e le giacenze del patrimonio mobiliare sulla base dei criteri stabiliti dal citato comma 2 dell'articolo 4 del decreto ministeriale 9 agosto 2019" (sul quale v. il parere favorevole 20 giugno 2019, n. 136, doc. web n. 9124390).

Il Garante si è pronunciato positivamente, considerato che le informazioni indicate nel modello proposto risultano conformi a quelle stabilite nel citato decreto e che già quest'ultimo prevedeva alcune misure volte a proteggere i dati personali degli interessati da accessi abusivi e non autorizzati anche in relazione alla produzione, da parte dall'Inps, dell'attestazione Isee (provv. 9 aprile 2020, n. 68, doc. web n. 9343042).

4.2.5. Altri benefici economici

Rispetto all'erogazione di ulteriori provvidenze e contributi economici (con modalità telematica) in forza di provvedimenti adottati dal Governo, l'intervento dell'Autorità è stato preordinato al rafforzamento del quadro di garanzie in materia di protezione dei dati personali.

Dispositivi antiabbandono

È stato reso al Ministero delle infrastrutture e dei trasporti un parere sullo schema di decreto di attuazione dell'art. 52, d.l. 26 ottobre 2019, n. 124 (convertito con modificazioni dalla l. n. 157/2019), recante la disciplina del riconoscimento di un contributo per l'installazione di dispositivi di allarme per prevenire l'abbandono di bambini nei veicoli chiusi (provv. 15 gennaio 2020, n. 2, doc. web n. 9264222). In particolare, il Ministero ha inteso disciplinare le modalità di attribuzione del contributo *una tantum* per l'acquisto o per il rimborso (in base ad apposita dichiarazione rilasciata ai sensi del d.P.R. n. 445/2000) di parte del costo sostenuto relativo a dispositivi antiabbandono da uno dei genitori o da altro soggetto esercente la responsabilità genitoriale per un minore che non abbia compiuto il quarto anno di età al momento dell'acquisto. Le indicazioni fornite dall'Autorità hanno riguardato, in particolare, la necessità di individuare chiaramente la tipologia di dati trattati,

nel rispetto del principio di trasparenza (art. 5, par. 1, lett. *a*), del RGPD), sia con riferimento al richiedente e al minore (quali nome, cognome e codice fiscale), sia con riguardo ai dati necessari per effettuare il rimborso (coordinate bancarie del richiedente), nonché di chiarire la tipologia delle verifiche poste in essere da Sogei, responsabile del trattamento del Ministero, sulla validità dei codici fiscali del richiedente e del minore mediante un collegamento con l'Anagrafe tributaria.

Con specifico riferimento, invece, ai profili di sicurezza, è previsto che il Ministero stipuli apposite convenzioni con Sogei e Consap, entrambe responsabili del trattamento, nell'ambito delle quali dovranno essere individuate, oltre ad adeguati tempi di conservazione dei dati, le misure tecniche e organizzative volte a soddisfare un adeguato livello di sicurezza nel rispetto dell'art. 32 del RGPD.

È stato infine richiesto di precisare che l'attività di monitoraggio effettuata da Sogei sia volta esclusivamente a rendicontare gli oneri derivanti dall'emissione dei buoni elettronici, ai soli fini del rispetto dei limiti di spesa.

Bonus paratie

Analogamente, l'Autorità si è espressa in relazione allo schema di decreto del medesimo Ministero volto a definire le modalità di concessione di un contributo per l'acquisto di paratie divisorie, conformi a particolari caratteristiche tecniche, nei veicoli destinati ai servizi di autotrasporto pubblico non di linea, ai sensi dell'art. 93, d.l. 17 marzo 2020, n. 18, convertito dalla legge n. 27/2020 (provv. 9 luglio 2020, n. 136, doc. web n. 9441718). A tal fine, il richiedente, la cui l'identità è verificata attraverso Spid, deve registrarsi su una piattaforma informatica accessibile dal sito del Ministero e corredare l'istanza con una dichiarazione sostitutiva (redatta ai sensi del d.P.R. n. 445/2000), ivi attestando alcuni dati (tra gli altri, il numero di targa del veicolo su cui è installata la paratia; il titolo che legittima la disponibilità del veicolo; il codice Iban per l'accredito del rimborso e i dati dell'intestatario del conto; l'indirizzo *e-mail* per eventuali comunicazioni connesse all'erogazione del rimborso). L'Autorità ha invitato il Ministero, nel rispetto dei principi di liceità, correttezza e trasparenza, ad apportare alcune integrazioni allo schema volte a individuare chiaramente, in particolare, la tipologia di dati trattati; inoltre, alle convenzioni stipulate tra Ministero, titolare del trattamento, e altri soggetti coinvolti (quali Sogei e Consap, individuati quali responsabili del trattamento) è rimessa l'individuazione di adeguati tempi di conservazione dei dati nonché di misure tecniche e organizzative volte ad assicurare un adeguato livello di sicurezza, nel rispetto dell'articolo 32 del RGPD.

Voli con la Sicilia

L'Autorità è intervenuta anche sullo schema di decreto del Ministero delle infrastrutture e dei trasporti in attuazione dell'art. 1, commi 124, 125 e 126, l. n. 160/2019, che disciplina le modalità di erogazione di un contributo su ogni biglietto aereo da e per Palermo e Catania acquistato dai residenti nella Regione Sicilia che rientrano in alcune particolari categorie sociali (quali, studenti universitari fuori sede, disabili gravi, lavoratori dipendenti con sede al di fuori della Regione e con redditi annui non superiori a 20.000 euro nonché, infine, migranti per ragioni sanitarie). Le osservazioni dell'Autorità hanno riguardato, in particolare, l'utilizzo, per la richiesta del beneficio, di una piattaforma informatica, realizzata e gestita da Sogei, cui si accede previa registrazione su un sito web dedicato, in alternativa all'applicazione per dispositivi mobili (APP IO, gestita da PagoPA). È stata altresì evidenziata la necessità di definire il ruolo di Sogei e PagoPA, alle quali, in conformità all'art. 28 del RGPD, dovranno esser impartite adeguate istruzioni, nonché di precisare le amministrazioni presso le quali il Ministero, attraverso Sogei, provvederà a effettuare le verifiche sui requisiti dichiarati dai beneficiari, nel rispetto dell'art. 71, d.P.R. n. 445/2000 (provv. 12 novembre 2020, n. 217, doc. web n. 9519453).

Bonus cultura

Il Garante si è espresso anche sullo schema di decreto recante modifiche al decreto 24 dicembre 2019, n. 177, concernente i criteri e le modalità di attribuzione

e di utilizzo della Carta elettronica prevista dall'art. 1, comma 604, l. 30 dicembre 2018, n. 145 (cd. *bonus* cultura o 18*app*) (provv. 26 novembre 2020, n. 234, doc. web n. 9505279). Il decreto conferma i contenuti della misura del cd. *bonus* cultura previsto in favore dei diciottenni e, in continuità con i precedenti regolamenti, ne ha previsto l'estensione anche ai giovani che compiono diciotto anni nel 2020 oltre all'ampliamento delle categorie di beni acquistabili, ricomprendendovi gli abbonamenti a quotidiani, anche in formato digitale. Le osservazioni dell'Autorità hanno riguardato, in particolare, il cd. registro vendite, tenuto e compilato dagli esercenti, nel quale devono essere indicate, per ciascuna delle vendite effettuate, alcune informazioni (codice ed importo del buono validato; numero e data della fattura elettronica inviata tramite il Sistema di interscambio; categoria, descrizione, prezzo e codice del bene ceduto; tipologia, numero e data del documento fiscale emesso). In particolare, si è ritenuto necessario che la disciplina di tale registro fosse inserita direttamente nel decreto esplicitando la finalità del registro e del conseguente trattamento dei dati personali previsti, con particolare riguardo al rispetto del principio di minimizzazione dei dati.

Altri sono stati gli ambiti nei quali il Garante è stato chiamato ad esprimersi in relazione all'erogazione di provvidenze di natura economica che qui ci si limita ad enumerare: si pensi al cd. *bonus* rottamazione (sul quale v. parere 26 novembre 2020, n. 233, doc. web n. 9519436), al contributo a favore di imprese che svolgono attività in campo di guida escursionistica e tutela ambientale, in conseguenza dell'emergenza Covid-19 (cfr. parere 29 ottobre 2020, n. 211 doc. web n. 9487962) o, ancora, al cd. *bonus* mobilità, oggetto di uno schema di decreto interministeriale di natura regolamentare attuativo dell'art. 2, comma 1, d.l. 14 ottobre 2019, n. 111, convertito con modificazioni dalla legge 12 dicembre 2019, n. 141 e modificato dal d.l. 19 maggio 2020, n. 34 (cfr. parere 9 luglio 2020, n. 135, doc. web n. 9439976).

4.3. *L'istruzione scolastica*

Particolarmente intensa è stata l'interlocuzione con il Ministero dell'istruzione, le istituzioni scolastiche e con altri soggetti pubblici nel corso di incontri e contatti volti a fornire chiarimenti e indicazioni in merito alla corretta applicazione della disciplina in materia di protezione dei dati personali, anche e soprattutto alla luce delle diverse iniziative assunte per assicurare la prosecuzione delle attività didattiche e formative nel contesto dell'emergenza epidemiologica da Covid-19.

4.3.1. I trattamenti di dati personali nell'ambito della pandemia da Covid-19

A partire dalle prime settimane dell'emergenza sanitaria, numerosi sono stati i reclami, le segnalazioni e i quesiti riguardanti diversi profili relativi alla protezione dei dati personali sollevati dal crescente ricorso alle piattaforme per l'attività didattica a distanza resosi necessario a seguito dalla sospensione delle attività scolastiche e di formazione superiore prevista a partire dal d.P.C.M. 8 marzo 2020 (v. artt. 1, comma 1, lett. *h*) e 2, comma 1, lett. *m*) e *n*).

In tale ambito l'Autorità, tenuto conto dell'assoluta imprevedibilità delle circostanze che hanno imposto la completa riorganizzazione dell'attività didattica e delle conseguenti difficoltà in cui si sono trovati ad operare gli istituti scolastici (anche in ragione delle risorse disponibili), ha ritenuto opportuno fornire tempestivamente a scuole, università, studenti e famiglie prime indicazioni, al fine di favorire la necessaria consapevolezza riguardo ai rischi nonché alle garanzie e ai diritti che, anche nel contesto dell'emergenza, devono essere salvaguardati.

4

Intervenendo fin da subito con il provvedimento del 26 marzo 2020, n. 64 (doc. web n. 9300784, sul quale v. anche par. 13.2), è stato chiarito che scuole e università non devono richiedere a personale scolastico, studenti e genitori il consenso al trattamento dei dati personali necessari allo svolgimento dell'attività didattica a distanza in quanto tale trattamento è riconducibile alle funzioni istituzionalmente poste in essere. I titolari sono però tenuti, per assicurare la trasparenza e la correttezza del trattamento, a informare gli interessati (con un linguaggio comprensibile anche ai minori) circa le sue caratteristiche essenziali (artt. 5, lett. *a*) e 13 del RGPD).

È stato evidenziato che scuole e università, nell'individuare gli strumenti più utili per la realizzazione della didattica a distanza, devono orientarsi verso piattaforme che siano in grado di soddisfare le effettive esigenze didattiche e formative e che offrano, al contempo, maggiori garanzie sul piano della protezione dei dati personali, prestando particolare attenzione a quelle che includono una pluralità di servizi, non sempre specificatamente rivolti alla didattica. Il trattamento di dati effettuato per conto della scuola o dell'università deve essere limitato a quanto strettamente necessario alla fornitura dei servizi richiesti ai fini della didattica *online* e non deve essere effettuato per finalità ulteriori, proprie del fornitore; in tale quadro, i gestori delle piattaforme non possono condizionare la fruizione dei richiamati servizi alla sottoscrizione, da parte di studenti o famiglie, di un contratto o alla manifestazione del consenso al trattamento dei dati per la fornitura di servizi *online* ulteriori, non collegati all'attività didattica (art. 5, lett. *b*), del RGPD).

Infine, il rapporto con il fornitore che effettua il trattamento di dati personali dei richiamati soggetti per conto di scuole e università deve essere regolato con contratto, o altro atto giuridico, ai sensi dell'art. 28 del RGPD.

Nel caso in cui si ritenga necessario ricorrere a piattaforme che erogano servizi più complessi (anche non rivolti in via esclusiva alla didattica), si dovranno attivare i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare.

Considerato il numero delle problematiche sottoposte all'attenzione dell'Autorità con riferimento al trattamento dei dati personali nel contesto emergenziale in ambito scolastico, l'Ufficio ha altresì provveduto, fin dalle prime settimane di emergenza, a fornire chiarimenti e precisazioni in merito a talune delle questioni più ricorrenti sollevate in ambito scolastico (cfr. FAQ - Trattamento dati nel contesto scolastico nell'ambito dell'emergenza sanitaria, doc. web n. 9337010).

È stato così chiarito che le scuole possono trattare i dati personali di insegnanti, alunni e famiglie, anche relativi a categorie particolari, nell'ambito delle proprie finalità istituzionali e non devono chiedere agli interessati di prestare il consenso al trattamento dei propri dati, neanche in relazione alla didattica a distanza (FAQ n. 1); si è ribadito che i titolari sono tenuti ad assicurare la trasparenza del trattamento informando, con un linguaggio facilmente comprensibile, gli interessati in merito, in particolare, ai tipi di dati e alle modalità di trattamento degli stessi, ai tempi di conservazione e alle altre operazioni effettuate, specificando che le finalità perseguite sono limitate esclusivamente all'erogazione della didattica a distanza (FAQ n. 2).

È stato precisato che non spetta agli istituti scolastici ma alle autorità sanitarie competenti informare i contatti stretti del contagiato al fine di attivare le previste misure di profilassi; l'istituto scolastico è tenuto a fornire alle istituzioni competenti le informazioni necessarie a ricostruire la filiera dei contatti del contagiato e, sotto altro profilo, ad attivare le necessarie misure di sanificazione (FAQ n. 4).

Con specifico riferimento alle campagne di *screening* sulla positività al Covid-19 che le strutture sanitarie possono promuovere in contesti a rischio di contagio, come quello scolastico, è stato evidenziato che la partecipazione degli alunni ai test può

avvenire solo su base volontaria e che il ruolo della scuola deve limitarsi a quello di promozione, supporto ed intermediazione tra struttura sanitaria e famiglie, evitando (di regola) di acquisire dati personali, essendo la struttura sanitaria l'unica legittimata a raccogliere le adesioni e a comunicare i risultati alla famiglia (FAQ n. 5).

Nel periodo emergenziale, l'Ufficio ha rafforzato la consueta collaborazione istituzionale con il Ministero dell'istruzione. In particolare, a seguito della disponibilità manifestata nella comunicazione inviata dal presidente Soro al Ministro dell'istruzione in vista del possibile utilizzo del registro elettronico anche come piattaforma per le attività di didattica a distanza (nota 4 maggio 2020, doc. web n. 9334326), è stato istituito un gruppo di lavoro congiunto in relazione ai trattamenti di dati personali di alunni e docenti effettuati mediante il registro elettronico e altri principali strumenti di svolgimento della didattica a distanza e didattica digitale integrata (DAD e DDI). Nell'ambito del gruppo di lavoro, il Ministero, in collaborazione con il Garante, ha adottato un documento di portata generale concernente la "Didattica digitale integrata e tutela della *privacy*: indicazioni generali" (consultabile all'indirizzo www.istruzione.it/rientriamoascuola/domandeerisposte.html) volto a fornire alle scuole linee di indirizzo e principi generali per l'implementazione della didattica digitale integrata, con particolare riguardo agli aspetti inerenti alla tutela dei dati personali. Il documento, riprendendo le prime indicazioni formulate dal Garante, ha fornito un quadro approfondito delle diverse questioni affrontate con il richiamato provvedimento del 26 marzo 2020, chiarendo la base giuridica del trattamento effettuato attraverso le menzionate piattaforme, la necessità di garantire un trattamento corretto e trasparente, improntato al rispetto dei principi applicabili al trattamento dei dati, il ruolo dei fornitori delle piattaforme di *e-learning* e le misure tecniche e organizzative che gli istituti scolastici sono tenuti a porre in essere.

Le linee guida hanno anche evidenziato l'importanza della figura del Rpd quale soggetto incaricato dal dirigente scolastico di fornire consulenza rispetto alle principali decisioni da assumere, ad esempio, in merito alla definizione del rapporto con il fornitore della piattaforma prescelta e alle istruzioni da impartire allo stesso, all'adeguatezza delle misure di sicurezza rispetto ai rischi connessi a tale tipologia di trattamenti e alle misure necessarie affinché i dati siano utilizzati solo in relazione alla finalità della DDI, nonché alle modalità per assicurare la trasparenza del trattamento mediante l'informativa da fornire a tutte le categorie di interessati.

Il documento ha toccato anche la tematica della valutazione d'impatto, chiarendo che questa deve essere effettuata solo nelle ipotesi in cui ricorrano i presupposti di cui all'art. 35 del RGPD ed evidenziando che le scuole, in linea generale, non effettuano trattamenti su larga scala e non sono tenute ad effettuare la valutazione d'impatto in relazione a trattamenti effettuati ove utilizzino semplici sistemi di videoconferenza o piattaforme che non comportano il monitoraggio sistematico degli utenti oppure se non sia fatto ricorso a soluzioni tecnologiche nuove e particolarmente invasive. La valutazione di impatto deve essere invece effettuata nel caso di impiego di piattaforme per la didattica che offrono funzioni più avanzate e complesse e che comportano un rischio elevato per i diritti e le libertà delle persone fisiche.

Nell'ambito delle attività del menzionato tavolo congiunto, l'Ufficio ha altresì collaborato all'elaborazione delle FAQ della sezione denominata "Protezione dei dati personali" consultabile sul sito web del Ministero dell'istruzione. Con esse il Ministero, d'intesa con il Garante, ha fornito risposta a talune delle questioni che, con maggiore insistenza, sono state sollevate nel corso dell'anno. È stato chiarito che le scuole non possono chiedere ad alunni e genitori di sottoscrivere autodichiarazioni sullo stato di salute o in merito all'eventuale esposizione al contagio da Covid-19 quale condizione per l'accesso a scuola in quanto attraverso le dichiarazioni sostitu-

tive non è possibile autocertificare il proprio o l'altrui stato di salute e non devono, neanche nell'ambito dei cd. patti di corresponsabilità o attraverso altra modulistica, imporre ad alunni e genitori di dichiarare periodicamente l'assenza di impedimenti riconducibili al Covid-19 come condizione per accedere ai locali scolastici.

Quesiti e segnalazioni si sono incentrati sulla possibilità di consentire la ripresa e la registrazione audio-video delle lezioni svolte nell'ambito della DDI. Al riguardo, le FAQ hanno precisato che il docente, per il tramite delle piattaforme utilizzate per la didattica digitale, può mettere a disposizione degli studenti materiali didattici (anche proprie video lezioni) per la consultazione e i necessari approfondimenti da parte degli alunni e che, invece, non è ammessa la videoregistrazione della lezione a distanza nel corso della quale si manifestano le dinamiche di classe. Ciò in quanto l'utilizzo delle piattaforme deve essere funzionale a ricreare lo spazio virtuale in cui si esplica la relazione e l'interazione tra il docente e gli studenti, non diversamente da quanto accade nelle lezioni in presenza.

Con le FAQ è stato infine specificato che, quando la creazione di un *account* personale è necessaria per l'utilizzo di piattaforme per la DDI, il trattamento dei dati personali, riconducibile alle funzioni istituzionalmente assegnate alle scuole, è ammesso a condizione che vengano attivati i soli servizi strettamente necessari allo svolgimento dell'attività didattica: in tali casi non deve essere richiesto il consenso dell'utente (studente, genitore o docente) o la sottoscrizione di un contratto.

Nel periodo emergenziale l'Autorità ha ricevuto numerosi quesiti relativi alla possibilità per gli istituti scolastici di pubblicare sul sito web istituzionale i dati relativi alla composizione delle classi in occasione dell'avvio del nuovo anno scolastico. Con la FAQ n. 6 è stato chiarito che, in assenza di una specifica disposizione normativa, le scuole che intendano garantire in via preventiva la conoscibilità di tali informazioni devono utilizzare modalità idonee ad assicurare la tutela dei dati personali e dei diritti degli interessati, ad es. tramite apposita comunicazione all'indirizzo *e-mail* fornito dalla famiglia in fase di iscrizione per le classi prime delle scuole di ogni ordine e grado o utilizzando, nelle restanti ipotesi, l'area documentale riservata del registro elettronico a cui accedono tutti gli studenti della classe di riferimento.

L'utilizzo crescente da parte degli istituti scolastici di strumenti digitali ha reso necessario un intervento del Garante anche in merito alla consultabilità, da parte delle famiglie e degli studenti, degli esiti scolastici. In tale ambito l'Autorità ha chiarito che, a differenza delle tradizionali forme di pubblicità degli scrutini, la pubblicazione dei voti *online* costituisce una forma di diffusione di dati particolarmente invasiva e non conforme all'attuale quadro normativo in materia di protezione dei dati. Una volta pubblicati, infatti, i voti rischiano di rimanere in rete per un tempo indefinito e possono essere utilizzati, anche incrociandoli con altre informazioni presenti sul web, da soggetti estranei alla comunità scolastica, determinando un'ingiustificata violazione del diritto alla riservatezza degli studenti. Il Garante ha rappresentato che la necessaria pubblicità degli esiti scolastici può essere realizzata utilizzando il registro elettronico o altre piattaforme che evitino i rischi sopra evidenziati (cfr. l'intervento del presidente Soro "Scuola: *Privacy*, pubblicazione voti *online* è invasiva. Ammissione non sull'albo ma in piattaforme che evitino rischi", Ansa, 11 giugno 2020, doc. web n. 9367295). Sul punto sono state avviate interlocuzioni con il Ministero dell'istruzione a seguito delle quali è stato istituito un tavolo di lavoro congiunto avente ad oggetto le "valutazioni intermedie e finali, valutazione di ammissione agli esami di stato e risultati finali e composizione delle classi", al fine di elaborare specifiche indicazioni per le istituzioni scolastiche e individuare misure tecniche e organizzative adeguate ai rischi per assicurare la conoscibilità di dati personali degli studenti mediante accesso ad aree riservate dei siti istituzionali delle scuole o tramite il registro elettronico.

Diffusione *online* di dati personali nel contesto scolastico

Sono stati definiti numerosi reclami e segnalazioni aventi ad oggetto la diffusione sui siti web istituzionali di istituti scolastici di dati personali riguardanti alunni e personale dipendente in assenza di una base giuridica idonea a giustificare tale diffusione.

Il Garante ha così censurato il comportamento di due scuole che avevano pubblicato sul proprio sito web istituzionale graduatorie d'istituto relative al personale docente contenenti, oltre ad informazioni relative all'indirizzo di residenza, al numero di telefono (fisso o mobile), all'indirizzo *e-mail*, anche l'indicazione dei titoli di preferenza del personale scolastico e, tra questi, informazioni relative alle condizioni di salute: in proposito, è stato rilevato che l'associazione della lettera "S" (che individua la categoria degli "invalidi e mutilati civili", secondo quanto riportato nell'all. 6 al decreto del Ministero dell'istruzione università e ricerca 1° aprile 2014, n. 235) a taluni nominativi comporta profili di illiceità nel trattamento, con violazione, quanto alla pubblicazione, degli artt. 6 e 9 RGPD e dell'art. 2-*ter* del Codice, nonché dei principi di liceità e minimizzazione del trattamento (art. 5 del RGPD); in relazione a tali elementi, ai sensi dell'art. 83 del RGPD, è stata comminata ad alcuni istituti scolastici una sanzione amministrativa (provv.ti 30 gennaio 2020, n. 21, doc. web n. 9283014 e 6 febbraio 2020 n. 27, doc. web n. 9283029).

La diffusione di dati personali è stata oggetto di una verifica anche in relazione a un reclamo avente ad oggetto la pubblicazione sul sito web di un istituto scolastico di dati personali di alcuni alunni, anche relativi allo stato di salute; in particolare, è stata accertata la pubblicazione di una graduatoria degli studenti contenente una serie di informazioni relative alle votazioni riportate, all'indice Isee e allo stato di disabilità riferite ai minori. A seguito dell'intervento del Garante la graduatoria è stata prontamente rimossa e l'istituto è stato sanzionato per violazione degli artt. 5, 6, 9 del RGPD e dell'art. 2-*ter* del Codice (provv. 9 luglio 2020, n. 140, doc. web n. 9451734).

In un altro caso, l'Autorità ha ricevuto un reclamo con cui veniva segnalata l'affissione, sulla porta di ingresso di una scuola dell'infanzia, di taluni elenchi contenenti, oltre ai nominativi dei minori, anche indicazioni relative alla data di nascita, all'indirizzo e ai recapiti telefonici agli stessi riferibili, nonché informazioni relative al loro stato vaccinale; gli approfondimenti effettuati hanno permesso di accertare che gli elenchi erano stati affissi per mero errore materiale. Anche in questo caso il Garante ha sanzionato l'istituto scolastico per aver pubblicato gli elenchi dei minori in assenza di un idoneo presupposto normativo e in violazione dei principi applicabili al trattamento dei dati (artt. 5 e 6 del RGPD e 2-*ter* del Codice) (provv. 2 luglio 2020, n. 117, doc. web n. 9445324).

L'Autorità è intervenuta nei confronti di un liceo ammonendolo per aver effettuato un'illecita comunicazione di dati relativi alla salute di un alunno, con riferimento alla pubblicazione, da parte di un docente, di una nota sul registro elettronico di classe, accessibile da parte di tutte le famiglie, relativa alle visite mediche che, settimanalmente, lo interessavano. Il Garante ha in particolare evidenziato che tali informazioni avrebbero dovuto essere rese visibili esclusivamente alla famiglia dell'interessato ed eventualmente agli altri docenti della classe in servizio nel giorno successivo alla visita medica (per esigenze didattiche) (provv. 5 marzo 2020, n. 45, doc. web n. 9365147).

Provvedimenti di ammonimento sono stati adottati a seguito della pubblicazione sul sito web istituzionale di graduatorie relative al personale amministrativo, tecnico e ausiliario contenenti anche l'indicazione (eccedente) del codice fiscale degli interessati (provv. 12 marzo 2020, n. 50, doc. web n. 9365159); così pure è accaduto nei confronti di una scuola per la pubblicazione, sul sito web dell'istituto, di un

documento recante l'indicazione di nome, cognome, indirizzo di posta elettronica e numero di cellulare di una professoressa, nonostante la stessa avesse presentato un'istanza di cancellazione dei propri dati personali; a seguito dell'intervento del Garante i dati sono stati rimossi (provv. 29 luglio 2020, n. 149, doc. web n. 9463997).

4.4. *Trasparenza e pubblicità dell'azione amministrativa*

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

4.4.1. Partecipazione ai tavoli di lavoro per la revisione della disciplina vigente e pareri a soggetti istituzionali

Commissione trasparenza e anticorruzione

Particolare attenzione è stata dedicata al tema della trasparenza e della pubblicità dell'azione amministrativa, fra l'altro, attraverso la partecipazione ai lavori della Commissione per la ricognizione e la revisione del sistema normativo della trasparenza e della prevenzione della corruzione nominata dal Ministro per la pubblica amministrazione con decreto 28 novembre 2019, con il compito di: "i) fornire un quadro ricognitivo della normativa, della giurisprudenza, della dottrina e delle prassi applicative relativi alla legge 6 novembre 2012, n. 190, al decreto legislativo 14 marzo 2013, n. 33 e alle norme ad essi collegate; ii) esaminare gli esiti della consultazione pubblica *online* in via di predisposizione su questi temi; iii) predisporre gli schemi degli opportuni interventi di aggiornamento e di riordino, ovvero di modifica, del quadro normativo in materia di trasparenza e prevenzione della corruzione nella pubblica amministrazione. La Commissione ha tenuto 22 riunioni e ulteriori incontri hanno avuto luogo in sotto-commissione e in singoli gruppi di lavoro, concludendo i propri lavori nel corso dell'anno con proposte di modifiche ai testi legislativi vigenti in materia di trasparenza e anticorruzione, compresi gli obblighi di pubblicazione *online* e la disciplina dell'accesso civico e documentale (d.lgs. n. 33/2013 e l. n. 241/1990).

Art. 12, d.lgs. n. 33/2013

In sede consultiva, si segnala il parere fornito al Consiglio di Stato, a seguito di specifica richiesta, in ordine al problema della diffusione di dati personali *online* e all'individuazione dei casi e delle condizioni nei quali ciò può essere considerato conforme alla normativa in materia di protezione dei dati personali (parere 26 febbraio 2020, n. 38, doc. web n. 9303645). Ciò con specifico riferimento a un quesito formulato dall'Anac ai giudici di Palazzo Spada in ordine all'interpretazione dell'art. 12, d.lgs. n. 33/2013, con particolare riferimento alla tipologia degli atti da pubblicare obbligatoriamente *online* e alla legittima diffusione dei dati personali eventualmente in essi contenuti. Al riguardo, è stato evidenziato che la disposizione, come si ricava dal relativo titolo, riguarda esclusivamente gli obblighi di pubblicazione di atti normativi o amministrativi di carattere generale in esso elencati, come: direttive, circolari, programmi, istruzioni che dispongono sull'organizzazione, funzionamento, obiettivi e procedimenti, ovvero che determinano l'interpretazione di norme giuridiche quali codici di condotta, misure integrative di prevenzione della corruzione, documenti di programmazione strategico-gestionale, atti degli organismi indipendenti di valutazione. Si tratta di atti che, per le loro caratteristiche, non dovrebbero

contenere dati personali (atteso che, in linea di massima, non dovrebbero essere rivolti a soggetti determinati), salvo ipotesi residuali per le quali risultano comunque applicabili i principi di limitazione della finalità e di minimizzazione, secondo le indicazioni contenute nelle linee guida del Garante in materia di trasparenza (provv. 15 maggio 2014, n. 243, doc. web n. 3134436). È stato evidenziato che, in relazione a eventuali dati personali pubblicati *online*, sarebbe opportuno valutare anche l'assunzione di ulteriori cautele per assicurare il rispetto del principio di proporzionalità e di minimizzazione dei dati (art. 5, par. 1, lett. *c*), del RGPD), come l'adozione, tenuto conto delle tecnologie disponibili, di misure volte a impedire ai motori di ricerca generalisti di indicizzarli ed effettuare ricerche rispetto ad essi, trascorso un congruo arco temporale dall'adozione della deliberazione.

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

In materia di diffusione di dati personali *online* per finalità di trasparenza o di pubblicità dell'azione amministrativa, nel dare riscontro a reclami, segnalazioni e quesiti, il Garante è stato chiamato a pronunciarsi su numerose questioni, di cui si riportano solo i casi più rilevanti definiti con provvedimento collegiale. In particolare, permane – come già rilevato in passato (cfr. Relazione 2019, par. 4.5.1) – il problema della diffusione *online* da parte di soggetti pubblici di dati sulla salute o di dati personali in assenza di un idoneo presupposto normativo (norma di legge o, nei casi previsti dalla legge, di regolamento) oppure in violazione del principio di minimizzazione.

Il Garante ha in proposito censurato il comportamento di diversi soggetti pubblici comminando sanzioni amministrative modulate in base alla condotta tenuta ai sensi dell'art. 83, par. 2, del RGPD.

Diffusione di dati sulla salute

Si segnala così il provvedimento sanzionatorio adottato nei confronti di un'azienda sanitaria per illecita diffusione di dati sulla salute (in violazione dell'art. 2-*septies*, comma 8, del Codice, nonché dell'art. 9 del RGPD), avendo la stessa pubblicato sul proprio sito web istituzionale una delibera del commissario *ad acta* contenente (sia nell'oggetto che nel testo) dati personali delle persone fisiche aventi diritto al risarcimento dei danni subiti dall'azienda, con indicazione di dati identificativi, residenza, codice fiscale, importo da liquidare e codice Iban su cui accreditare le somme (provv. 1° ottobre 2020, n. 173, doc. web n. 9483375).

Analogamente, è stato censurato un comune che aveva pubblicato la graduatoria per la realizzazione di progetti a favore delle persone con disabilità, indicando nominativamente quanti avevano presentato la domanda, i rispettivi punteggi nonché, in relazione al reclamante, le (ritenute) ragioni di esclusione (provv. 17 dicembre 2020, n. 277, doc. web n. 9559923; cfr., in materia di diffusione illecita di dati sulla salute, anche provv.ti 15 gennaio 2020, n. 3, doc. web n. 9261227; 26 febbraio 2020, n. 42, doc. web n. 9361162; 10 giugno 2020, n. 101, doc. web n. 9438157).

Diffusione di dati in mancanza di idonea base normativa o in violazione del principio di minimizzazione

Numerosi gli interventi, anche comminando specifiche sanzioni, in relazione alla diffusione *online* da parte di soggetti pubblici (es. comuni e regioni) di dati personali in assenza di un'idonea base normativa ai sensi dell'art. 2-*ter*, commi 1 e 3, del Codice (cfr. anche art. 6, par. 1, lett. *c*) ed *e*); par. 2 e par. 3, lett. *b*), del RGPD) e/o in violazione del principio di minimizzazione di cui all'art. 5, par. 1, lett. *c*), del RGPD. Ciò con particolare riferimento alla pubblicazione:

- di verbali di commissione di concorsi pubblici, in forma integrale, comprensivi di dati personali (quali dati identificativi ed esiti delle prove intermedie) dei concorrenti ma non vincitori, non ammessi o ritirati dal concorso (provv. 3 settembre 2020, n. 154, doc. web n. 9468523);

- di graduatorie *online* contenenti i dati dei soggetti ammessi, anche con riserva, a sostenere le prove scritte, o di quelli che avevano partecipato alle prove scritte e orali con indicazione dei punti assegnati, delle domande fatte in sede di esame, della votazione, dell'esito delle prove scritte oppure dei soggetti che avevano estratto le tracce o presenziato alle operazioni di consegna degli elaborati (provv. 30 gennaio 2020, n. 20, doc. web n. 9302897);
- di atti o documenti sull'albo pretorio *online* per periodi superiori a quelli previsti dalla normativa di riferimento, come nel caso dei quindici giorni previsti dall'art. 124, comma 1, d.lgs. n. 267/2000 (provv.ti 17 dicembre 2020, nn. 272 e 274, rispettivamente doc. web n. 9557593 e 9557753);
- di delibera contenente i dati personali (nominativo e residenza) dei segnalanti nonché informazioni relative al debito maturato per un risarcimento del danno da parte di una regione nei loro confronti in esecuzione di una sentenza esecutiva, con specificazione del relativo ammontare (provv. 2 luglio 2020, n. 120, doc. web n. 9440075);
- dell'atto di citazione di un comune nei confronti di un interessato allegato alla delibera di affidamento dell'incarico per la difesa dell'ente a un avvocato (provv. 5 marzo 2020, n. 52, doc. web n. 9361186);
- di dati personali pubblicati sul sito web istituzionale o contenuti in allegati a deliberazioni *online* (provv.ti 10 giugno 2020, n. 100 e 101, rispettivamente doc. web n. 9437853 e 9438157);
- di atti o documenti eccedenti rispetto alla finalità del trattamento o in violazione del principio di minimizzazione (art. 5, par. 1, lett. *c*), del RGPD), con particolare riferimento all'avvenuta diffusione del codice Iban del conto corrente (provv.ti 17 dicembre 2020, n. 274, doc. web n. 9557753; 15 gennaio 2020, n. 3, doc. web n. 9261227, già citati).

4.4.3. L'accesso civico

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

Richiesta di rivalutazione

Come in passato, si registrano in primo luogo casi in cui il Garante ha evidenziato di non potersi esprimere nel merito della richiesta di accesso per la presenza di carenze istruttorie o di provvedimenti di diniego non sufficientemente motivati oppure basati su argomentazioni deboli (cfr. pareri 16 aprile 2020, n. 75, doc. web n. 9347818; 5 novembre 2020, n. 216, doc. web n. 9563423).

Dati relativi a casi di Covid-19

Tra le fattispecie più significative, si segnala l'intervento dell'Autorità con riferimento a una richiesta di accesso civico generalizzato avente a oggetto il rilascio dei dati concernenti la distribuzione dei casi di Covid-19 registrati in una regione suddivisi per comune, sesso, età, esito (guariti, deceduti, casi attivi), domicilio (proprio oppure presso casa di riposo/microcomunità/RSA), data delle diagnosi di infezione, numero ed esiti dei tamponi eseguiti per paziente, nonché concernenti numero, distribuzione per comune e data dei contatti telefonici della Centrale a ciò deputata con le persone prese in carico per infezione da Covid-19 (parere 3 settembre 2020, n. 155, doc. web n. 9461036). Al riguardo è stato affermato che i dati e le informazioni riferiti a persone fisiche, identificate o identificabili, che hanno contratto il virus da Covid-19 rientrano nella definizione di dati sulla salute per i quali va escluso l'accesso civico ai sensi dell'art. 5-*bis*, comma 3, d.lgs. n. 33/2013. La particolarità del caso sottoposto all'attenzione del Garante risiedeva, tuttavia, nella circostanza che i dati e le informazioni richieste relative alla diffusione del Covid-19 nel territorio regionale

sarebbero stati privi dell'indicazione del nome e del cognome dei soggetti contagiati; è stato tuttavia evidenziato che la circostanza per la quale il soggetto istante aveva fatto accesso civico a dati di dettaglio riguardanti i casi di Covid-19 nella regione riferiti anche a singoli pazienti non escludeva la possibile reidentificazione degli interessati, anche *a posteriori* – considerando fra l'altro il particolare regime di pubblicità dei dati ricevuti tramite l'accesso civico (art. 3, comma 1, d.lgs. n. 33/2013) –, attraverso il "raffronto" dei dati richiesti con altre informazioni eventualmente in possesso di terzi. Ciò anche considerando quanto rappresentato dalla stessa regione in sede di diniego dell'accesso civico, ossia che l'esiguità demografica che caratterizza molti comuni del territorio (per non parlare delle residenze sanitarie assistenziali) fa sì che dall'incrocio dei dati in oggetto con informazioni facilmente acquisibili *in loco* sia possibile, almeno in taluni casi, risalire all'identità dei soggetti coinvolti e, conseguentemente, al loro stato di salute. Per tale motivo, è stato ritenuto conforme alla normativa in materia di protezione dei dati personali la soluzione adottata dalla regione, che – tenuto conto del contesto e del rischio di reidentificazione delle persone fisiche cui si riferivano i dati richiesti – ha accordato un accesso civico parziale, volto a evitare l'ostensione di dati e informazioni che potevano rivelare, anche indirettamente, l'identità degli interessati e il rispettivo stato di salute. L'amministrazione però – allo scopo di soddisfare 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 provveduto in ogni caso a fornire i dati sull'emergenza sanitaria relativi a: a) tamponi effettuati ogni settimana, per ogni comune, divisi per sesso; b) casi positivi totali (nell'intero periodo), per ogni comune, divisi per sesso; c) casi positivi nell'intera regione, divisi per sesso; d) guariti nell'intera regione, divisi per sesso; e) decessi nell'intera regione, divisi per sesso.

Richiedenti asilo

Il Garante è intervenuto in relazione all'accesso civico alla documentazione relativa alla rendicontazione annuale di un progetto di protezione per soggetti richiedenti asilo e rifugiati appaltato da un comune a una società cooperativa (pareri 2 luglio 2020, n. 114, doc. web n. 9438264 e 9 luglio 2020, n. 134, doc. web n. 9441527). Al riguardo, in merito alla richiesta di accesso al registro delle erogazioni economiche e delle presenze riferite a soggetti richiedenti asilo, è stato osservato che si trattava di atti contenenti dati di natura particolarmente delicata – sia con riferimento alla sola identità dei richiedenti asilo (in alcuni casi anche minori) e dei rifugiati, sia in relazione ai benefici economici ricevuti o ai giorni di presenza nei centri di accoglienza –, la cui generale conoscenza tramite l'istituto dell'accesso civico poteva essere fonte di discriminazione o foriera di rischi specifici per i soggetti interessati, anche considerando la possibile ricostruzione della vita e delle abitudini dei soggetti ospitati nei centri di accoglienza, sottoposti peraltro a protezione internazionale e tutelati dalla Convenzione di Ginevra sullo statuto dei rifugiati del 1951. Si è concordato, pertanto, con la decisione dell'amministrazione di rifiutare l'accesso a qualsiasi dato e informazione riferiti, anche indirettamente, a tali soggetti. Ciò ricordando, con particolare riferimento ai soli benefici economici, che anche la normativa in materia di trasparenza prevede un espresso divieto di diffusione di dati dei soggetti beneficiari di aiuti economici laddove "da tali dati sia possibile ricavare informazioni relative […] alla situazione di disagio economico-sociale degli interessati" (art. 26, comma 4, d.lgs. n. 33/2013), con la conseguenza di ricadere, per queste specifiche informazioni, in un caso di esclusione assoluta dell'accesso civico vigendo un espresso divieto di divulgazione previsto dalla legge (cfr. art. 5-*bis*, comma 3, d.lgs. n. 33/2013). Per i summenzionati motivi, è stato ritenuto corretto escludere l'accesso civico anche al documento relativo al registro delle erogazioni che conteneva il nominativo dei

beneficiari (tutti soggetti, secondo quanto riportato dal Rpct, richiedenti asilo fra i 18 e i 35 anni), il numero di giorni di presenza nella struttura di accoglienza (diviso per mesi), l'importo giornaliero e totale del beneficio economico ricevuto (cd. *pocket money*), la data e la firma del soggetto interessato. Analogamente – anche considerando il particolare regime di pubblicità che caratterizza l'istituto (art. 3, comma 1, d.lgs. n. 33/2013) – è stato ritenuto corretto rifiutare l'accesso civico al registro delle presenze contenente il nominativo dei soggetti interessati (secondo quanto riportato dal Rpct, richiedenti asilo minorenni), con l'indicazione dei giorni di presenza mensile e dell'indirizzo della struttura adibita ad accoglienza, per evitare un rischio concreto per la protezione dei relativi dati personali ai sensi dell'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013. Non è stato accordato, come invece domandato in sede di riesame, neanche un accesso parziale, oscurando i nominativi dei soggetti interessati e la firma; ciò in quanto tale accorgimento non avrebbe eliminato la possibilità che i richiedenti asilo potessero essere reidentificati, anche indirettamente, tramite ulteriori dati di dettaglio e di contesto contenuti nella documentazione richiesta o mediante altre informazioni in possesso di terzi. Nulla osta, invece, allo scopo di soddisfare comunque le esigenze informative alla base dell'accesso civico, a fornire all'istante dati aggregati, non riferibili ai singoli soggetti richiedenti asilo e, in ogni caso, privi di qualsiasi informazione idonea a identificarli, anche solo indirettamente.

Verbali di un consiglio di quartiere

In relazione alla richiesta di accesso civico generalizzato alla copia integrale del manoscritto recante i verbali di un consiglio di quartiere di un comune, è stato affermato che l'amministrazione ha operato correttamente rilasciando alcuni verbali con le firme autografe oscurate e accordando l'accesso dei restanti atti alla versione dattiloscritta laddove esistente (parere 23 marzo 2020, n. 59, doc. web n. 9304448). È necessario evitare, secondo quanto affermato dal Garante, la comunicazione di dati personali eccedenti rispetto alla finalità dell'accesso generalizzato, quali la sottoscrizione autografa oppure, per analogia, anche altri elementi calligrafici e grafologici che possano essere riferiti univocamente a singoli e che potrebbero favorire eventuali furti di identità o la creazione di identità fittizie attraverso le quali esercitare attività fraudolente.

Dati relativi a sgravi fiscali

Stesso pregiudizio alla tutela dei dati personali è stato verificato nel caso della richiesta di accesso civico a dati identificativi di soggetti che hanno ricevuto sgravi dall'Agenzia delle entrate (provv. 23 novembre 2020, n. 230, doc. web n. 9563405). Ciò alla luce della delicatezza di tali informazioni personali – connesse ad eventi della vita privata che non sempre si desidera portare a conoscenza di terzi –, essendo riferite al pagamento di tributi per i quali vi era stata un'iscrizione a ruolo o l'emissione di una cartella esattoriale oppure un semplice avviso di pagamento e successivamente oggetto di "sospensione legale della riscossione e del successivo annullamento dei ruoli".

Autorizzazione per accesso in area pedonale

Si segnala ancora la richiesta di accesso civico alla documentazione relativa alla segnalazione fatta a un comune ai danni del richiedente, nonché all'autorizzazione per accedere con un motociclo all'interno di un'area pedonale. Al riguardo è stato affermato che il comune aveva correttamente respinto l'istanza, in quanto l'eventuale ostensione dei documenti menzionati, unita alla generale conoscenza e al particolare regime di pubblicità dei dati oggetto di accesso civico, poteva costituire un'interferenza sproporzionata nei diritti e libertà del controinteressato, arrecando a quest'ultimo un pregiudizio che dipende, in concreto, dalle ipotesi e dal contesto in cui i dati e le informazioni possono essere utilizzate da terzi. Inoltre, la valutazione se rifiutare o meno l'accesso doveva essere effettuata nel rispetto del principio di minimizzazione dei dati (parere 23 gennaio 2020, n. 5, doc. web n. 9266087).

Continuano a pervenire richieste di parere su dati di dipendenti o di soggetti che

hanno avuto contratti o rapporti con la p.a. oppure che hanno sostenuto selezioni pubbliche. Al riguardo, è stata più volte affermata la sussistenza di un pregiudizio concreto alla tutela della 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. Anche in questo caso, è stata evidenziata la necessità di rispettare il principio di minimizzazione dei dati (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 le ulteriori informazioni di contesto contenute nei documenti richiesti. In molti casi, l'amministrazione è stata comunque invitata a fornire dati aggregati (privi di informazioni che possano identificare i soggetti interessati anche indirettamente) al fine di dare soddisfazione all'interesse conoscitivo del soggetto istante, evitando di fornire ulteriori dati personali eccedenti e sproporzionati rispetto alla finalità dell'accesso generalizzato (es. data di nascita, codice fiscale, recapiti degli interessati, indirizzo di residenza o di posta elettronica). Resta in ogni caso ferma la possibilità che, come più volte rappresentato, in presenza di un interesse specifico del soggetto istante all'accesso, laddove i documenti non possono essere forniti con l'istituto dell'accesso civico generalizzato, si ricorra all'accesso alla documentazione richiesta ai sensi della diversa disciplina in materia di accesso agli atti amministrativi contenuta negli artt. 22 ss., l. n. 241/1990, previa però dimostrazione dell'esistenza di "un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso".

Registri del ruolo matricolare dei militari

In relazione alla richiesta di accesso civico generalizzato volta a ottenere i registri del Ruolo matricolare comunale dei militari riferiti ad un arco temporale di 35 anni (dal 1950 al 1985) e i dati personali ivi contenuti (parere 23 gennaio 2020, n. 6, doc. web n. 9277716), è stato evidenziato che l'istanza aveva a oggetto una mole di dati e informazioni personali riferibili a dati comuni e, in alcuni casi, anche a "categorie particolari di dati personali" (art. 9 del RGPD) appartenenti a circa 170.000 interessati. I registri in parola, infatti, riportavano nominativi, data e luogo di nascita, informazioni in ordine alla residenza, data di registrazione, unità militare di assegnazione, grado rivestito, data di congedo, nonché annotazioni spesso coinvolgenti profili attinenti alla salute (ad es. in ordine all'eventuale esonero permanente dal servizio militare obbligatorio), unitamente ad indicazioni circa la condizione di obiettore di coscienza e di eventuale successiva rinuncia al relativo *status*, di per sé sintomatiche di opinioni politiche e/o di convinzioni religiose o filosofiche. Per tale motivo, è stato ritenuto che il riconoscimento di un accesso civico generalizzato ai dati e informazioni personali dei militari sopradescritti, unito alla generale conoscenza e al particolare regime di pubblicità dei dati oggetto di accesso civico, avrebbe potuto causare un pregiudizio concreto alla tutela della protezione dei dati personali dei controinteressati, previsto dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013.

Ordine di servizio della Polizia locale

Sempre con riferimento all'accesso civico a dati di dipendenti pubblici, si segnala il caso dell'accesso a ordini di servizio di particolari categorie di dipendenti pubblici, quali gli appartenenti alla polizia municipale; nel caso di specie, era stata chiesta l'ostensione degli ordini di servizio e del registro delle variazioni degli stessi, riferito al personale della Polizia locale addetto all'Ufficio ricorsi all'Autorità giudiziaria di un comune di grandi dimensioni, per un arco temporale di 3 mesi (parere 15 ottobre 2020, n. 180, doc. web n. 9483596). Nel caso esaminato si è dovuto tenere conto della peculiare tipologia dei dati e delle informazioni personali, anche di dettaglio,

contenuti negli ordini di servizio – di tipo preventivo e consuntivo – oggetto di richiesta, quali, per ogni singolo lavoratore: turno di servizio previsto, lavoro svolto, attività da svolgere nel giorno seguente, prestazioni effettive alla luce delle eventuali variazioni intervenute, dati su eventuali assenze programmate o su assenze dal servizio comunicate a seguito di malattie o infortuni, posizione lavorativa del dipendente, turno di riposo, prestazione svolta in regime di straordinario e permessi fruiti anche ai sensi della legge n. 104/1992. È stato quindi ritenuto corretto il diniego opposto dall'amministrazione alla richiesta di accesso civico, motivato sulla base dell'esistenza di pregiudizio concreto alla tutela della protezione dei dati personali.

Dati di dipendenti, concorsi e *curricula*

Analogamente è stato ritenuto sussistere il citato pregiudizio di cui all'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013, in ragione del quale l'amministrazione ha correttamente rifiutato l'accesso civico generalizzato, in relazione a istanze aventi a oggetto, fra l'altro:

- l'elenco anagrafico nominativo delle assunzioni effettuate da una società in totale partecipazione pubblica, con relativa mansione/inquadramento, nonché le graduatorie delle selezioni pubbliche effettuate con l'indicazione nominativa dei partecipanti. Al riguardo è stato affermato che nulla osta all'ostensione, tramite l'istituto dell'accesso civico generalizzato, delle graduatorie finali con i nominativi dei vincitori aggiornate con l'eventuale scorrimento degli idonei non vincitori, ma va rifiutato l'accesso agli ulteriori dati e informazioni quali, fra gli altri, i nominativi di tutti i partecipanti a selezioni della società anche se non vincitori (parere 25 febbraio 2020, n. 39, doc. web n. 9309442);
- i dati di un procedimento disciplinare archiviato riferito a un professionista iscritto all'ordine (parere 5 marzo 2020, n. 44, doc. web n. 9309491);
- le retribuzioni, i cedolini, le buste paga riferiti a dipendenti e lavoratori (parere 2 luglio 2020, n. 114, doc. web n. 9438264);
- i punteggi attribuiti ai dirigenti e/o ai direttori di un comune, relativi all'indennità di risultato per l'anno 2018, nonché la copia delle singole schede di valutazione a essi riferiti relative ai "comportamenti organizzativi" (parere 29 luglio 2020, n. 147, doc. web n. 9445796);
- i dati e le informazioni personali del segretario generale e dei direttori generali di un ministero relativi al numero di buoni pasto a essi singolarmente attribuiti, con contemporanea ostensione delle timbrature giornaliere dagli stessi effettuate per l'ingresso e l'uscita dalla sede di lavoro (parere 17 agosto 2020, n. 152, doc. web n. 9477809);
- i dati e le informazioni personali di un docente, immesso in ruolo, contenuti nei documenti e titoli dallo stesso presentati per partecipare a una procedura concorsuale (parere 17 agosto 2020, n. 153, doc. web n. 9477865);
- i *curricula* presentati da tutti i soggetti che hanno avanzato la propria proposta di candidatura per la nomina alla carica di amministratore unico di una società *in house* di un comune che però non sono stati selezionati (parere 17 settembre 2020, n. 156, doc. web n. 9464939).

Interventi urbanistici, titoli e abusi edilizi

Si menzionano, infine, i numerosi pareri resi su istanze di accesso civico aventi a oggetto interventi urbanistici, titoli e abusi edilizi. In proposito, il Garante è nuovamente intervenuto rinviando ai propri precedenti (parere 16 aprile 2020, n. 75, doc. web n. 9347818) e confermando gli orientamenti già espressi (parere 17 dicembre 2020, n. 271, doc. web n. 9521857; v. anche precedenti Relazioni di attività).

Si segnala, in ogni caso, il parere reso in materia di accesso civico generalizzato agli elenchi mensili dei rapporti comunicati agli organi di Polizia riguardanti abusi edilizi (parere 16 marzo 2020, n. 57, doc. web n. 9304437). Al riguardo, è stato affermato che la normativa di settore già prevede specifici obblighi di pubblicità in

materia di opere abusive (art. 31, comma 7, d.P.R. n. 380/2001), per cui nulla osta all'ostensione dei dati quali il numero di protocollo del rapporto, la data, l'organo da cui proviene il rapporto, la località, il tipo di abuso, gli estremi dell'ordinanza di sospensione. Quanto invece agli altri dati personali, come il nominativo del proprietario committente e l'indirizzo, il Garante ha rappresentato che un'eventuale ostensione tramite accesso generalizzato potrebbe causare effetti sfavorevoli sui controinteressati, considerando che, in alcuni casi, potrebbe essere ancora pendente un giudizio penale o si potrebbero fornire informazioni risalenti nel tempo, riguardanti procedure già definite, realizzando in tal modo un pregiudizio concreto alla tutela della protezione dei dati personali.

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

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

Continuano a pervenire al Garante richieste di parere da parte di amministrazioni o di singoli in materia di accesso ai documenti amministrativi e accesso agli atti da parte di consiglieri comunali ai sensi dall'art. 43, comma 3, d.lgs. n. 267/2000. In particolare, numerose richieste di accesso da parte di consiglieri comunali hanno riguardato le liste degli aventi diritto a buoni spesa o altri contributi erogati per far fronte all'emergenza da Covid-19 o elenchi dei nominativi dei soggetti posti in quarantena o risultati positivi al Covid-19. È stato al riguardo ribadito che, a prescindere dalla natura del documento oggetto della richiesta di accesso, è l'amministrazione destinataria dell'istanza a dover entrare nel merito della valutazione della richiesta – eventualmente sindacabile dal giudice amministrativo – rispettando i principi di limitazione della finalità e di minimizzazione dei dati e, nei casi in cui la richiesta attiene a particolari categorie di dati (art. 9 del RGPD) o a dati relativi a condanne penali o a reati (art. 10 del RGPD), la loro indispensabilità, consentendo l'accesso alle sole informazioni che risultano in concreto necessarie per lo svolgimento del mandato. L'Autorità ha rammentato che resta ferma la necessità, da parte del consigliere richiedente, di rispettare l'obbligo del segreto "nei casi specificatamente determinati dalla legge" nonché i divieti di divulgazione dei dati personali (si pensi, ad es., all'art. 2-*septies*, comma 8, del Codice, che vieta la diffusione dei dati idonei a rivelare lo stato di salute). Ne consegue che sono i consiglieri medesimi a rispondere dell'eventuale utilizzo delle informazioni, anche sul piano della disciplina in materia di protezione dei dati personali (cfr. note 29 maggio 2020).

Accesso dei consiglieri comunali ai dati di soggetti positivi al Covid-19

Ad un comune che aveva formulato un quesito in merito alla possibilità di consentire ai consiglieri comunali di ottenere, ai sensi dell'art. 43, d.lgs. n. 267/2000, gli elenchi dei soggetti positivi al Covid-19 o in isolamento, è stato evidenziato che tali elenchi – la cui titolarità in capo all'azienda sanitaria è finalizzata all'adozione delle misure di profilassi, diagnosi ed assistenza sanitaria dei contagiati nonché per la gestione emergenziale del Ssn – sono comunicati o messi a disposizione dei sindaci e dei prefetti esclusivamente e nella misura in cui risultino "necessari all'espletamento delle funzioni ad essi attribuite nell'ambito dell'emergenza determinata dal diffondersi del Covid-19", tra le quali quella di "monitorare e […] garantire l'esecuzione delle misure disposte ai sensi dell'articolo 2 del decreto-legge 25 marzo 2020, n. 19" (art. 17-*bis*, d.l. 17 marzo 2020, n. 18), sotto il coordinamento della prefettura. Spetta poi ai sindaci e ai prefetti rendere disponibili tali informazioni – adottando misure appropriate a tutela dei diritti e delle libertà degli interessati e nel rispetto dei principi di cui all'articolo 5 del RGPD, tra cui si configura il principio

di minimizzazione – soltanto agli operatori, alle strutture comunali e alle Forze di polizia (inclusa la Polizia locale) direttamente coinvolte negli interventi, nel rigoroso rispetto delle funzioni e delle competenze loro assegnate per la gestione dell'emergenza. Considerata la stretta funzionalizzazione dei dati relativi ai soggetti positivi al Covid-19, trasmessi dalle Asl unicamente ai fini della gestione di attività legate all'emergenza – cui non sembrano potersi ascrivere le funzioni esercitate dai consiglieri –, è stata evidenziata la possibilità per il comune di fornire comunque un riscontro comunicando indici numerici relativi al periodo di interesse; ciò solo nell'ipotesi in cui il comune abbia ragione di ritenere che tali informazioni risultino necessarie per l'adozione di eventuali atti di indirizzo e di controllo politico-amministrativo di competenza dei consiglieri (nota 9 dicembre 2020).

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

Anche nel settore degli enti locali sono pervenute numerose segnalazioni, reclami, richieste di parere e quesiti relativi ai trattamenti di dati personali connessi alla gestione delle attività necessarie a fronteggiare l'emergenza epidemiologica da Covid-19. Oltre a fornire chiarimenti a enti e singoli, l'Autorità ha pubblicato alcune FAQ per chiarire dubbi e fornire indicazioni per un corretto trattamento dei dati personali da parte delle p.a.

Diffusione dei dati di soggetti positivi al Covid-19 o in isolamento domiciliare

In relazione a numerosi quesiti con i quali, in particolare nella prima fase della pandemia, è stata richiesto se fosse legittimo pubblicare, quale misura di contenimento della diffusione dell'epidemia o per contrastare *fake news*, i dati identificativi dei soggetti risultati positivi al Covid-19 o sottoposti alla misura dell'isolamento domiciliare, è stato ricordato che la disciplina vigente vieta la diffusione dei dati relativi alla salute. Tale divieto non è stato derogato dalla normativa d'urgenza sull'emergenza epidemiologica da Covid-19. Pertanto, non possono essere diffusi, attraverso siti web o altri canali, i nominativi delle persone risultate positive al test per la ricerca del Covid-19 o sottoposte alla misura dell'isolamento (nota 27 aprile 2020).

Cionondimeno, a seguito di reclami e segnalazioni, sono state aperte diverse istruttorie relative alla diffusione o alla circolazione di tali elenchi su diversi canali (Facebook, Whatsapp, ecc.).

Servizi di supporto alla popolazione

Nell'ambito delle prime iniziative adottate dai comuni al fine di attivare servizi di supporto alla popolazione, alcune richieste hanno riguardato la possibilità di accedere agli elenchi dei soggetti risultati positivi al Covid-19 o in isolamento, ai fini dell'organizzazione di tali attività. Al riguardo, è stato evidenziato che i servizi assistenziali comunali a favore della popolazione (es. consegna di beni di prima necessità o di farmaci) possono essere offerti su richiesta degli interessati, pubblicizzando, con i canali ritenuti più efficaci, le modalità di attivazione del servizio (ad es. numero verde), senza quindi che risulti necessario raccogliere gli elenchi dei soggetti posti in isolamento domiciliare tenuti dalle aziende sanitarie competenti. Non tutti i soggetti in isolamento domiciliare, infatti, potrebbero essere interessati a fruirne, potendo tali esigenze, ad esempio, essere assolte da familiari o da altre reti sociali individuate dall'interessato. Peraltro, la modalità di attivazione "a richiesta" dei servizi citati potrebbe consentirne la fruizione anche ad una platea più ampia di soggetti che, pur non essendo in isolamento domiciliare, hanno (o avvertono) una maggiore esposizione al contagio o non possono usufruire di reti familiari o sociali (anziani, invalidi, malati cronici, ecc.).

Isolamento domiciliare e verifiche

Con riferimento ai quesiti relativi alle verifiche della polizia locale sul rispetto della misura dell'isolamento domiciliare, nell'ambito delle FAQ è stato chiarito che l'attività di sorveglianza sanitaria dei soggetti posti in isolamento domiciliare integra

un intervento di sanità pubblica che deve essere realizzato da operatori sanitari in grado di valutare, in relazione alle condizioni di salute del soggetto, le misure sanitarie più opportune. Le disposizioni d'urgenza adottate all'inizio della situazione pandemica pongono infatti in capo all'"operatore di sanità pubblica" l'obbligo di "contattare, quotidianamente, per avere notizie sulle condizioni di salute, la persona in sorveglianza" (art. 3, comma 6, d.P.C.M. 8 marzo 2020; art. 2, comma 6, d.P.C.M. 4 marzo 2020). Le prefetture, al fine di controllare che la misura dell'isolamento domiciliare sia effettivamente rispettata, possono avvalersi delle Forze di polizia, deputate anche ad adottare i provvedimenti sanzionatori connessi al mancato rispetto delle predette misure. Le Forze di polizia locale, pertanto, possono venire a conoscenza dei dati identificativi dei soggetti posti in isolamento nello svolgimento delle attività di controllo effettuate sotto il coordinamento della prefettura competente.

Controlli su strada

Nelle FAQ rivolte al trattamento dei dati da parte degli enti locali è stato ribadito che la verifica sull'attuazione delle misure emergenziali nazionali disposte per fronteggiare lo stato emergenziale da Covid-19 è assicurata dalle prefetture avvalendosi delle Forze di polizia, tra le quali la Polizia locale. In particolare, il personale di Polizia locale preposto ai controlli su strada deve assicurare il rispetto delle restrizioni dei movimenti delle persone sul territorio effettuando il controllo delle autodichiarazioni rese (ai sensi degli artt. 46 e 47, d.P.R. n. 445/2000 sul modello ministeriale) nonché provvedendo all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative o, nei casi più gravi, alla trasmissione delle notizie di reato alle autorità competenti. Gli accertamenti sulla veridicità delle dichiarazioni, in ragione della gravità delle conseguenze che possono derivare agli interessati, devono poter essere effettuati dalle Forze di polizia sui dati aggiornati tenuti dalle aziende sanitarie competenti e con modalità che garantiscano l'esattezza dei dati e il loro aggiornamento. A tal fine è stato quindi raccomandato di preferire soluzioni che permettano l'interrogazione puntuale e in tempo reale degli elenchi concernenti l'eventuale adozione della misura dell'isolamento domiciliare nei confronti del soggetto controllato. Nulla osta alla possibilità di effettuare tale interrogazione presso ciascuna delle strutture sanitarie dislocate sul territorio ovvero, in modo coordinato, presso un ufficio a ciò deputato della prefettura.

In tema di controlli sul rispetto delle misure di limitazione della circolazione previste dalle ordinanze, sono stati forniti chiarimenti anche ai singoli, ribadendo che il trattamento di dati da parte del Corpo di polizia nell'ambito dei controlli su strada è necessario per lo svolgimento di un compito di interesse pubblico (art. 6 del RGPD) e, pertanto, non poteva essere accolta da parte degli enti preposti la richiesta di cancellazione dei dati personali (note 14 luglio 2020).

Autodichiarazioni

Nel definire una segnalazione nella quale si lamentava l'assenza di informativa sui moduli di autodichiarazione previsti dalle circolari del Ministero dell'interno (nella fattispecie, Dipartimento della Pubblica sicurezza, 555doc/C/DIPP/FUN/CTR/1425/20 del 18 marzo 2020), è stato chiarito che l'art. 14, d.l. 9 marzo 2020, n. 18, recante disposizioni urgenti per il potenziamento del Ssn in relazione all'emergenza Covid-19, ha previsto che "Nel contesto emergenziale in atto, ai sensi dell'articolo 23, paragrafo 1, lettera *e*), del menzionato regolamento (UE) 2016/679, fermo restando quanto disposto dall'articolo 82 del decreto legislativo 30 giugno 2003, n. 196, i soggetti di cui al comma 1 possono omettere l'informativa di cui all'articolo 13 del medesimo regolamento o fornire una informativa semplificata, previa comunicazione orale agli interessati della limitazione" (nota 1° aprile 2020).

Gestione dei rifiuti

Sul tema della gestione dei rifiuti, considerate le raccomandazioni fornite dall'Istituto superiore della sanità (rapporto n. 3/2020, Rev. 2 del 31 maggio 2020) volte ad assicurare che nelle abitazioni in cui sono presenti soggetti positivi o in quaran-

tena sia interrotta la raccolta differenziata e che, ove possibile, siano utilizzati sacchi e/o contenitori di colore differente da quelli già utilizzati per rifiuti di altro tipo, anche istituendo un servizio dedicato di ritiro da parte di operatori qualificati (es. Protezione civile, Esercito, Croce rossa, ecc.), l'Autorità ha chiarito che i comuni, nonché le aziende affidatarie del servizio di raccolta, possono venire a conoscenza dei dati personali dei soggetti positivi o in isolamento, che dovranno essere aggiornati ed esatti (cfr. FAQ). I comuni devono, in ogni caso, effettuare le proprie scelte organizzative tenendo nella dovuta considerazione l'esigenza di rispettare la riservatezza degli interessati, in un'ottica di proporzionalità e minimizzazione del potenziale impatto sugli stessi. Pertanto, tenuto conto delle dimensioni territoriali, delle risorse disponibili, del numero dei contagi nonché delle modalità ordinarie di raccolta dei rifiuti, la scelta dovrà adeguatamente bilanciare le esigenze sanitarie con il diritto alla riservatezza. Dovranno essere pertanto individuate adeguate soluzioni organizzative tese a evitare l'esposizione a terzi della situazione degli interessati (ad es. preavviso telefonico prima del passaggio degli addetti alla raccolta; previsione di finestre temporali, anche notturne, per il ritiro, riducendo così il tempo di permanenza del contenitore o del sacco in prossimità dell'abitazione; ove possibile, individuazione di punti di raccolta isolati).

Sul tema della raccolta domiciliare dei rifiuti sono stati forniti diversi chiarimenti anche per rammentare i rischi connessi alla circolazione degli elenchi oltre che all'interno degli enti locali, anche tra i soggetti privati che erogano i servizi comunali (gestori dei pubblici servizi), nonché i rischi relativi alla violazione del principio di "esattezza" di cui all'art. 5, par. 1, lett. *d*), del RGPD.

Buoni spesa e altri contributi

Con riferimento al trattamento dei dati personali effettuati ai fini dell'attribuzione di buoni spesa o buoni alimentari, previsti dall'ordinanza del Capo della protezione civile 29 marzo 2020, n. 658, o di altri benefici economici a favore di soggetti che versano in condizioni di difficoltà economiche a causa della pandemia, sono stati forniti numerosi chiarimenti anche con le FAQ pubblicate sul sito.

In relazione ai moduli predisposti dai comuni con cui autocertificare il possesso dei requisiti previsti per ottenere le misure di sostegno, è stato chiarito che gli stessi devono prevedere la raccolta dei soli dati indispensabili alla verifica dei presupposti (es. reddito, fruizione di altri aiuti, composizione nucleo familiare, ecc.) e non anche informazioni non necessarie o non pertinenti per ottenere il beneficio richiesto. Con specifico riferimento ai cd. buoni spesa, alcuni bandi rivolti agli esercizi commerciali hanno previsto il rimborso del valore nominale degli stessi a fronte della presentazione, da parte degli esercenti, di adeguata documentazione giustificativa (es. buoni spesa in originale e/o gli scontrini fiscali per cui il rimborso è richiesto). In tale ipotesi, piuttosto che presentare direttamente gli scontrini con i dettagli di spesa, è stato raccomandato che l'esercizio commerciale presenti all'ente locale che ha erogato i buoni un'autodichiarazione sulla conformità dell'utilizzo di quelli di cui chiede il rimborso, conservando gli scontrini per gli eventuali controlli che il comune riterrà di effettuare. In tal modo si evita la produzione sistematica di documentazione di dettaglio che, associata all'identità del beneficiario del buono, comporterebbe la comunicazione di dati personali, anche di natura particolare.

Pubblicazione degli elenchi di beneficiari di buoni spesa

In risposta a numerosi quesiti, è stato altresì chiarito che la normativa sulla trasparenza stabilisce l'obbligo di pubblicazione, fra l'altro, dei nominativi dei soggetti destinatari in generale di benefici economici superiori a mille euro nel corso dell'anno solare (quali sovvenzioni, contributi, sussidi o altri vantaggi economici), fermo restando il divieto di diffusione nel caso in cui da tali dati "sia possibile ricavare informazioni relative allo stato di salute [o] alla situazione di disagio economico-sociale degli interessati" (art. 26, comma 4, d.lgs. n. 33/2013). Si tratta di un divieto

funzionale alla tutela della dignità, dei diritti e delle libertà fondamentali degli interessati, al fine di evitare che soggetti in condizioni disagiate (economiche o sociali) soffrano le ulteriori conseguenze pregiudizievoli derivanti della diffusione di tali informazioni. Nel caso di benefici economici superiori a mille euro nell'anno solare, spetta al comune valutare quando le informazioni di contesto rivelino dati sulla salute ovvero l'esistenza di un disagio economico o sociale degli interessati e non procedere, di conseguenza, alla pubblicazione di dati o altre informazioni idonee ad identificare gli interessati. In ogni caso, nel rispetto del principio di minimizzazione dei dati rispetto alla finalità perseguita, non risulta comunque giustificato pubblicare dati quali l'indirizzo di abitazione o la residenza, il codice fiscale, le coordinate bancarie per l'accredito dei contributi o dei benefici economici, la ripartizione degli assegnatari secondo le fasce dell'equivalente-Isee, l'indicazione di analitiche situazioni reddituali, di condizioni di bisogno o di peculiari situazioni abitative (nota 27 aprile 2020).

Sono stati altresì forniti chiarimenti alle amministrazioni locali in merito alla circolazione delle liste di beneficiari di buoni spesa su *social network* ribadendo la necessità che tali elenchi siano utilizzati solo da soggetti autorizzati, evitando illegittime comunicazioni delle liste tramite piattaforme quali Facebook e Whatsapp.

4.5.3. Mobilità e trasporti

Utilizzo di apparecchiature per il rilevamento delle violazioni del codice della strada

L'Autorità è stata interpellata in merito alla possibilità di utilizzo, ai fini della rilevazione di ulteriori violazioni non esplicitamente contemplate nei relativi decreti di approvazione (e tra queste il rilevamento della mancata copertura assicurativa e la eventuale conformità), di sistemi che effettuano il monitoraggio continuo del traffico, riferito anche ai veicoli non in violazione dei limiti di velocità. Premesso che l'utilizzo dei dispositivi automatici per le violazioni al codice della strada è condizionato all'esito positivo della procedura di omologazione (ovvero approvazione) da parte del competente Ministero delle infrastrutture e dei trasporti, l'Autorità ha chiarito che, allo stato, nessun dispositivo di rilevamento automatico delle infrazioni, di qualunque tipologia (controllo accessi, controllo velocità, semaforo rosso) può essere impiegato per un'analisi massiva dei transiti dei veicoli al fine di verificarne lo stato in relazione ai requisiti per la circolazione. Tali sistemi possono essere utilizzati solo per la rilevazione delle targhe dei veicoli di cui sia stata accertata l'infrazione ma non anche di quelle dei veicoli solo potenzialmente in infrazione; ad oggi, nessun dispositivo è stato infatti approvato/omologato specificatamente per il rilevamento automatico delle violazioni previste dall'art. 80 (mancata revisione), dall'art. 193 (mancata copertura assicurativa) e, in generale, dagli articoli del codice della strada inerenti i cd. requisiti per la circolazione (nota 15 giugno 2020).

Notifica a mezzo Pec delle contravvenzioni al codice della strada

L'Autorità ha ricevuto diversi reclami aventi ad oggetto la notifica di una sanzione per violazione del codice della strada effettuata utilizzando l'indirizzo Pec aziendale, accessibile, in quanto tale, anche al personale dell'azienda/ente presso cui i reclamanti lavorano, determinando così una comunicazione di informazioni personali a terzi, ovvero al personale addetto al protocollo/segreteria. Sul punto, in attesa dell'istituzione dell'Indice dei domicili digitali delle persone fisiche (che consentirà di separare l'aspetto "privato" da quello "professionale"), l'Autorità ha avviato un'attività di collaborazione con il Ministero dell'interno affinché vengano fornite indicazioni agli enti preposti ai controlli su strada sulle modalità di notifica via Pec delle contravvenzioni in conformità alla disciplina in materia di protezione dei dati personali. L'art. 3, d.m. 18 dicembre 2017 del Ministero dell'interno genericamente prevede, infatti, che la notificazione dei verbali di contestazione si effettua mediante Pec nei confronti

di colui che ha commesso la violazione. Qualora l'indirizzo Pec non sia stato fornito al momento della contestazione della violazione, esso deve essere ricercato nei pubblici elenchi per notificazioni e comunicazioni elettroniche (Ini-Pec). Con circolare 20 febbraio 2018, n. 300/A/1500/18/127/9, il Ministero dell'interno aveva fornito chiarimenti applicativi di tale disposizione, specificando che, al fine di reperire l'indirizzo Pec, "sarà sufficiente effettuare un'interrogazione dei dati dei veicoli presenti all'interno del PRA, dove, oltre agli elementi necessari alla notifica, dovrà essere reperito anche il codice fiscale del soggetto al quale dovrà essere notificato il verbale". Tuttavia tale circolare non teneva conto dell'ipotesi di abbinamento tra codice fiscale e indirizzo Pec riferibile ad una impresa o ente pubblico presso cui l'interessato lavora, potendo perciò prestarsi ad un'interpretazione non corretta circa la procedura da seguire per acquisire l'indirizzo Pec attraverso il registro Ini-Pec. Per tali ragioni il Ministero dell'interno, con la circolare 8 giugno 2020, n. 300/A/4027/20/127/9, su indicazione dell'Autorità, ha dato disposizioni agli organi accertatori di non interrogare il codice fiscale di persone fisiche nella sezione "Imprese" del registro Ini-Pec quando dagli atti non emerga chiaramente che la violazione è stata commessa con riferimento all'attività di impresa, specificando che, nei casi in cui il contravventore sia una persona fisica, la consultazione deve avvenire nella sezione "Professionisti", anche al fine di evitare di incorrere nell'eccezione in cui versano proprio le imprese individuali (abbinamento della Pec aziendale/societaria a codice fiscale di persona fisica). Nella stessa è stato altresì precisato che la ricerca degli indirizzi Pec dei contravventori non deve avvenire mediante una interrogazione massiva del registro Ini-Pec, svincolata da qualsiasi valutazione sulla fattispecie concreta da parte del Comando di polizia locale. Nel caso di abbinamento di un codice fiscale di una persona fisica a una Pec di chiara matrice "aziendale", il personale deputato alla notifica del verbale di contravvenzione procederà alla notifica del verbale via posta, secondo le modalità ordinarie (cfr. note del 13 luglio 2020).

Progetto Move-in

In attuazione dell'art. 13, comma 6-*bis*, legge Regione Lombardia, 11 dicembre 2006, n. 24 (e delle successive delibere attuative), la Regione Lombardia ha avviato il progetto Move-in (MOnitoraggio dei VEicoli INquinanti), che prevede modalità innovative per il controllo delle emissioni degli autoveicoli attraverso il monitoraggio delle percorrenze, dell'uso effettivo del veicolo e dello stile di guida adottato, tramite l'installazione sul veicolo di meccanismi elettronici che ne registrano l'attività (cd. scatola nera) fornita da operatori privati (cd. *Telematic Service Provider* o TSP), accreditati dalla Regione sulla base di un atto convenzionale intercorso con i proprietari del veicolo. Una volta installato, il dispositivo, identificato con un codice IMEI, acquisisce costantemente i dati di dettaglio relativi all'uso del veicolo (posizione, velocità di avanzamento istantanea, accelerazione lungo i tre assi, longitudinale, laterale e verticale, codice di stato, data e ora di rilevazione) e li trasmette giornalmente ai sistemi informatici del TSP prescelto; tali dati sono raccolti sui sistemi informatici dei singoli TSP e sono da questi elaborati per calcolare le percorrenze giornaliere di ogni veicolo, aggregate secondo i criteri territoriali e di eco-guida definiti dalla Regione. I dati raccolti dai TSP vengono poi trasmessi giornalmente alla piattaforma informatica gestita da Aria s.p.a. per il calcolo, in relazione a ciascun veicolo e secondo i coefficienti definiti dalla Regione, del numero di chilometri ancora disponibili sulla base di quelli già percorsi nelle aree oggetto di limitazione alla circolazione e degli eventuali *bonus* eco-guida maturati (nei casi di percorrenze su strade extraurbane e su autostrade, con velocità compresa tra 70 e 110 km/h, oppure su strade urbane, con stile di guida ecologico, calcolato sulla base degli eventi accelerometrici che caratterizzano la guida dell'interessato).

In tale quadro, la Regione Lombardia ha sottoposto al Garante uno schema di

delibera avente ad oggetto l'aggiornamento della disciplina del servizio e del trattamento dei dati personali degli utenti nonché l'estensione del servizio alle altre regioni del bacino padano e alle zone a traffico limitato (Ztl) dei comuni, in particolare alla Ztl del Comune di Milano "Area b".

Nel corso delle interlocuzioni con la Regione, l'Ufficio – sul presupposto che il progetto determina un trattamento di dati personali su larga scala con rischi elevati per i diritti e le libertà individuali, comportando anche un processo decisionale automatizzato con effetti significativi sugli interessati (ai quali, in caso di raggiungimento della soglia prefissata, può essere impedito di circolare nelle zone individuate) ed è fondato su dati relativi all'ubicazione aventi carattere personale raccolti attraverso il monitoraggio sistematico del veicolo (utilizzando nuove tecnologie) – ha fornito talune indicazioni volte ad assicurare il rispetto della disciplina in materia di protezione dei dati. In particolare, è stata evidenziata la necessità che nell'ambito del progetto siano raccolti e trattati esclusivamente i dati personali indispensabili all'attuazione dello stesso, nel rispetto dei principi di minimizzazione dei dati e di limitazione della conservazione (in particolare, garantendo che non siano raccolti, o vengano cancellati tempestivamente, i dati relativi agli spostamenti effettuati al di fuori delle aree soggette a limitazione del traffico; che non siano raccolti i dati relativi agli spostamenti una volta superata la soglia chilometrica prevista; che i dati relativi alla velocità puntuale del veicolo non siano raccolti, se tecnicamente possibile, oppure siano eliminati dai TSP, in un momento immediatamente successivo alla raccolta); che siano correttamente individuati i ruoli assunti dai diversi soggetti coinvolti; che siano assicurati accessi selettivi alle informazioni, il tracciamento delle operazioni compiute, nonché la conservazione separata dei dati raccolti attraverso i dispositivi dedicati da quelli raccolti con altri dispositivi per finalità proprie del TSP, qualora agisca in qualità di responsabile del trattamento.

Il Garante, preso atto che lo schema di delibera regionale ha tenuto adeguatamente conto di tali indicazioni e individuato le misure idonee a mitigare i rischi elevati che il trattamento presenta per i diritti e le libertà degli interessati, ha espresso il proprio parere favorevole ai sensi degli artt. 36, par. 4, e 57, par. 1, lett. *c*), del RGPD, e ha autorizzato (ai sensi degli artt. 36, par. 5, e 58, par. 3, lett. *c*), del RGPD nonché dell'art. 2-*quinquiesdecies* del Codice) i trattamenti di dati personali effettuati nell'ambito del progetto dalla Regione Lombardia, dal Comune di Milano e dalla Regione Piemonte, nonché da parte di eventuali altre regioni del bacino padano e dagli altri comuni situati nelle predette Regioni (in relazione a Ztl istituite per motivi ambientali) che, nel rispetto dei presupposti di cui all'art. 2-*ter* del Codice, riterranno in futuro di aderire al progetto, previa stipula di un accordo con Regione Lombardia, a condizione che vengano rispettate le misure individuate a garanzia degli interessati nello schema di delibera (provv. 10 dicembre 2020, n. 259, doc. web n. 9513683).

4.5.4. Il trattamento di dati personali effettuato mediante l'utilizzo di app

Prenotazione di servizi allo sportello (TuPassi)

Con riguardo al tema dell'utilizzo di *app* nel settore pubblico, il Garante, facendo seguito a un precedente provvedimento prescrittivo del 7 marzo 2019, n. 81 (doc. web n. 9121890: cfr. Relazione 2019, parr. 4.6 e 13.8), ha adottato un provvedimento sanzionatorio nei confronti di un comune per illecito trattamento di dati personali di utenti e dipendenti effettuato attraverso il sistema per la gestione delle prenotazioni dei servizi erogati al pubblico e delle code allo sportello, denominato TuPassi (cfr. anche, per i profili lavoristici, *infra* par. 13.10). I trattamenti hanno interessato un ingente numero di dati personali, anche molto delicati, in quanto relativi a prenotazioni di vari servizi; il sistema consentiva, infatti, di acquisire e

memorizzare sui *server* del comune, per un lungo periodo di tempo, numerosi dati riferibili agli utenti (tipo di prestazione, canale utilizzato, data e ora della prenotazione) come pure al personale impiegato nella gestione degli appuntamenti (data, tipo di servizio, nominativo dell'addetto allo sportello, tempo di chiamata e tempo di attesa). Tutte le operazioni erano effettuate in assenza di un'idonea informativa sui trattamenti resi possibili dall'applicativo. Né l'ente aveva disciplinato il rapporto con la società fornitrice dell'applicativo che poteva trattare dati personali nell'ambito di attività di assistenza e manutenzione del sistema in qualità di responsabile del trattamento. Ai fini della quantificazione della sanzione, l'Autorità ha valutato anche le scelte organizzative dell'ente in relazione alla corretta individuazione della figura del Rpd, soggetta ad avvicendamenti nel corso dell'istruttoria, circostanza che ha reso meno efficace la cooperazione con il Garante.

Tenuto conto che il sistema di prenotazione risultava largamente utilizzato da numerosi soggetti pubblici, tra i quali numerosi enti locali e privati, e che la maggior parte delle criticità rilevate derivavano dalle caratteristiche della versione standard originariamente distribuita dalla società (che non consentiva di configurare caso per caso la tipologia di dati trattati e i tempi di conservazione), è stato altresì adottato un provvedimento di avvertimento nei confronti della società fornitrice del servizio e di tutti i soggetti pubblici e privati che utilizzano il sistema di prenotazione TuPassi in ordine alla possibilità che il suo utilizzo, con le modalità già censurate dal Garante, possa violare il RGPD. È stato pertanto ingiunto alla società di avviare con i clienti i necessari aggiornamenti per rendere il sistema conforme alla disciplina in materia di protezione dati secondo le indicazioni del Garante (provv. 17 dicembre 2020, n. 282, doc. web n. 9525337).

Roma Riparte

L'Autorità è stata interpellata da Roma Capitale in merito alla conformità alla normativa in materia di protezione dei dati personali di una web *app* denominata "Roma Riparte", finalizzata a raccogliere segnalazioni relative a specifiche situazioni di criticità individuate sul territorio comunale (es., l'inosservanza del cd. distanziamento quale forma di contrasto alla pandemia) nonché fenomeni di molestie ed episodi di bullismo. Sotto il profilo delle finalità perseguite, l'Autorità ha specificato che se una *app* mira a realizzare molteplici finalità con il coinvolgimento di strutture e competenze dell'ente locale diversificate (servizi sociali, polizia municipale, lavori pubblici, ecc.) che operano sulla base di diversi presupposti di liceità (normativa emergenziale Covid-19, sicurezza pubblica, ecc.), il titolare deve individuare in modo puntuale, nel rispetto dell'art. 5 del RGPD, i presupposti di liceità nonché i flussi di informazioni che fanno capo a ciascuna delle strutture comunali competenti. L'Autorità ha inoltre ribadito che anche qualora non sia prevista una procedura di autenticazione informatica degli utenti per l'utilizzo di una *app*, l'indirizzo IP di chi la utilizza va considerato comunque un dato personale, atteso che consente di identificare, direttamente o indirettamente, una persona fisica (nota 4 agosto 2020).

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

Provvedimenti correttivi

Si registrano i primi provvedimenti correttivi del Garante nei confronti di enti pubblici in materia di Rpd.

In questo contesto, è stato adottato un provvedimento di ammonimento nei confronti di un comune che, tra l'altro, aveva pubblicato i dati di contatto del Rpd con modalità inidonee a soddisfare le esigenze di conoscibilità sottese al relativo obbligo (e cioè, mediante la mera affissione presso gli uffici comunali, anziché provvedendo

tramite il proprio sito web istituzionale) (provv. 12 marzo 2020, n. 56, doc. web n. 9429218).

Una sanzione amministrativa è stata comminata ad un'azienda sanitaria provinciale per omessa comunicazione al Garante dei dati di contatto del Rpd: per tale ragione, con il medesimo provvedimento è stato ingiunto di provvedere alla richiamata comunicazione all'Autorità (seguendo l'apposita procedura disponibile *online*), nonché di disporre la pubblicazione dei dati di contatto in maniera completa. Il Garante ha altresì sottolineato che un ente pubblico, nelle more della selezione del nuovo Rpd esterno, dovrebbe comunque individuare temporaneamente, al proprio interno, un dirigente/funzionario da designare interinalmente in questo ruolo, in ossequio al principio generale di continuità dell'azione amministrativa che è strettamente correlato a quello di buon andamento dell'azione stessa, effettuando anche in tale occasione la relativa comunicazione dei dati di contatto all'Autorità (provv. 1° ottobre 2020, n. 173, doc. web n. 9483375).

È stata altresì irrogata una sanzione amministrativa ad un comune in quanto, oltre ad altri profili (cfr. par. 4.4.2), non aveva provveduto a designare il Rpd né a pubblicare e a comunicare al Garante i relativi dati di contatto (provv. 17 dicembre 2020, n. 272, doc. web n. 9557593).

Infine, all'esito di un'istruttoria nei confronti di un comune che ha riguardato altri profili, con il provvedimento che ha disposto l'applicazione di una sanzione pecuniaria si è tenuto conto delle modalità con le quali l'ente ha cooperato con l'Autorità (mediante numerosi invii di documentazione, talvolta non pertinente, con inevitabili riflessi sulla tempestività della definizione del procedimento), sottolineando le difficoltà operative che hanno impedito, anche a causa delle scelte organizzative dell'amministrazione, che la figura del Rpd potesse fungere adeguatamente da referente per l'amministrazione nonché da punto di contatto per l'Autorità (provv. 17 dicembre 2020, n. 280, doc. web n. 9524175).

È proseguita, in varie forme, l'attività di supporto ai Rpd: ciò è avvenuto mediante l'organizzazione di incontri, fornendo risposte ai quesiti, aggiornando la sezione informativa presente sul sito dell'Autorità, nonché coinvolgendo sistematicamente gli stessi nelle istruttorie svolte nei confronti di enti pubblici, al fine di accrescere la consapevolezza circa il rilevante ruolo di supporto che questa figura è chiamata a rivestire nel processo di adeguamento alla disciplina in materia di protezione dei dati personali.

Sono state inviate diverse note relativamente a vari profili concernenti il ruolo e la posizione del Rpd. Tra queste si segnalano: la comunicazione inviata a un grande comune circa l'inopportunità di affidare al Rpd ulteriori incarichi (quale quello di dirigente del Corpo di polizia locale) e circa la necessità di affidargli risorse umane adeguate allo svolgimento dei complessi compiti affidati (nota 15 gennaio 2020). La comunicazione inviata ad alcune aziende sanitarie locali circa l'assenza nel Regolamento di norme che impongano la sussistenza di un rapporto di subordinazione tra la persona giuridica designata quale Rpd e la persona fisica indicata quale referente presso l'ente designante, pur sottolineando che, in sede di procedura di affidamento del servizio di Rpd, nulla osta a che possano essere richieste alle società candidate adeguate informazioni circa la persona fisica da indicare come referente e che sia inserita, all'interno del contratto, una clausola che obblighi la persona giuridica affidataria a comunicare qualsiasi variazione, intervenuta in sede di esecuzione, riguardante tale referente (nota 6 maggio 2020). La comunicazione inviata ad un ente nazionale di formazione con la quale si è ritenuto che il componente dell'organismo collegiale direttivo investito dell'incarico di Rpd della scuola non versi, per ciò stesso, in una situazione di conflitto di interessi, a condizione che siano rispettate le misure, specificatamente già previste dalle disposizioni che regolano il funzionamento

dell'organismo, per prevenire eventuali conflitti di interesse; nel caso di specie, però, si è ritenuto che la ricorrenza di un ruolo apicale direttivo (quale quello di vicepresidente dell'ente stesso) in relazione al candidato a rivestire il ruolo di Rpd determinerebbe una situazione di conflitto di interessi, potendo ostacolare l'esercizio, in maniera imparziale, dei compiti di sorveglianza sull'osservanza della disciplina e sulle politiche del titolare in materia di protezione dei dati personali (nota 14 settembre 2020). La comunicazione, inviata a comuni facenti parte di unioni di comuni, con la quale si è precisato che gli adempimenti della pubblicazione e della comunicazione all'Autorità dei dati di contatto del Rpd sono attribuiti, in conformità all'art. 37, par. 7, del RGPD, in capo a ciascun titolare (o responsabile) del trattamento, anche nel caso che questi ultimi si siano avvalsi della misura di semplificazione di cui al par. 3 dell'art. 37 con riferimento alla facoltà di designazione di un Rpd unico per più enti (nota 24 settembre 2020). La comunicazione, inviata a un comune, con la quale si è affermato che, a seguito di cessazione dell'incarico di un Rpd esterno e nelle more della conclusione della procedura di selezione del nuovo Rpd esterno, un'amministrazione pubblica è tenuta a designare un soggetto interno per lo svolgimento delle funzioni di Rpd, valutando la sussistenza di un effettivo rischio di conflitto di interessi anche in relazione all'effettivo periodo in cui tale soggetto interno manterrà l'incarico di Rpd (nota 13 ottobre 2020).

Da segnalare, infine, che il menzionato documento "Didattica digitale integrata e tutela della *privacy*: indicazioni generali", adottato dal Ministero dell'istruzione a seguito del lavoro congiunto con l'Autorità, nel fornire indicazioni agli istituti scolastici in materia di didattica digitale integrata, valorizza il ruolo del Rpd quale importante figura di supporto (*in primis*, nei confronti del dirigente scolastico) in relazione alla scelta e regolamentazione degli strumenti più adeguati al trattamento dei dati personali (cfr. par. 4.3).

Documento di indirizzo sul Rpd in ambito pubblico

Proprio in considerazione delle incertezze rilevate e delle decisioni non sempre adeguate adottate dalle amministrazioni pubbliche in merito alle scelte concernenti la figura del Rpd, è stata avviata un'istruttoria di più ampio respiro, che ha visto anche il coinvolgimento delle autorità di controllo degli altri Paesi UE attraverso una specifica procedura di assistenza reciproca volontaria, con l'obiettivo di adottare un nuovo documento di indirizzo su designazione, posizione e compiti del Rpd in ambito pubblico: attraverso la stesura di tale documento si intende approfondire le principali problematiche finora emerse sul tema e fornire, conseguentemente, gli opportuni chiarimenti, anche indicando misure volte a definire alcune *best practices* sul piano organizzativo e funzionale. Tra i profili che saranno oggetto di trattazione si segnalano, in particolare: l'omessa designazione del Rpd; l'omessa pubblicazione e/o comunicazione all'Autorità di controllo dei dati di contatto; i casi di incompatibilità con altri incarichi e di conflitto di interesse; diverse questioni relative alla procedura di selezione di un Rpd esterno; il coinvolgimento da parte dell'ente designante e le modalità di svolgimento dei suoi compiti; la messa a disposizione del Rpd delle necessarie risorse.

4.7. *Ordini professionali*

Esercizio dei diritti

Il Garante ha trattato un reclamo presentato nei confronti di un ordine professionale territoriale, concernente il mancato riscontro a una richiesta di esercizio del diritto di accesso formulata ai sensi dell'art. 15 del RGPD. Nel caso di specie, l'ordine professionale aveva dato riscontro alla richiesta dell'interessato ben oltre il termine di trenta giorni (previsto dal Regolamento) e solo a seguito dell'intervento del Ga-

rante, senza peraltro aver informato il reclamante dei motivi dell'inottemperanza e della possibilità di proporre reclamo all'autorità di controllo e ricorso giurisdizionale entro il medesimo termine. Ai fini della quantificazione della sanzione, il Garante ha considerato, tra l'altro, che la violazione era stata determinata da un comportamento colposo, al cui verificarsi aveva contribuito anche il fatto che la richiesta dell'interessato fosse stata preceduta da altre numerose comunicazioni in relazione a questioni non attinenti alla protezione dei dati personali (provv. 17 dicembre 2020, n. 276, doc. web n. 9557793).

4.8. *Digitalizzazione della pubblica amministrazione*

Con riferimento al tema della digitalizzazione della p.a., l'Autorità si è espressa su alcune linee guida predisposte da AgID in attuazione degli artt. 71 e 14-*bis* del Cad, anche se occorre segnalare che talvolta la loro adozione è avvenuta in assenza del prescritto parere del Garante (cfr. linea di indirizzo sull'interoperabilità tecnica delle p.a. e linee guida recanti regole tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del Cad), nonostante il rilievo dei trattamenti di dati personali disciplinati in tali atti.

Linee guida sulla sicurezza nel *procurement* ICT

Un parere è stato espresso sullo schema di linee guida sulla sicurezza nel *procurement* ICT (provv. 30 gennaio 2020, n. 16, doc. web n. 9283857) recanti regole di indirizzo generale rivolte ai dirigenti e ai funzionari delle p.a. che si occupano di acquisizioni informatiche, nonché ai fornitori della p.a. Esse contengono indicazioni di carattere tecnico-amministrativo per garantire, nell'ambito delle procedure per l'approvigionamento di beni e servizi informatici delle p.a., la rispondenza ad adeguati livelli di sicurezza (art. 32 del RGPD). Infatti, durante i procedimenti di acquisizione dei servizi, i fornitori possono accedere al patrimonio informativo delle p.a. committenti introducendo potenziali rischi informatici, con riflessi su riservatezza, integrità, disponibilità, autenticità dei dati pubblici. Il Garante ha inteso rilevare che, in ogni caso, qualora le p.a. si avvalgano di fornitori per compiere operazioni applicate a dati personali, devono individuare tali soggetti quali responsabili del trattamento nel rispetto dell'art. 28 del RGPD; tale individuazione deve avvenire tenendo conto dei rischi per i diritti e le libertà degli interessati nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento effettuato; i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita, di cui all'art. 25 del RGPD, dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici (cfr. cons. 78 del RGPD) attraverso strumenti, metodologie e competenze finalizzati a gestire adeguatamente i rischi che derivano dal trattamento.

Le indicazioni dell'Autorità hanno riguardato, in particolare, il contenuto del contratto (o di altro atto giuridico) che vincola il responsabile al titolare, le garanzie da richiedere in relazione all'ipotesi che il responsabile del trattamento possa ricorrere ad altro responsabile – individuando misure organizzative volte ad attribuire al titolare, in ossequio al principio di *accountability*, idonei strumenti di controllo delle attività di trattamento effettuate sotto la propria responsabilità (ad es., modalità di aggiornamento dell'elenco degli altri responsabili) –, nonché l'individuazione nell'ambito del capitolato di gara (ovvero degli altri strumenti di acquisizione di cui l'amministrazione decida di avvalersi) delle misure di sicurezza tecniche e organizzative, con una corretta ripartizione delle relative responsabilità tra titolare e responsabile per quanto concerne il trattamento dei dati personali. Inoltre, è stata richiesta l'introduzione di un requisito di sicurezza specifico volto ad esplicitare l'obbligo per

il fornitore di garantire misure tecniche e organizzative adeguate ai rischi per i diritti e le libertà degli interessati, che derivano, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, nonché un ulteriore requisito riferito all'adozione di procedure tecniche e organizzative per la gestione delle violazioni di dati personali, in conformità a quanto previsto dagli artt. 33 ss. del RGPD.

L'Autorità ha ritenuto necessario rappresentare all'Agenzia che il mero riferimento alle linee guida AgID in materia di misure minime di sicurezza nell'ambito dei requisiti di sicurezza, non è di per sé sufficiente a garantire la sicurezza del trattamento in conformità al RGPD, atteso che le misure tecniche ed organizzative che il titolare e il responsabile del trattamento sono tenuti ad adottare devono essere tali da garantire un livello di sicurezza adeguato al rischio che presenta il trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi (di varia probabilità e gravità) per i diritti e le libertà delle persone fisiche (art. 32 del RGPD).

Linee guida sulla gestione dei documenti informatici

Il Garante si è espresso anche sullo schema di linee guida relative alla formazione, gestione e conservazione dei documenti informatici (provv. 13 febbraio 2020, n. 32, doc. web n. 9283921), che hanno l'obiettivo di aggiornare, in un'ottica di semplificazione normativa, le regole tecniche concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici. Al fine di rendere il testo pienamente conforme ai principi e alle garanzie in materia di protezione dei dati personali, con particolare riferimento alla possibilità per il titolare del trattamento (p.a.) di esternalizzare alcuni servizi anche a soggetti terzi, l'Autorità ha evidenziato la necessità di specifiche garanzie sotto il profilo della sicurezza dei dati. In particolare, con riferimento al possibile utilizzo di sistemi di conservazione in *cloud*, i titolari sono tenuti ad assicurare il rispetto del principio di integrità e riservatezza nonché dei principi di protezione fin dalla progettazione e per impostazione predefinita (artt. 25 e 32 del RGPD). Nel caso di esternalizzazione del servizio di conservazione, al fine di assicurare un livello di sicurezza adeguato al rischio, i sistemi di autenticazione informatica devono garantire modalità di accesso diverse, in funzione delle tipologie di dati personali trattati nonché delle operazioni di trattamento, nel caso in cui sia consentito l'accesso diretto da parte dei soggetti autorizzati, anche da remoto, agli oggetti digitali conservati. Infine, nell'ambito delle diverse fasi di gestione documentale che vedono il coinvolgimento di soggetti diversi a cui sono attribuiti compiti e funzioni specifiche, è stata evidenziata la necessità di procedere ad una chiara attribuzione dei compiti quale presupposto necessario per garantire una corretta ripartizione delle responsabilità in relazione al trattamento dei dati personali.

Linee guida per la stesura del piano di cessazione del servizio di conservazione dei documenti digitali

Il Garante si è espresso sullo schema di linee guida per la stesura del piano di cessazione del servizio di conservazione dei documenti digitali (provv. 16 aprile 2020, n. 74, doc. web n. 9347287), i cui destinatari sono i soggetti accreditati per l'erogazione del servizio di conservazione dei documenti informatici, sia nel caso di cessazione volontaria che involontaria (ad es., in caso di ritiro dell'accreditamento). Al fine di assicurare il rispetto del Regolamento, l'Autorità ha suggerito ad AgID di integrare lo schema prevedendo che il conservatore, nel predisporre tale piano, effettui una analisi dei rischi anche tenendo conto di quelli connessi al trattamento dei dati personali valutando, tra l'altro, la presenza di particolari categorie di dati personali (come quelli relativi alla salute, alle condanne penali o a reati). Il conservatore dovrà altresì adottare adeguate misure di sicurezza per il "trasferimento degli archivi di conservazione", così da garantire riservatezza, integrità e disponibilità dei dati contenuti nei documenti. Si è poi precisato che la normativa in materia di dati

personali impone al conservatore (che in questo caso riveste il ruolo di responsabile del trattamento) precisi obblighi in materia di restituzione dei dati al produttore (titolare del trattamento) e che, in caso di cancellazione degli archivi di conservazione, questa deve avvenire con modalità sicure. Per tali ragioni l'Autorità ha chiesto di prevedere che nel processo di cessazione venga coinvolto anche il responsabile per la protezione dei dati.

Nuova procedura di identificazione da remoto per ottenere lo Spid

In relazione allo Spid, l'Autorità ha espresso il proprio parere sulla bozza di determina che modifica il regolamento recante le modalità attuative per la realizzazione dello Spid e sulla bozza di determina volta a disciplinare una nuova modalità di verifica dell'identità da remoto con l'ausilio di un bonifico bancario (provv. 17 settembre 2020, n. 163, doc. web n. 9461061). In particolare, nel modificare il citato regolamento, AgID ha previsto che con propria determinazione possano essere individuate, sentito il Garante, procedure di identificazione da remoto ulteriori rispetto a quelle già disciplinate. Anche per ragioni legate all'emergenza sanitaria, per effetto della quale le richieste di identità digitale e il conseguente carico di lavoro dei gestori sono aumentati, AgID ha ritenuto di introdurre una nuova procedura di riconoscimento da remoto per il rilascio di Spid. Tale procedura non prevede più la presenza contestuale dell'operatore del gestore dell'identità digitale e del richiedente, che dovrà però effettuare un bonifico dal suo conto corrente.

In sintesi, per ottenere Spid con la nuova modalità, il richiedente, dopo una prima registrazione sul sito del gestore, dovrà avviare una sessione automatica audio-video, durante la quale mostrerà il proprio documento di riconoscimento e il tesserino del codice fiscale o la tessera sanitaria. Per evitare tentativi di furti di identità, la procedura è stata rafforzata con specifiche misure di sicurezza e verifiche incrociate: durante la sessione audio-video, il richiedente dovrà leggere un codice ricevuto via sms o tramite un'apposita *app* installata sul cellulare personale ed effettuare un bonifico, da un conto corrente italiano a lui intestato o cointestato, indicando nella causale un codice precedentemente ricevuto. Tutte queste informazioni e la registrazione audio-video saranno in seguito verificate dall'operatore di *back-office* che procederà al rilascio dell'identità digitale. Come ulteriore misura di garanzia, e per poter valutare l'affidabilità della procedura, nel corso delle interlocuzioni per il rilascio del parere l'Autorità ha chiesto che il gestore dell'identità digitale sottoponga le richieste a ulteriori controlli a campione, con verifica della procedura da parte di un secondo operatore. Al termine di un periodo di test di sei mesi, AgID dovrà trasmettere al Garante un rapporto con l'esito di queste verifiche, così da valutare l'efficacia del controllo di secondo livello.

AgID dovrà poi inviare al Garante i *report* settimanali, redatti dai gestori Spid, relativi alle richieste di rilascio respinte per profili critici connessi al trattamento dei dati personali e configurabili come tentativi fraudolenti. Tali riscontri potranno essere utili al Garante per svolgere eventuali accertamenti e per individuare eventuali ulteriori misure tecniche e organizzative per rafforzare il procedimento di identificazione da remoto.

Linee guida per l'erogazione del servizio pubblico *Wi-Fi free*

Infine, l'Autorità ha esaminato lo schema di linee guida per l'erogazione del servizio pubblico *Wi-Fi free* (provv. 29 ottobre 2020, n. 201, doc. web n. 9487928), che offrono indicazioni alle p.a. che intendono fornire alla collettività la connessione *wireless* ad internet presso gli uffici e altri luoghi pubblici, in particolare nei settori scolastico, sanitario e turistico, anche mettendo a disposizione la porzione di banda non utilizzata dagli uffici. Le indicazioni dell'Autorità sono state volte a richiamare le p.a. sull'obbligo di garantire una corretta applicazione del RGPD, adottando misure tecniche ed organizzative adeguate al rischio e configurando il servizio in modo da assicurare la protezione dei dati trattati fin dalla progettazione e per impostazio-

4

ne predefinita. Con specifico riferimento alla possibilità per le p.a. di identificare gli utenti per poter rintracciare eventuali comportamenti fraudolenti, l'Autorità ha precisato che le amministrazioni non sono autorizzate a conservare dati di traffico telematico e ha chiesto ad AgID di integrare le linee guida indicando alle amministrazioni modalità rispettose del RGPD per individuare, *a posteriori*, i responsabili di condotte illecite (ad es. utilizzando i soli dati relativi alla connessione e disconnessione degli utenti), nonché di fornire alle amministrazioni indicazioni puntuali in merito alle tipologie di dati da raccogliere e ai tempi di conservazione, nel rispetto del principio di minimizzazione. Dovrà essere vietato qualunque trattamento di dati relativi ai dispositivi degli utenti a fini di tracciamento dell'ubicazione o degli spostamenti (mediante tecniche di *Wi-Fi location tracking*), consentendo solo l'uso di quelli indispensabili per l'accesso al servizio o per individuare, *a posteriori*, eventuali illeciti.

In considerazione del fatto che il servizio di *Wi-Fi free* pubblico viene offerto anche ai turisti, attraverso le strutture alberghiere, il Garante ha richiesto che lo schema venga integrato precisando che il turista deve poter decidere autonomamente se aderire al servizio di *Wi-Fi free* in interoperabilità o utilizzare la sola connettività alberghiera. L'eventuale interoperabilità non deve, infatti, automaticamente prevedere la comunicazione alle amministrazioni dei dati dei clienti degli alberghi.

Infine, è stato richiesto che le linee guida ribadiscano alle p.a. la necessità di adottare adeguate misure di sicurezza, anche per la gestione delle violazioni di dati personali, nonché l'adozione di specifiche cautele nel caso in cui il servizio *Wi-Fi free* sia utilizzato anche dai dipendenti della p.a. che lo fornisce.

5 La sanità

5.1. *Il trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19: l'*app *Immuni*

5.1.1. Tracciamento dei contatti fra soggetti mediante apposita applicazione su dispositivi di telefonia mobile nell'ambito delle strategie di contenimento dell'epidemia da Covid-19

Nell'ambito delle strategie di contenimento dell'epidemia Covid-19, la Presidenza del Consiglio dei ministri ha chiesto il parere del Garante su una proposta normativa per il tracciamento dei contatti individuali mediante apposita applicazione su dispositivi di telefonia mobile, successivamente confluita nell'art. 6, d.l. 30 aprile 2020, n. 28 (cfr. par. 2.1, n. 7). In materia, il Presidente del Garante aveva fornito indicazioni nell'audizione tenutasi in data 8 aprile 2020 presso la IX Commissione trasporti e comunicazioni della Camera dei deputati (doc. web n. 9308774: cfr. par. 3.1.1) in riscontro alle ipotesi avanzate all'interno del Gruppo di lavoro *data-driven* per l'emergenza da Covid-19, istituito presso la Presidenza del Consiglio dei ministri (doc. web n. 9316821).

Nel parere espresso il 29 aprile 2020, n. 79 (doc. web n. 9328050: v. anche par. 3.1.2), il Garante ha ritenuto la menzionata proposta normativa conforme ai principi fondamentali in materia di protezione dei dati personali nonché ai criteri indicati dalle linee guida del Cepd relative ai sistemi di *contact tracing* (doc. web n. 9321621). In particolare, è stato verificato che la previsione di legge fosse sufficientemente dettagliata quanto alla definizione delle modalità del trattamento, tipologia di dati raccolti, garanzie accordate agli interessati, temporaneità della misura, rilevando altresì la volontarietà nell'adesione al sistema, essendo esclusa ogni forma di condizionamento della determinazione individuale né previste disparità di trattamento connesse alla scelta di acconsentire o meno al tracciamento. È stato appurato che il trattamento in parola fosse funzionale al perseguimento di fini di interesse pubblico indicati con sufficiente determinatezza, essendo escluso il trattamento secondario dei dati raccolti per scopi diversi, salva la possibilità (nei termini generali previsti dal RGPD) di utilizzo, in forma anonima o aggregata, dei dati a fini statistici o di ricerca scientifica. La norma è risultata conforme al principio di trasparenza nei confronti dell'interessato e ai principi di minimizzazione nonché – nella misura in cui prevede la raccolta dei soli dati di prossimità dei dispositivi, escludendo il ricorso a dati di geolocalizzazione e limitandone la conservazione al tempo strettamente necessario ai fini del perseguimento dello scopo indicato, con cancellazione automatica alla scadenza del termine – a quelli della *privacy by design* e *by default.*

*5.1.2. Autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 (*app *Immuni)*

Con provvedimento del 1° giugno 2020, n. 95 (doc. web n. 9356568) è stato autorizzato il trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 (*app* Immuni). In particolare, con il parere reso ai sensi degli artt. 36, par. 5, e 58, par. 3, lett. *c*), del RGPD e dell'art. 2-*quinquiesdecies* del Codice, il Garante

5

ha autorizzato il Ministero della salute ad avviare il trattamento dei dati relativi al Sistema di allerta Covid-19, di cui all'art. 6, d.l. 30 aprile 2020, n. 28. Il trattamento di dati personali effettuato nell'ambito del Sistema è stato ritenuto legittimo e proporzionato in quanto sono stati rispettati i diritti e le libertà degli interessati e previste adeguate misure di prevenzione e diagnosi volte ad agevolare la presa in carico delle persone contagiate da parte del Ssn nonché la precoce individuazione di nuovi focolai di infezione. Ciò assicurando la trasparenza, la correttezza e la sicurezza in ogni fase del trattamento. In particolare, il Sistema comporta il trattamento dei dati necessari (es., *Temporary Exposure Key* - TEK; *Rolling Proximity Identifier* - RPI, la data di inizio dei sintomi per le persone positive al tampone naso faringeo per la rilevazione del Sars-CoV-2, l'avvenuta ricezione della notifica di esposizione) per il tracciamento dei contatti al fine di allertare, per fini di sanità pubblica, le persone che siano entrate in contatto stretto con soggetti risultati positivi.

In merito alla volontarietà dell'utilizzo dell'*app*, l'Autorità ha verificato che la autodeterminazione dell'interessato si possa manifestare in tutte le fasi del suo funzionamento: il *download*, l'istallazione, la configurazione, l'attivazione della tecnologia *bluetooth*, il caricamento delle TEK sui sistemi di *backend* di Immuni in caso di risultato positivo del tampone, la raccolta delle diverse categorie di *analytics* nelle fasi in cui si articola il trattamento, la consultazione del medico di fiducia dopo aver ricevuto un messaggio di allerta sul rischio di essere entrato in contatto stretto con soggetti risultati positivi, la disinstallazione dell'applicazione, ecc. (cfr. punti 24 e 31 delle linee guida 04/2020 sull'utilizzo dei dati di localizzazione e degli strumenti per il tracciamento dei contatti del Cepd).

Con riferimento alla pseudonimizzazione dei dati personali, è stata condivisa la scelta di consentire la distribuzione delle chiavi TEK (vale a dire il risultato della pseudonimizzazione) ai partecipanti al Sistema, ma non anche delle chiavi di decodifica (vale a dire l'informazione aggiuntiva), di fatto precludendo in radice di risalire all'identità di qualsiasi altro partecipante. A tal riguardo, la previsione di adeguate tecniche di cifratura asimmetrica (ad es., basate su algoritmi di *hash*) con un'adeguata custodia delle chiavi da parte del soggetto centrale (l'unico in grado di addivenire alla reidentificazione per ragioni meramente funzionali all'operatività del Sistema) ha permesso di introdurre uno schema di pseudonimizzazione idoneo a realizzare il disaccoppiamento tra le TEK e le loro chiavi di decodifica, atto a garantire la corretta applicazione dell'art. 6, comma 2, lett. *c*), d.l. n. 28/2020, nonché, su tale base, la pubblicazione delle TEK dei soli soggetti risultati positivi. Ciò stante, il Garante, nell'autorizzare il trattamento, ha raccomandato che:

- l'algoritmo, basato su criteri epidemiologici di rischio e modelli probabilistici, sia puntualmente indicato e costantemente aggiornato nella valutazione d'impatto, in osservanza del principio di responsabilizzazione, rendendolo disponibile allo scrutinio da parte della comunità scientifica;
- gli utenti siano adeguatamente informati in ordine alla possibilità che l'*app* generi notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio e siano fornite agli stessi informazioni semplici e chiare sul funzionamento dell'algoritmo (anche attraverso una cd. infografica);
- gli utenti dell'*app* possano temporaneamente disattivare la stessa attraverso una funzione facilmente accessibile nella schermata principale e che di tale funzione di disattivazione temporanea siano informati gli utenti in modo chiaro attraverso le infografiche visualizzate all'atto dell'installazione dell'*app*;
- gli *analytics* siano accuratamente protetti nel *backend* di Immuni, evitando ogni forma di riassociazione degli stessi a interessati identificabili e assicurando l'adozione di adeguate misure di sicurezza e tecniche di anonimizzazione,

da individuarsi in ragione delle specifiche finalità in concreto perseguite, nel rispetto dei principi di *privacy by design* e *by default*;
- con specifico riferimento all'utilizzo dell'*app* anche da parte di minori ultraquattordicenni, sia prestata particolare attenzione alle informazioni da fornire e al contenuto dei messaggi di avvenuta esposizione a rischio di contagio;
- la funzionalità necessaria ad adattare l'utilizzo dell'*app* in contesti in cui sarebbero prodotti falsi positivi, sopra descritta, possa utilmente essere impiegata per garantire l'esercizio del diritto di opposizione qualora l'utente ne ravvisi l'esigenza, su base temporanea, evitando di ricorrere alla soluzione più radicale della disinstallazione dell'*app*.

In relazione ai rischi elevati presentati dal trattamento, individuati anche nella valutazione d'impatto, il Garante ha ravvisato poi l'opportunità di apportare ulteriori miglioramenti alla sicurezza complessiva intervenendo sui seguenti aspetti:
- conservazione degli indirizzi Ip dei dispositivi mobili: necessità di commisurare i tempi di conservazione nella misura strettamente necessaria al rilevamento di anomalie e di attacchi. Ciò in quanto gli indirizzi Ip possono costituire quell'informazione aggiuntiva che, collegata ai dati raccolti, in determinate circostanze, consente l'identificazione degli utenti;
- tracciamento delle operazioni compiute dagli amministratori di sistema: necessità di introdurre misure volte ad assicurare il tracciamento delle operazioni compiute sui sistemi operativi, sulla rete e sulle basi dati;
- caricamento erroneo di TEK non riferite a soggetti positivi a seguito di errori materiali o diagnostici: necessità di considerare l'ulteriore scenario di compromissione dell'integrità dei dati derivante dall'ipotesi in cui, una volta pubblicate le TEK di un soggetto ritenuto positivo, per varie ragioni (ad es., casi di omonimia, scambio di referti, errori materiali), si renda necessario un intervento di rettifica dei dati inseriti al fine di ripristinarne l'accuratezza.

5.1.3. Trattamenti di dati personali effettuati tramite il Sistema tessera sanitaria nell'ambito del Sistema di allerta Covid-19

Il provvedimento di autorizzazione dell'*app* relativa al Sistema allerta Covid-19 si completa con il parere fornito dal Garante, in pari data, sullo schema di decreto del Mef relativo ai trattamenti di dati personali effettuati tramite il Sistema tessera sanitaria (Sistema TS) (parere 1° giugno 2020, n. 94, doc. web n. 9357932). Le misure indicate nello schema di decreto in parola completano infatti l'individuazione dei dati personali raccolti dall'*app*, necessari ad avvisare gli utenti della stessa di rientrare tra i contatti stretti di altri utenti accertati positivi al Covid-19, che sono stati determinati dal Ministero della salute e specificati nell'ambito della valutazione di impatto presentata al Garante contestualmente al menzionato schema di decreto (art. 6, comma 2, lett. *b*), d.l. n. 28/2020).

Secondo quanto riportato nello schema di decreto, il Sistema TS rende disponibili agli operatori del Dipartimento di prevenzione delle Asl, anche tramite i Sistemi di accoglienza regionale (Sar), le funzionalità per la trasmissione di alcuni dati al Sistema di allerta Covid-19. In caso di esito positivo di un tampone naso faringeo per la rilevazione del Sars-CoV-2, l'operatore del competente Dipartimento di prevenzione dell'Asl contatta il paziente per effettuare l'indagine epidemiologica che prevede anche la verifica dell'installazione dell'*app* Immuni. Se il paziente ha installato l'*app*, gli sarà richiesto di utilizzare la funzione di generazione del codice OTP che il paziente comunicherà all'operatore; a questo punto, ottenuta l'autorizzazione, il sistema procederà con il caricamento sul *server* di *backend* del Sistema di allerta Covid-19 delle chiavi crittografiche casuali (TEK) generate dal dispositivo mobile su

cui è installata l'*app* (art. 2 dello schema di decreto). Ciò in conformità alle disposizioni di settore che attribuiscono proprio ai menzionati Dipartimenti di prevenzione il compito di ricostruire la filiera dei contatti stretti del soggetto risultato positivo al Covid-19 e di determinare le misure di contenimento di contagio più opportune (art. 3, comma 6, d.P.C.M. 8 marzo 2020 e circolare 22 febbraio 2020, n. 5443 del Ministero della salute, e successive modificazioni e integrazioni). L'Ufficio ha altresì rappresentato la necessità che, con riferimento ai trattamenti effettuati tramite il Sistema TS nell'ambito del Sistema di allerta Covid-19, il Mef sia designato responsabile del trattamento ai sensi dell'art. 28 del RGPD.

Nell'ambito della collaborazione istituzionale, sono stati espressi alcuni rilievi tecnici anche in relazione alle procedure di autenticazione informatica per l'accesso alla funzionalità del Sistema TS da parte degli operatori sanitari, alle informazioni memorizzate nei *file* di *log* e al relativo periodo di conservazione, alle procedure di autenticazione informatica per l'accesso al Sistema TS da parte dei cd. amministratori di sicurezza, alle informazioni memorizzate nei *file* di *log* degli accessi e delle operazioni compiute dagli amministratori di sistema e al relativo periodo di conservazione.

5.1.4. Il call center *Immuni*

L'art. 20, d.l. 28 ottobre 2020, n. 137 (cd. d.l. Ristori) ha previsto che il Ministero della salute attivi un Servizio nazionale di supporto telefonico e telematico alle persone risultate positive al virus Sars-CoV-2 che hanno avuto contatti stretti o casuali con soggetti risultati positivi o che hanno ricevuto una notifica di allerta attraverso l'applicazione Immuni. Il Commissario straordinario, in virtù della delega del Ministero della salute a disciplinare l'organizzazione e il funzionamento del suddetto Servizio, ha sottoposto al parere del Garante – poi espresso il 17 dicembre 2020, n. 273 (doc. web n. 9516719: cfr. par. 2.1, n. 2) – uno schema di ordinanza concernente le modalità di funzionamento del menzionato Servizio nazionale (cfr. anche par. 3.2).

Al riguardo, l'Ufficio, nel corso delle interlocuzioni con il Ministero della salute, il Mef, la struttura commissariale e il Dipartimento per la trasformazione digitale presso la Presidenza del Consiglio dei ministri, ha fornito il proprio contributo affinché, seppur con l'urgenza connessa al contesto emergenziale, le soluzioni individuate fossero conformi alla disciplina in materia di protezione dei dati. Le osservazioni così formulate hanno riguardato l'individuazione di una procedura per autorizzare il caricamento delle chiavi (TEK) del dispositivo mobile del soggetto risultato positivo – su cui è installata l'*app* Immuni – conforme alla disciplina in materia di protezione dei dati personali e, in particolare, alle disposizioni relative al Sistema di allerta Covid-19, al relativo provvedimento di autorizzazione dell'Autorità del 1° giugno 2020, nonché all'art. 20, d.l. Ristori, a cui lo schema di ordinanza dà attuazione.

Con specifico riferimento alla procedura di autorizzazione, sono state formulate osservazioni con riguardo alle modalità attraverso le quali gli operatori del Servizio possono accertare l'identità del chiamante e verificare che lo stesso sia un caso accertato di positività al Covid-19, senza che sia creata una banca dati dei referti liberamente consultabile dagli operatori del *call center* Immuni.

In merito alle regole di generazione del Codice univoco nazionale (Cun) rilasciato dal Sistema TS, che identifica univocamente, a livello nazionale, tutti gli esiti (positivi e negativi) dei test per Covid-19, anche a seguito di interlocuzioni con il Ministero della salute, il Mef, la struttura commissariale e il Dipartimento per la trasformazione digitale presso la Presidenza del Consiglio dei ministri, è stato rite-

nuto che l'identificazione del chiamante e del suo stato di positività al Covid-19, attraverso il Cun associato al codice fiscale dello stesso, fosse preferibile rispetto alle altre possibili modalità operative del Servizio, in conformità alla normativa in materia di protezione dei dati personali e alla disciplina di settore sopra richiamata relativa al Sistema di allerta Covid-19. Sono state inoltre formulate osservazioni anche con riferimento al ruolo dei *call center* e del Commissario straordinario relativamente al trattamento dei dati personali effettuato nell'ambito del suddetto Servizio, evidenziando in particolare la necessità che il Ministero della salute integri la designazione a responsabile del trattamento del Mef.

In occasione delle richiamate interlocuzioni è stata evidenziata la necessità che la piattaforma utilizzata dagli operatori del *call center* Immuni per accedere al Sistema TS sia progettata e realizzata adottando misure di sicurezza, tecniche e organizzative, adeguate al rischio presentato dal trattamento, con particolare riferimento alle modalità di autenticazione informatica, ai profili di autorizzazione e al tracciamento delle operazioni compiute dagli operatori. È stato pure richiesto che il Ministero della salute assicuri una costante vigilanza nei confronti dei responsabili del trattamento, anche attraverso apposite attività di *audit*.

Riguardo alla protezione dei dati personali dell'interessato risultato positivo che intende "sbloccare" l'*app* Immuni, è stata segnalata la necessità di adottare cautele adeguate a scongiurare il rischio di indebolire l'efficacia della pseudonimizzazione quale principale misura di garanzia adottata nell'ambito del Sistema di allerta Covid-19. Ciò con particolare riguardo alle attività effettuate dal *call center* Immuni e dai Dipartimenti di prevenzione delle Asl che provvedono alla raccolta e al successivo trattamento del Cun e/o del codice fiscale dell'interessato.

È stato infine ritenuto necessario che la comunicazione del Cun all'assistito sia effettuata esclusivamente al numero di telefonia mobile o all'indirizzo *e-mail* fornito dallo stesso all'atto dell'esecuzione del test e che il Ministero della salute aggiorni, ai sensi degli artt. 35, par. 11, del RGPD e 6, comma 2, d.l. n. 28/2020, la valutazione di impatto sulla protezione dei dati relativa ai trattamenti effettuati nell'ambito del Sistema di allerta Covid-19.

5.2. *Dematerializzazione delle prescrizioni mediche*

5.2.1. Modalità di consegna della ricetta dematerializzata

Con parere 19 marzo 2020, n. 58 (doc. web n. 9296257), il Garante si è espresso sulle modalità di consegna della ricetta dematerializzata. Sebbene la dematerializzazione della ricetta medica per le prescrizioni a carico del Ssn fosse stata introdotta con decreto del Mef del 2 novembre 2011, non erano stati definiti negli anni i canali alternativi sui quali, su richiesta dell'assistito, il promemoria della ricetta dematerializzata potesse essere reso disponibile. Al riguardo l'Autorità, sin dal 2015 aveva evidenziato al Ministero della salute che la mancata individuazione di modalità alternative alla stampa del promemoria cartaceo aveva determinato il diffondersi di iniziative autonome da parte dei medici, molto differenziate sul territorio nazionale, che presentavano profili di criticità in merito alla sicurezza del trattamento dei dati relativi allo stato di salute degli assistiti dal Ssn (nota 2 ottobre 2015: cfr. Relazione 2015, p. 72).

In tale contesto, l'Autorità aveva da tempo manifestato la propria disponibilità ad avviare un confronto con le amministrazioni deputate a intervenire sulla materia, al fine di assicurare il trattamento dei dati personali nel rispetto della dignità e della riservatezza degli interessati e con modalità uniformi sull'intero territorio nazionale,

evidenziando la possibilità di prevedere canali digitali, alternativi alla stampa cartacea, rispettosi della disciplina in materia di trattamento dei dati sulla salute, come del resto già normativamente previsto in altri ambiti sanitari (cfr. 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, nonché di effettuazione del pagamento *online* delle prestazioni erogate, su cui l'Autorità ha fornito il parere del 6 dicembre 2012, n. 382, doc. web n. 2223206; cfr. anche la disciplina sul Fse, di cui all'art. 12, d.l. n. 179/2012).

Il contesto emergenziale ha favorito l'esigenza di portare a compimento il processo di dematerializzazione della ricetta per evitare che gli assistiti si recassero negli studi medici per questioni amministrative e così contenere la diffusione del virus Sars-CoV-2. Sul punto, l'Autorità ha condiviso la scelta, effettuata dal Ministero, di individuare i canali di trasmissione del promemoria, con misure adeguate a tutela dei dati personali degli assistiti, valide su tutto il territorio nazionale e alle quali le regioni e le province autonome dovranno adeguarsi. Lo schema di decreto sottoposto al Garante ha fatto rinvio a un ulteriore atto normativo concordato con il Ministero della salute per l'individuazione delle specifiche modalità di trasmissione all'assistito del promemoria dematerializzato della ricetta elettronica (cfr. par. 5.2.2).

Nel corso delle richiamate interlocuzioni con il Mef sono state manifestate alcune perplessità in merito alla delimitazione, prevista in una prima versione dello schema di decreto, delle modalità alternative al promemoria cartaceo alla sola consultazione del Fse, attesa la non completa attuazione dello stesso sull'intero territorio nazionale, la cui attivazione è (allo stato) rimessa all'interessato.

Tali osservazioni sono state recepite e, nella versione dello schema di decreto sottoposta al parere del Garante, si è previsto che siano individuati canali ulteriori, rispetto al Fse, per la consegna all'assistito del promemoria dematerializzato della ricetta elettronica.

5.2.2. Estensione della ricetta elettronica ai farmaci non a carico del Ssn e modalità facilitate per la ricezione del promemoria dematerializzato della ricetta

Con parere del 2 aprile 2020, n. 66 (doc. web n. 9308089) il Garante si è espresso sullo schema di decreto che completa la disciplina in materia di dematerializzazione delle prescrizioni a carico del Ssn, da poco innovata con il decreto del Mef del 25 marzo 2020 (sul quale il Garante aveva reso il proprio parere pochi giorni prima, il 19 marzo). Il decreto in parola aveva infatti definito i canali attraverso i quali effettuare la consegna del cd. promemoria dematerializzato della ricetta elettronica all'assistito, rimettendo a un successivo decreto dello stesso Dicastero, da adottarsi di concerto con il Ministero della salute e sentito il Garante, le modalità di rilascio del promemoria dematerializzato (art. 3-*bis*, d.m. 2 novembre 2011, introdotto dal d.m. 25 marzo 2020). Nello schema di decreto si sono quindi individuate, con il concerto del Ministero della salute, le modalità attraverso le quali l'assistito può accedere al portale Sistema TS per consultare e "scaricare" le proprie ricette elettroniche generate dai medici prescrittori e i relativi promemoria dematerializzati e per utilizzare questi ultimi direttamente presso la farmacia prescelta, individuando altresì le modalità di dematerializzazione delle prescrizioni di farmaci non a carico del Ssn.

Le interlocuzioni con il Mef e con il Ministero della salute si sono incentrate sulla individuazione di soluzioni di facile e immediata implementazione per comunicare gli estremi della prescrizione alla farmacia individuata dall'assistito affinché questi possa recarsi direttamente presso la stessa per ritirare il farmaco.

5.2.3. Dematerializzazione della ricetta

Successivamente all'adozione del richiamato parere del 2 aprile 2020, il Mef ha rappresentato di aver modificato lo schema di decreto, già sottoposto all'attenzione dell'Autorità, per recepire le osservazioni espresse dalle regioni e dall'Ordine dei farmacisti, anche con riferimento all'emergenza sanitaria da Covid-19.

In particolare, le modifiche apportate al precedente schema di decreto sono state funzionali all'esigenza di specificare che il processo di dematerializzazione della ricetta riguarda sia quelle ripetibili (valide per l'acquisto ripetuto di farmaci), sia quelle non ripetibili e che tale processo, come già disciplinato dalle vigenti disposizioni in tema di ricetta elettronica a carico del Ssn, può essere integrato con i Sistemi informativi regionali (Sar).

La revisione dello schema di decreto ha portato poi ad evidenziare la necessità, espressa dalle regioni, di precisare che resta ferma la possibilità per l'interessato di consultare il promemoria della ricetta dematerializzata anche attraverso il proprio Fse.

Tenendo conto delle osservazioni formulate dall'Ordine dei medici e dei farmacisti, il Mef ha poi evidenziato la necessità di sopprimere l'art. 4, commi 5 e 6, della versione di schema di decreto su cui l'Autorità aveva espresso il richiamato parere il 2 aprile 2020, relativa alla possibilità per l'interessato di delegare telefonicamente il medico prescrittore, al momento della compilazione della ricetta elettronica, all'invio del promemoria direttamente a una farmacia specificatamente indicata. Nello schema di decreto, come evidenziato nel parere, permangono le garanzie in materia di protezione dei dati personali già individuate nella precedente versione trasmessa all'Autorità, che teneva conto delle indicazioni fornite dall'Ufficio anche con riferimento ai trattamenti effettuati nel contesto emergenziale (provv. 12 novembre 2020, n. 218, doc. web n. 9519603).

5.3. *Indagine di sieroprevalenza sulla diffusione del virus Sars-Cov-2*

Il Garante si è espresso su uno schema di disposizione normativa di rango primario proposta dal Ministero della salute volta in particolare a consentire, attraverso l'istituzione di una specifica piattaforma tecnologica, la realizzazione di studi epidemiologici e di statistiche affidabili e complete da parte del Ministero della salute e dell'Istat sullo stato immunitario della popolazione, indispensabili per garantire la protezione dall'emergenza sanitaria in atto, evidenziando specifiche criticità correlate all'applicazione dei principi in materia di protezione dei dati personali (parere 4 maggio 2020, n. 82, doc. web n. 9340513: v. anche parr. 2.1, n. 6 e 3.1.2).

In primo luogo, è stato osservato come lo schema inizialmente proposto individuasse una serie di finalità di rilevante interesse pubblico eccessivamente eterogenee tra loro (in particolare, attività amministrative e certificatorie correlate all'assistenza sanitaria o sociale, tutela e cura della salute, di sanità pubblica, protezione civile, programmazione sanitaria, ricerca scientifica, medica, biomedica ed epidemiologica nonché statistica), ciascuna presidiata nell'ordinamento da specifiche misure a tutela degli interessati che la disposizione, così come inizialmente concepita, non avrebbe consentito di rispettare.

L'Autorità ha poi evidenziato come il trattamento di dati personali per scopi statistici e di ricerca scientifica, se svolto da soggetti facenti parte del Sistan, debba conformarsi – oltre che alle norme del RGPD (artt. 5, par. 1, lett. *c*) ed *e*), e 89) e del Codice (artt. 104 e ss.) – anche alle pertinenti regole deontologiche (art. 2-*quater* e all. A4 e A5 al Codice) e alla specifica disciplina di settore di cui al d.lgs. n.

322/1989. In tal senso, il Garante ha sottolineato l'esigenza che l'individuazione da parte dell'Istat, sulla base delle fonti amministrative di cui dispone per i propri fini istituzionali, di un campione di popolazione da sottoporre ad accertamento sierologico, i cui risultati sarebbero stati utilizzati per perseguire le finalità di cui alla norma in esame, dovesse essere riconsiderata alla luce del divieto di utilizzo dei dati trattati a fini statistici o di ricerca scientifica per l'assunzione di decisioni o provvedimenti individuali o comunque per fini eterogenei (art. 105 del Codice, cons. 162 del RGPD, cons. 27 del regolamento (CE) n. 2009/223 sulle statistiche europee e art. 4 della raccomandazione del Consiglio d'Europa n. R(97) relativa alla protezione dei personali raccolti e trattati per scopi statistici; cfr. anche parere del Garante sullo schema di Programma statistico nazionale 2017-2019, Aggiornamento 2018-2019 del 9 maggio 2018, n. 271, doc. web n. 9001732).

Su tali basi, è stata ritenuta non conforme la previsione dell'accesso da parte delle regioni e delle province autonome per finalità di analisi e programmazione nell'ambito dell'emergenza epidemiologica ai dati identificativi trasmessi dall'Istat all'apposita piattaforma del Ministero della salute, arricchiti di quelli sulla salute e genetici, suscettibili peraltro di interconnessione con ulteriori, non meglio precisati, dati personali presenti in banche dati dell'Istat e del medesimo Dicastero.

Parimenti critica è stata considerata la previsione dell'interconnessione dei dati sulla salute e genetici raccolti nell'ambito dell'indagine di sieroprevalenza tra numerosissimi soggetti cui sono attribuite differenti competenze e funzioni, quali il Ministero della salute, l'Istat, la Croce rossa italiana, le regioni, le province autonome, i laboratori che effettuano il prelievo e gli altri soggetti (tra i quali, università e centri ricerca), nonché l'Istituto superiore di sanità (Iss). Ciò in quanto, per effetto di una disposizione siffatta, numerosi soggetti, in parte indeterminati, sarebbero stati autorizzati ad accedere a informazioni individuali sanitarie e genetiche su larga scala, senza un'adeguata esplicitazione delle finalità del trattamento, dei ruoli ricoperti (con le conseguenti responsabilità), delle misure a garanzia dei diritti e delle libertà degli interessati.

Tali trattamenti sono stati ritenuti incompatibili, oltre che con il principio di cui all'art. 105 del Codice, anche con la disciplina del segreto statistico, con il regime di comunicabilità dei dati raccolti dall'Istat di cui al d.lgs. n. 322/1989, nonché con le citate regole deontologiche e il disposto dell'art. 5-*ter*, d.lgs. n. 33/2013. Su tali basi, il Garante ha ritenuto necessario che, nell'ambito dei sistemi informativi del Ministero della salute e delle regioni, fosse previsto il trattamento di dati aggregati risultanti dall'indagine di sieroprevalenza effettuata a scopi statistici e di ricerca scientifica.

Con riferimento alla creazione del campione, lo schema di disposizione faceva riferimento al concetto di stratificazione della popolazione sul quale il Garante si era già espresso con un parere reso al Consiglio di Stato in relazione a un progetto del medesimo Ministero della salute basato sulla stratificazione della popolazione (cfr. parere 5 marzo 2020, n. 43, doc. web n. 9304455). È stata pertanto ribadita la necessità che tale attività fosse in ogni caso preceduta da un'adeguata analisi dei rischi per i diritti degli interessati, nel rispetto dei principi di responsabilizzazione e protezione dei dati personali fin dalla progettazione (artt. 5, par. 2 e 25 del RGPD).

Banca biologica nazionale contenente i campioni di fonte sierologica

Il Garante ha infine ritenuto necessario che fossero meglio definite le caratteristiche essenziali dell'istituenda banca biologica nazionale contenente i campioni di fonte sierologica, richiedendo, in particolare, l'indicazione dell'ambito di istituzione, delle finalità perseguite, della titolarità del trattamento, delle operazioni eseguibili, dei soggetti legittimati all'accesso e delle misure di sicurezza adeguate, anche tenuto conto del trattamento di dati genetici ivi previsto.

A seguito della trasmissione del parere al Ministero richiedente, sono state avviate intense e proficue interlocuzioni tra gli uffici del Ministero della salute, dell'Istat, della Protezione civile e dell'Autorità che hanno consentito di riformulare la disposizione in modo da superare i rilievi evidenziati.

5.4. *Sistema di refertazione dei tamponi antigenici rapidi da parte dei medici di medicina generale e dei pediatri di libera scelta*

Il Garante ha espresso il proprio parere su uno schema di decreto del Mef concernente le modalità attuative del sistema di refertazione dei tamponi antigenici rapidi da parte dei medici di medicina generale e dei pediatri di libera scelta e di messa a disposizione dei referti elettronici agli interessati e ai soggetti deputati alle operazioni di *contact tracing* tramite il Sistema TS (parere d'urgenza del Presidente, 3 novembre 2020, n. 215, doc. web n. 9563445: cfr. par. 2.1, n. 2).

Al riguardo, l'Ufficio, nel corso delle interlocuzioni con il Mef e con il Ministero della salute, ha fornito il proprio contributo affinché, seppur con l'urgenza connessa al contesto emergenziale, le soluzioni individuate fossero rispettose della disciplina in materia di trattamento dei dati sulla salute. Le osservazioni formulate hanno riguardato in particolare la necessità che fosse definita la titolarità del trattamento in capo al Mef, le modalità con cui rendere le informazioni di cui agli artt. 13 e 14 del RGPD agli interessati e che le misure a protezione dei dati trattati descritte nel disciplinare tecnico fossero individuate e adottate a seguito di una valutazione dei rischi per i diritti e le libertà degli interessati, costantemente verificata.

L'Ufficio ha collaborato per individuare le modalità attraverso le quali i medici, utilizzando le funzionalità del Sistema TS, anche tramite servizi web, possano predisporre il referto elettronico relativo al tampone naso faringeo per la rilevazione del Sars-CoV-2 eseguito per ciascun assistito, individuato univocamente a livello nazionale dal Numero di referto elettronico (Nrfe) assegnato dal Sistema TS in fase di compilazione del referto da parte del medico; il Nrfe costituisce così la chiave attraverso la quale identificare e rendere disponibile il referto all'interessato.

È stato inoltre assicurato che il referto sia reso disponibile all'assistito, nel rispetto della disciplina in materia di protezione dei dati personali, con diverse modalità: attraverso il Fse; inserendo nella Piattaforma nazionale del Sistema TS il Nrfe ricevuto dal medico (anche via sms), il codice fiscale e la data di scadenza della tessera sanitaria, oppure mediante un messaggio di posta elettronica. La Piattaforma verrà utilizzata anche dall'operatore sanitario del dipartimento di prevenzione dell'Asl territorialmente competente al fine di contattare il paziente per effettuare l'indagine epidemiologica, che (come detto) prevede anche la verifica dell'installazione dell'*app* del Sistema di allerta Covid-19 nei casi confermati di Covid-19.

Con specifico riferimento alle modalità di accesso da parte dell'interessato alla Piattaforma nazionale, il Garante ha suggerito le seguenti misure ulteriori a garanzia della riservatezza dei dati: a) la possibilità, per l'interessato, di non rendere più consultabile il singolo referto attraverso la Piattaforma; b) la visualizzazione, nell'area riservata all'utente, della data e dell'ora degli ultimi accessi alla Piattaforma, al fine di consentire allo stesso di controllare le consultazioni che sono state effettuate al referto del tampone; c) l'adozione di un meccanismo di tipo CAPTCHA in grado di contrastare efficacemente eventuali attacchi a "forza bruta" (*brute force*), basati sull'enumerazione delle credenziali di accesso e condotti mediante l'utilizzo di sistemi automatici (*bot*); d) la definizione che l'accesso con modalità semplificata sia limitato esclusivamente al referto identificato dal Nrfe.

5

5.5. *Diffusione di dati sulla salute di pazienti affetti da Covid-19*

Numerosi i reclami e le segnalazioni trattate concernenti la diffusione da parte di strutture sanitarie di dati sulla salute di pazienti affetti o deceduti per Covid-19.

In un caso, i parenti di un paziente deceduto a causa delle complicanze del Covid-19 hanno segnalato al Garante che l'ospedale che aveva prestato le cure al loro caro aveva diffuso numerose informazioni di dettaglio sulla storia clinica del defunto mediante la diramazione di un comunicato stampa, riportato poi da alcune testate giornalistiche locali. Il Garante ha sanzionato il titolare del trattamento, avendo accertato che, tramite il comunicato, la struttura sanitaria aveva effettuato una diffusione di numerosi dati sulla salute del paziente deceduto per Covid-19 espressamente vietata dal Codice (provv. 27 gennaio 2021, n. 35, doc. web 9549143). Nel provvedimento l'Autorità ha ritenuto che l'esigenza di informare l'opinione pubblica sull'appropriatezza dell'assistenza prestata ai pazienti ricoverati per Covid-19, richiamata dalla struttura sanitaria, non richiedeva la diffusione di informazioni cliniche di dettaglio sullo stato di salute del paziente.

Al riguardo, con specifico riferimento alla diffusione di dati personali riguardanti persone risultate positive al Covid-19 sui *social media* e sugli organi di stampa, anche digitali, sin dall'inizio della pandemia il Garante ha sottolineato che anche nella situazione di emergenza sanitaria, nella quale l'informazione svolge un servizio indispensabile per la collettività, non possono essere disattese alcune garanzie a tutela della riservatezza e della dignità delle persone colpite dalla malattia contenute nella normativa vigente e nelle regole deontologiche relative all'attività giornalistica (v. comunicato stampa 31 marzo 2020, doc. web n. 9303613).

Alcune istruttorie sono state avviate con riferimento alla diffusione di notizie relative allo stato di salute di soggetti affetti da Covid-19 da parte del personale sanitario operante presso le strutture ove erano ricoverati gli interessati.

Attraverso lo strumento delle FAQ, sono state poi fornite indicazioni in ordine al divieto di diffondere i dati identificativi delle persone positive al Covid-19 o sottoposte ad isolamento domiciliare. È stato infatti chiarito che le aziende sanitarie e qualsiasi altro soggetto pubblico o privato non possono diffondere, attraverso siti web o altri canali, i nominativi dei casi accertati di Covid-19 o dei soggetti sottoposti alla misura dell'isolamento per finalità di contenimento della diffusione dell'epidemia (cfr. FAQ su trattamento dati nel contesto sanitario nell'ambito dell'emergenza sanitaria).

5.6. *Sistemi informativi regionali per il controllo della diffusione del virus*

Nell'ambito dell'emergenza sanitaria sono state avviate alcune istruttorie in merito a trattamenti dei dati effettuati tramite *app* promosse da regioni e da altri soggetti pubblici.

In particolare, a seguito di numerose segnalazioni, l'Ufficio ha avviato procedimenti istruttori in merito al trattamento effettuato con *app* regionali aventi una pluralità di finalità: tracciare una mappa del contagio tramite la compilazione di un questionario giornaliero da parte degli utenti, monitorare la diffusione del virus dei contagiati asintomatici previamente registrati su un apposito portale, controllare i soggetti in isolamento domiciliare, tracciare i contatti, censire i soggetti che facevano ingresso nel territorio regionale nonché raccogliere autodichiarazioni circa la sintomatologia da Covid-19 per facilitare i rapporti tra il paziente e l'operatore sanitario.

Al riguardo, anche attraverso lo strumento delle FAQ, il Garante ha rappresen-

tato che la normativa d'urgenza adottata per il Covid-19 ha previsto misure rigorose per lo svolgimento delle visite mediche al fine di favorire l'adozione di misure di protezione per il paziente e per il personale sanitario, nonché per garantire il distanziamento interpersonale tra gli stessi pazienti.

In tale contesto, le strutture sanitarie che intendono avvalersi di strumenti di telemedicina (*app* di telediagnosi, teleconsulto, teleassistenza e telemonitoraggio utilizzate dal personale medico) per effettuare diagnosi o terapie a distanza non devono richiedere uno specifico consenso al trattamento dei dati personali dell'interessato, in quanto si tratta di una diversa modalità di svolgimento del rapporto medico-paziente (cfr. in particolare art. 9, par. 2, lett. *h*) e par. 3 del RGPD). Il titolare del trattamento dovrà in ogni caso provvedere a effettuare la valutazione di impatto (art. 35 del RGPD), fornire all'interessato un'informativa completa con riferimento al trattamento dei dati effettuato attraverso l'*app*, nonché assicurare il rispetto dei principi di integrità, riservatezza ed esattezza dei dati trattati. È stato poi precisato che il Ssn deve garantire la prestazione sanitaria anche a coloro che non possono o non intendono installare *app* di telemedicina (cfr. FAQ - *app* nazionale di *contact tracing* e *app* regionali per Covid-19).

Nel caso della Regione Veneto, l'Ufficio è stato coinvolto con riferimento all'attuazione della legge regionale 17 novembre 2020, n. 35, volta ad istituire e implementare una piattaforma informatica regionale per il monitoraggio dell'emergenza epidemiologica da Covid-19. In particolare, si prevede che, all'esito della valutazione di impatto sul trattamento dei dati posti in essere attraverso la piattaforma, la Regione proceda a richiedere l'autorizzazione del Garante ai sensi dell'art. 2-*quinquiedecies* del Codice.

Alcune regioni che avevano promosso *app* di *contact tracing* su base volontaria (sulle quali l'Ufficio aveva avviato specifiche attività istruttorie) hanno interrotto tali iniziative a seguito dell'adozione dell'*app* di *contact tracing* nazionale.

A fronte delle diverse iniziative a livello regionale, il Garante, al fine di richiamare il quadro normativo legato ad un sistema di *contact tracing* digitale e uniformare a livello nazionale le garanzie poste a tutela degli interessati, ha elaborato le FAQ - *app* nazionale di *contact tracing* e *app* regionali per Covid-19 (pubblicate sul sito il 13 luglio 2020). In particolare, con specifico riferimento alle *app* regionali, è stato chiarito che la loro installazione non può essere obbligatoria e non può condizionare l'accesso ad aree o territori, in quanto ciò inciderebbe sull'esercizio dei diritti fondamentali degli interessati, tra i quali, in particolare, la libertà di circolazione (art. 16 Cost.). In tal senso depone anche la norma nazionale che ha autorizzato il tracciamento digitale dei contatti attraverso il Sistema di allerta Covid-19 stabilendo che le persone non possono essere obbligate a installare l'*app* Immuni e che la mancata installazione non può comportare alcuna conseguenza pregiudizievole per gli interessati.

L'Autorità ha ribadito che le *app* devono trattare solamente i dati strettamente necessari a perseguire le finalità del trattamento, evitando di raccogliere dati eccedenti (ad es., quelli relativi all'ubicazione del dispositivo mobile dell'utente) e limitandosi a richiedere permessi per l'accesso a funzionalità o informazioni presenti nel dispositivo solo se indispensabili. Infine, è stato ribadito che amministrazioni pubbliche, regioni e strutture sanitarie dovranno valutare i rischi che potrebbero derivare dall'eventuale trasferimento di dati a terze parti (ad es., mediante *social login*, notifiche *push*, ecc.), soprattutto se stabilite al di fuori dell'UE (cfr. FAQ - *app* nazionale di *contact tracing* e *app* regionali per Covid-19).

5.7. *Modalità semplificate per la consegna dei referti dei test per la ricerca del Covid-19*

L'emergenza sanitaria ha portato le strutture sanitarie pubbliche e private a implementare sistemi di refertazione *online* sia con riferimento ai test per il Covid-19 che per le altre prestazioni sanitarie. Tale esigenza discende soprattutto dalla necessità di evitare assembramenti nei luoghi deputati al ritiro dei referti e di assicurare che il referto per il Covid-19 sia reso noto all'interessato nel più breve tempo possibile, affinché possano essere prestate le necessarie cure e adottate tempestivamente le necessarie misure di contenimento.

Oltre alle modalità previste a livello nazionale per favorire una rapida consultazione dei referti Covid-19, tra cui la richiamata Piattaforma nazionale (cfr. par. 5.6), l'Ufficio è stato coinvolto da alcune regioni sul tema dell'individuazione di modalità semplificate di accesso ai referti durante il periodo emergenziale nonché da alcune strutture sanitarie pubbliche sull'attuazione delle garanzie previste dalla disciplina sulla refertazione *online* nel contesto pandemico (d.P.C.M. 8 agosto 2020).

Una significativa attività di collaborazione istituzionale è stata svolta con la Regione Lombardia in merito all'individuazione di una nuova modalità di consultazione dei referti dei tamponi naso faringei per la rilevazione del Sars-CoV-2 per quanti non siano ancora in possesso di credenziali o dispositivi di autenticazione per accedere al Fse. Con specifico riferimento all'emergenza sanitaria in atto e in considerazione dell'aumento delle richieste dei tamponi, è reso indispensabile incentivare la consultazione dell'esito dei tamponi da remoto, evitando che i singoli si recassero fisicamente a ritirare la copia cartacea, con i connessi rischi di diffusione del virus, alleggerendo contestualmente l'attività dei dipartimenti di prevenzione che non avrebbero dovuto più dedicare personale alla trasmissione del referto con altre modalità (ad es. via e-*mail*). In considerazione di tali esigenze e della specifica disciplina emergenziale vigente, è stato considerato compatibile con la disciplina in materia di protezione dei dati personali un servizio telematico regionale che prevede, previo consenso informato dell'interessato, successivamente revocabile, l'accesso a una specifica sezione del proprio Fse dove prendere visione unicamente del referto relativo all'ultimo tampone effettuato per la rilevazione del Covid-19, ivi disponibile per un tempo limitato (15 giorni).

Sono state avviate attività istruttorie a seguito di reclami e segnalazioni in ordine a quanto riportato dalla stampa circa le modalità attraverso le quali alcuni portali regionali garantivano la corretta identificazione dell'utente nelle operazioni di accesso ai referti Covid-19.

L'Ufficio ha istruito numerose segnalazioni e reclami aventi ad oggetto il mancato rispetto della disciplina vigente in materia di protezione dei dati personali con riferimento alle modalità, sia cartacee che digitali, di consegna dei referti per Covid-19. Alcune segnalazioni hanno riguardato anche le modalità di effettuazione dei test, talvolta risultate poco rispettose delle disposizioni a tutela della confidenzialità del rapporto medico-paziente e della dignità dei soggetti che si sottopongono a tali test. In alcuni dei casi oggetto di istruttoria sono stati avviati specifici procedimenti sanzionatori.

5.8. *Il trattamento dei dati personali da parte delle strutture sanitarie nell'ambito della gestione dell'emergenza sanitaria*

Sono pervenuti al Garante numerosi reclami e segnalazioni in merito al trattamento dei dati personali effettuati da parte delle strutture sanitarie nell'ambito della

gestione dell'emergenza sanitaria (circa 150).

Talora le segnalazioni hanno riguardato le modalità con le quali le strutture sanitarie hanno trasmesso ai pazienti affetti da Covid-19 o posti in isolamento fiduciario informazioni relative alla loro condizione (regole di isolamento, profilassi, ecc.). In molti dei casi segnalati tali comunicazioni sono avvenute attraverso l'invio di *e-mail* a tutti i destinatari inseriti in chiaro nel campo relativo ai destinatari, circostanza che ha consentito, di fatto, senza giustificato motivo e in assenza di qualsivoglia presupposto normativo, a ciascuno di questi di prendere conoscenza dell'indirizzo di posta elettronica degli altri soggetti affetti da Covid-19 o sottoposti alla medesima misura di limitazione del contagio. Al riguardo, l'Ufficio ha evidenziato che la finalità di fornire, in tempi rapidi, ai pazienti affetti da coronavirus o ai soggetti sottoposti ad isolamento domiciliare indicazioni relative alla loro condizione poteva essere utilmente perseguita, senza pregiudizio per la riservatezza degli interessati, inserendo l'indirizzo di posta elettronica dei destinatari dell'*e-mail* nel campo denominato "copia conoscenza nascosta".

Numerose istruttorie hanno riguardato anche il trattamento dei dati effettuato nell'ambito delle attività di sorveglianza sanitaria svolte dai dipartimenti di prevenzione delle aziende sanitarie. Le disposizioni d'urgenza adottate nel corso dell'ultimo anno prevedono interventi emergenziali che implicano il trattamento dei dati e che sono frutto di un delicato bilanciamento tra le esigenze di sanità pubblica e quelle relative alla protezione dei dati personali, in conformità a quanto dettato dal Regolamento per il perseguimento di motivi di interesse pubblico nei settori della sanità pubblica (cfr. art. 9, par. 1, lett. *i*). Tali disposizioni prevedono, allo stato, che l'operatore di sanità pubblica, al fine di determinare le misure di contenimento di contagio più opportune, sia chiamato a ricostruire la filiera dei contatti stretti del soggetto risultato positivo al Covid-19 (art. 3, comma 6, d.P.C.M. 8 marzo 2020, circolare del Ministero della salute 22 febbraio 2020, n. 5443 e successive modificazioni e integrazioni). L'Ufficio, nel rinvenire alcune modalità di sorveglianza poco rispettose della disciplina sulla protezione dei dati, con riferimento alle quali sono stati avviati anche procedimenti sanzionatori, ha rappresentato che risultano invece legittime le richieste da parte dell'operatore sanitario di conoscere l'identità delle persone con cui il soggetto positivo ha avuto un contatto stretto, in quanto informazioni indispensabili alla ricostruzione della filiera dei contatti.

Numerosi i reclami relativi alla ricezione, da parte di pazienti, di referti Covid-19 (tamponi e test) riferiti ad altri soggetti, ovvero, da parte di istituzioni, di elenchi dei soggetti positivi, al di fuori dei casi previsti dalla legge. L'Ufficio, pur tenendo in considerazione lo stato di emergenza legato all'epidemia da Covid-19 (con il relativo sovraccarico di lavoro e le difficoltà operative affrontate dalle strutture sanitarie), ha avviato distinte attività istruttorie che, in alcuni casi, hanno portato all'avvio di procedimenti sanzionatori.

Persone in stato di detenzione

Nell'ambito delle istruttorie avviate, si segnalano, in particolare, i chiarimenti forniti alla Presidenza del Consiglio dei ministri in ordine alla possibilità che i Dipartimenti dell'amministrazione penitenziaria (Dap) possano accedere direttamente alle banche dati relative a persone positive al Covid-19, ovvero in situazione di quarantena, in vista dell'eventuale riattivazione dei colloqui visivi dei detenuti con i propri congiunti. Al riguardo, l'Ufficio ha evidenziato che, nel contemperamento tra la tutela dei diritti degli interessati e la tutela della salute del detenuto, va tenuta in considerazione l'assenza di una mappatura dell'intera popolazione in merito al contagio da Covid-19. Pertanto gli istituti penitenziari, coerentemente a quanto raccomandato dall'Iss, fino al perdurare dell'emergenza in corso, devono adottare le misure di protezione individuale disposte dal Governo per i detenuti (es. dispositivi

personali) che, con riferimento ai colloqui, consistono nell'adozione di misure di protezione individuale in occasione di ogni visita, atteso che lo stato di positività al coronavirus del visitatore potrebbe non essere stata (ancora) accertata. Il contenimento del contagio e la protezione dei detenuti non risultano essere assicurati infatti dalla conoscenza dell'eventuale stato di salute dei soggetti che intendono effettuare i previsti colloqui con gli stessi ma, come ribadito dalle disposizioni vigenti, dal regolare uso di adeguati dispositivi di protezione individuale. A tali considerazioni si aggiungono quelle relative al costante e difficile aggiornamento degli elenchi, in continua implementazione da parte delle diverse e numerose strutture sanitarie presenti sul territorio nazionale.

Pertanto, attese le peculiarità del contesto carcerario e le particolari esigenze di prevenzione che lo caratterizzano, si è ritenuto che la finalità sottesa alla richiesta delle informazioni possa essere utilmente perseguita dal Dap attraverso una diversa procedura, maggiormente rispettosa dei richiamati principi in materia di protezione dei dati personali. In particolare, la Direzione degli istituti penitenziari potrebbe avanzare una richiesta alla competente prefettura (quale ente avente accesso alle banche dati relative ai soggetti positivi al Covid-19 o sottoposti a isolamento domiciliare) affinché svolga un'interrogazione puntuale sulla condizione dei soggetti ammessi a colloquio con detenuti. La comunicazione dei soli risultati della interrogazione puntuale consentirebbe al Dap di soddisfare le menzionate esigenze informative, limitando la conoscenza ai dati che sono effettivamente necessari allo svolgimento delle proprie funzioni ai sensi dell'art. 5, par. 1, lett. *c*), del RGPD, senza determinare un accesso indiscriminato e generalizzato a tutte le informazioni in possesso delle prefetture.

Unep

Di contenuto sostanzialmente analogo sono stati i chiarimenti forniti al Ministero della giustizia in ordine alla possibilità che gli Uffici notifiche, esecuzioni e protesti (Unep) possano accedere agli elenchi aggiornati delle persone risultate positive o di quelle poste in isolamento al fine di gestire lo svolgimento delle attività giurisdizionali anche alla luce di alcune circolari ministeriali che sono state adottate sul tema (nota 9 giugno 2020, doc. web n. 9429175).

5.9. *Procedura IMI su "Covid: registro viaggiatori"*

È pervenuta una richiesta di assistenza reciproca, ai sensi dell'art. 61 del RGPD, volta conoscere se esistono negli altri Stati membri procedure specifiche per i viaggiatori finalizzate a contrastare il diffondersi della pandemia da Covid-19.

In particolare, l'Autorità lettone era interessata a conoscere la base giuridica e le finalità di tali trattamenti, le autorità che trattano tali informazioni, il tipo di elaborazioni consentite e se vi siano questionari da compilare e da presentare alle autorità sanitarie da parte dei turisti italiani che rientrano nel nostro Paese.

Nella risposta fornita si è svolta una sintetica ricostruzione normativa, evidenziando le disposizioni maggiormente rilevanti, in particolare quelle contenute nei d.P.C.M, 7 agosto e 7 settembre 2020, e si è portato all'attenzione dell'Autorità lettone il *link* alla pagina web del Ministero della salute che riassume le regole Covid-19 per i viaggiatori. Infine l'Ufficio ha dato riscontro alle specifiche domande sottoposte dalla Autorità lettone alle altre autorità in merito alla base giuridica e alle finalità del trattamento.

5.10. *Il trattamento di dati personali per scopi di ricerca scientifica nell'ambito dell'emergenza da Covid-19*

A seguito di specifici quesiti relativi al trattamento dei dati personali per scopi di ricerca scientifica nell'ambito dell'emergenza da Covid-19, l'Autorità, attraverso lo strumento delle FAQ, ha chiarito alcuni profili di seguito riportati.

Il presupposto giuridico per trattare dati personali, anche relativi alla salute dei pazienti affetti da Covid-19, per lo svolgimento di sperimentazioni cliniche dei medicinali (quali ad es., gli studi clinici sperimentali sui medicinali di fase I, II, III e IV, gli studi osservazionali sui farmaci e i programmi di uso terapeutico compassionevole), strettamente necessari per contrastare e studiare la pandemia in corso è il consenso degli interessati, ovvero altro presupposto giuridico ai sensi dell'art. 9, par. 2, del RGPD, in conformità al diritto dell'Unione o nazionale per motivi di interesse pubblico rilevante, per motivi di interesse pubblico nel settore della sanità pubblica e per fini di ricerca scientifica (art. 9, par. 2, lett. *a*), *g*), *i*) e *j*), del RGPD).

Qualora non sia possibile acquisire il consenso direttamente dagli interessati, i titolari del trattamento sono tenuti, laddove possibile, a raccogliere tale consenso, previa idonea informativa, da chi esercita legalmente la potestà di questi ultimi, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato (in analogia con quanto previsto dal punto 4.11.2 delle prescrizioni relative al trattamento dei dati genetici, all. 4 al provv. 5 giugno 2019, n. 146, recante le prescrizioni relative al trattamento di categorie particolari di dati, doc. web n. 9124510).

Qualora, per specifiche e comprovate ragioni, non sia possibile acquisire il consenso informato al trattamento dei dati personali neanche presso terzi, ovvero ciò rischi di pregiudicare gravemente il buon esito della ricerca (si pensi al trattamento di dati riferiti a pazienti defunti o ricoverati in reparti di terapia intensiva), i titolari che intendano svolgere trattamenti di dati personali che riguardano esclusivamente studi sperimentali e gli usi compassionevoli dei medicinali per uso umano, per la cura e la prevenzione del virus Covid-19, non sono obbligati, in forza della normativa relativa alla fase emergenziale, alla preventiva sottoposizione del progetto di ricerca nonché della relativa valutazione di impatto alla consultazione preventiva del Garante di cui all'art. 110 del Codice (v. altresì art. 14, d.l. 9 marzo 2020, n. 14 e art. 17, d.l. 17 marzo 2020 n. 18).

Con specifico riguardo alle ricerche mediche relative al Covid-19 finanziate dal Ministero della salute sulla base del bando adottato il 1° aprile 2020 per invitare gli Istituti di ricovero e cura a carattere scientifico (Ircss) a presentare progetti di ricerca medica finalizzati a migliorare la comprensione dell'epidemia Covid-19, il Garante ha chiarito che i trattamenti di dati personali anche relativi alla salute svolti dagli Ircss beneficiari dei finanziamenti nell'ambito delle ricerche finalizzate al contrasto della pandemia possono essere effettuati senza il consenso degli interessati in quanto ineriscono alle funzioni di rilevante interesse pubblico attribuite anche ai soggetti del Ssn. I predetti Ircss che trattano dati personali nell'ambito delle ricerche mediche finanziate dal Ministero non devono, pertanto, porre in essere gli adempimenti previsti dall'art. 110 del Codice.

L'Ufficio ha altresì collaborato con Aifa nella predisposizione del comunicato stampa sulla gestione degli studi clinici in Italia in corso di emergenza da Covid-19. In particolare, sono state fornite specifiche indicazioni in materia di protezione dei dati personali nell'ambito della gestione da remoto della fase di monitoraggio delle sperimentazioni cliniche dei farmaci.

5.11. *Sanità digitale*

5.11.1. Il Fascicolo sanitario elettronico

La disciplina relativa al Fse è stata significativamente innovata attraverso la soppressione del comma 3-*bis* dell'art. 12, d.l. n. 179/2012 (cd. consenso all'alimentazione) ad opera del d.l. Rilancio. Tale modifica ha determinato la costituzione e l'alimentazione automatica del Fse, a prescindere dal consenso dell'interessato/assistito. Il consenso di quest'ultimo è invece ancora necessario per la consultazione del Fse per finalità di cura (cd. consenso alla consultazione). Il Fse è, pertanto, alimentato in maniera continuativa e tempestiva dagli esercenti le professioni sanitarie che prendono in cura l'assistito, operanti ora anche al di fuori del Ssn, nonché su iniziativa dello stesso interessato, arricchendo con i dati a sua disposizione la partizione del Fse denominata "Taccuino personale".

A seguito della recente modifica normativa, è stata esaminata la problematica relativa alla possibilità di rendere accessibili tramite il Fse anche i dati derivanti dagli eventi clinici occorsi all'assistito prima della data di entrata in vigore del d.l. Rilancio, a prescindere dalla circostanza che lo stesso interessato avesse prestato, prima di tale data, il consenso all'alimentazione del Fse all'epoca vigente.

Il Garante ha preso atto che la nuova formulazione dell'art. 12 evidenzia la volontà del legislatore di mettere a disposizione di ognuno un Fse completo con riferimento ai dati relativi agli eventi clinici e ha mantenuto il regime di accessibilità allo stesso precedentemente previsto, subordinato cioè al consenso dell'interessato. L'alimentazione automatica dei fascicoli sanitari prevista dalla novella legislativa non amplia significativamente il perimetro dei dati generati da strutture sanitarie facenti parte del Ssn, già disponibili agli organi di governo (Regioni e Ministero della salute) attraverso i cd. flussi amministrativi e utilizzati per finalità di controllo della qualità, informazione sulla gestione e supervisione generale (a livello nazionale e locale) del sistema di assistenza sanitaria. Alla luce di ciò il Garante ha ritenuto che il Fse possa essere alimentato anche con i dati e i documenti relativi alle prestazioni sanitare erogate dal Ssn antecedentemente alla data di entrata in vigore del d.l. Rilancio, senza necessità, al riguardo, di un'espressa manifestazione di volontà da parte dell'interessato. Ciò, però, qualora ricorrano le seguenti condizioni:

- sia effettuata un'adeguata campagna informativa a livello nazionale e regionale volta a rendere edotti gli interessati in merito alle caratteristiche del trattamento effettuato attraverso il Fse, con particolare riferimento alle novità introdotte dal d.l. Rilancio;
- sia comunque garantito all'interessato di poter esercitare il diritto di opporsi all'alimentazione del Fse con i dati sanitari generati da eventi clinici occorsi antecedentemente al 19 maggio 2020, entro un termine prestabilito, non inferiore a 30 giorni.

Per quanto riguarda invece i dati relativi alle prestazioni sanitarie erogate al di fuori del Ssn (che fino al 19 maggio non alimentavano il Fse), si è ritenuto che, alla luce delle disposizioni vigenti, questi possano essere inseriti nel Fse solo se relativi a prestazioni sanitarie erogate successivamente alla data di entrata in vigore del d.l. Rilancio. Come detto, resta ferma la possibilità per l'interessato di rendere disponibili le informazioni relative alle prestazioni sanitarie eventualmente ricevute dalle strutture sanitarie private prima del 19 maggio 2020 attraverso il "Taccuino personale" (cfr. nota 15 dicembre 2020).

In merito alle tematiche relative all'implementazione del Fse a livello nazionale, l'Ufficio ha continuato a partecipare al tavolo tecnico di monitoraggio e indirizzo per l'attuazione delle disposizioni in materia di Fse istituito presso il Ministero della

salute, fornendo chiarimenti sugli aspetti relativi al trattamento dei dati personali effettuati attraverso il Fse. In particolare, sono state fornite indicazioni in merito alle condizioni per l'accesso ai dati del fascicolo in condizioni di emergenza, alla definizione dei contenuti dei documenti consultabili attraverso il Fse, alla tipologia di informazioni da rendere agli interessati e al trattamento dei dati cd. a maggior tutela, quali le informazioni legate all'interruzione di gravidanza o all'Hiv (note 6 ottobre e 15 dicembre 2020).

Sono state avviate numerose istruttorie concernenti, principalmente, l'erronea attribuzione di referti e documenti sanitari in Fse di soggetti diversi dall'interessato e l'accesso al Fascicolo da parte di personale che, seppur autorizzato, non era coinvolto nel processo di cura dell'interessato.

Sempre in tema di Fse si segnala che, con provvedimento del 9 luglio 2020, n. 141 (doc. web n. 9440117), il Garante ha adottato un provvedimento di ammonimento nei confronti di un policlinico che aveva notificato una violazione dei dati personali in quanto, a seguito dell'errata identificazione di un paziente al pronto soccorso, aveva reso disponibile un referto sul Fse di una persona diversa dall'interessato. All'esito dell'istruttoria, il Garante ha ritenuto illecito il trattamento di dati personali effettuato dal policlinico, in quanto l'avvenuto inserimento all'interno di un Fse del referto di un paziente diverso dall'interessato ha determinato la violazione delle disposizioni riguardanti la comunicazione a terzi di dati personali relativi alla salute dell'interessato (art. 9 del RGPD e artt. 83 e 84 del Codice in combinato disposto con l'art. 22, comma 11, d.lgs. n. 101/2018) e, di conseguenza, dei principi di integrità e riservatezza del trattamento (art. 5, par. 1, lett. *f*), del RGPD). L'Autorità ha qualificato il caso come violazione minore, ai sensi del cons. 148 del RGPD, considerata la natura isolata della vicenda riconducibile ad un errore umano nonché in ragione della notificazione della violazione all'Autorità da parte del titolare del trattamento (che ha altresì informato dell'accaduto l'interessato e ha adottato molteplici atti organizzativi e iniziative formative volte a sensibilizzare le persone autorizzate al trattamento al rispetto della disciplina in materia di protezione dati personali e delle procedure adottate in tema di corretta identificazione dei pazienti).

In un altro caso, il Garante ha sanzionato un'azienda sanitaria per avere erroneamente inserito in 182 Fse (di cui solo 49 attivi) le lettere di dimissione ospedaliera di numerosi soggetti e per avere, quindi, reso possibile in 14 casi che l'intestatario del Fse avesse accesso allo stesso nel breve periodo in cui erano presenti i predetti documenti (provv. 14 gennaio 2021, n. 11, doc. web n. 9542155). Secondo quanto rilevato, la fattispecie sopra descritta, oggetto di notifica di violazione da parte del titolare, ha determinato una comunicazione di dati relativi alla salute a terzi in assenza di un idoneo presupposto giuridico e, quindi, in violazione dei principi di base del trattamento di cui agli artt. 5 e 9 del RGPD.

5.11.2. Il dossier *sanitario*

Il Garante ha continuato a ricevere numerose segnalazioni e reclami con riferimento a presunte violazioni della disciplina in materia di protezione dei dati personali nell'ambito dei trattamenti effettuati attraverso i *dossier* sanitari aziendali.

Le istruttorie, in fase di definizione, hanno riguardato in particolar modo l'accesso a *dossier* sanitari da parte di soggetti che, seppure autorizzati, non erano coinvolti nel processo di cura dell'interessato. Altri casi hanno riguardato il mancato oscuramento di alcuni dati e documenti a seguito di specifiche istanze presentate dagli interessati o, ancora, la presenza, nei *dossier* sanitari, di dati relativi alla salute di terzi.

In un caso, al termine del procedimento istruttorio avviato a seguito di tre notifiche di violazione, l'Autorità ha adottato un provvedimento correttivo e sanzionato-

rio nei confronti di una azienda ospedaliera per non aver adottato le misure tecniche e organizzative necessarie a tutelare i dati personali trattati attraverso il *dossier* sanitario aziendale (provv. 23 gennaio 2020, n. 18, doc. web n. 9269629).

Il Garante ha infatti accertato che si erano verificati 16 accessi al *dossier* sanitario aziendale da parte del personale medico per ragioni personali, descritte dall'azienda come "mera curiosità". È stato in particolare evidenziato che le misure adottate dall'azienda, con riferimento ai trattamenti effettuati attraverso il *dossier* sanitario aziendale, non hanno permesso di evitare la possibilità che il personale sanitario abilitato accedesse alla documentazione clinica di pazienti non in cura, determinando un trattamento illecito dei dati personali riguardanti gli interessati.

Il Garante ha poi rilevato che l'azienda aveva implementato le misure volte a limitare l'accesso al *dossier* sanitario dei pazienti a vantaggio del solo personale sanitario che li aveva in cura soltanto dopo aver accertato gli episodi oggetto delle menzionate comunicazioni, individuando soluzioni logico-informatiche ispirate alle indicazioni già fornite dal Garante nelle linee guida del 2015 (doc. web n. 4091542) e ribadite nei provvedimenti adottati dall'Autorità in materia sin dal 2013. L'adozione preventiva di tali misure, anche alla luce dei principi di protezione dei dati fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*) contemplati all'art. 25 del RGPD, avrebbe potuto impedire (o limitare) gli accessi non autorizzati ai *dossier* sanitari aziendali oggetto delle citate notifiche di violazioni effettuate dall'azienda.

5.11.3. App *in ospedale*

A seguito di notizie stampa, sono state avviate alcune istruttorie nei confronti di strutture ospedaliere in merito all'implementazione di applicazioni idonee a consentire ai pazienti che hanno effettuato un accesso al pronto soccorso e ai loro accompagnatori di monitorare l'*iter* diagnostico intrapreso. Tali iniziative si collocano all'interno di un percorso volto a ottimizzare le procedure di comunicazione tra gli operatori sanitari e gli accompagnatori del paziente attraverso l'introduzione di sistemi più avanzati di interazione. Tali progetti, condivisibili e meritori, possono essere realizzati nel pieno rispetto della disciplina in materia di protezione dei dati personali con l'adozione di adeguate cautele a salvaguardia dei diritti e delle libertà fondamentali degli interessati. A tal fine, è necessario che il titolare provveda a esaminare preventivamente i rischi per i diritti e le libertà degli interessati, individuando misure idonee ad offrire ai pazienti e ai loro accompagnatori soluzioni efficienti, realizzate con modalità che tutelino in modo efficace i dati che li riguardano, tenendo in particolare considerazione che, attraverso tali strumenti, possono essere trattate informazioni sulla salute anche di un numero considerevole di pazienti in pronto soccorso. Tuttavia, si dovrebbe evitare, come accaduto presso taluni presidi ospedalieri, l'utilizzabilità di tali *app* qualora l'interessato si avvalga dei servizi ospedalieri per particolari eventi o patologie (si pensi alle vittime di violenza domestica).

Nell'ambito di tali attività istruttorie, alcune delle quali sono ancora in fase di definizione, l'Ufficio ha evidenziato che 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 gestiscano e forniscano informazioni agli accompagnatori dei pazienti attraverso 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".

Le informazioni trattate attraverso tali applicativi si qualificano, senza ombra di dubbio, come informazioni sulla salute degli interessati, in quanto indicano la prestazione di un particolare servizio di assistenza sanitaria, ovvero di pronto soccorso, rivelando informazioni relative allo stato di salute dell'interessato attraverso l'indicazione della presenza dello stesso in specifici ambulatori dell'ospedale o nell'Osservazione breve intensiva (Obi), nonché del codice *triage* assegnatogli (art. 4, n. 15) e cons. 35 del RGPD).

In sede istruttoria l'Ufficio ha ritenuto che le fattispecie esaminate rientrassero tra quelle per le quali il titolare è tenuto ad effettuare una preventiva valutazione di impatto (art. 35 del RGPD), attesa la ricorrenza dei criteri indicati dal Comitato: formano oggetto di trattamento dati sulla salute, sono interessati soggetti vulnerabili (pazienti di un pronto soccorso) e si prevede l'uso innovativo o l'applicazione di nuove soluzioni tecnologiche od organizzative (cfr. linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 adottate il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 -WP 248 rev.01, III, lett. B, punti 4, 7 e 8).

Una delle attività istruttorie si è conclusa con l'adozione di un provvedimento sanzionatorio nei confronti di una Asl in quanto il trattamento dei dati, effettuato attraverso un'*app* destinata ai pazienti del pronto soccorso, era stato posto in essere in assenza della valutazione di impatto (provv. 12 marzo 2020, n. 49, doc. web n. 9310804). In particolare, la valutazione di impatto trasmessa dall'azienda era stata effettuata solo in tempi successivi rispetto alla richiesta di informazioni dell'Autorità e comunque non rispondeva ai principi e alle caratteristiche richiesti dal RGPD (artt. 5 e 35), in quanto priva di numerosi elementi richiesti dall'art. 35, par. 7, del RGPD.

In un altro caso esaminato dall'Ufficio si è rilevato positivamente che, nella valutazione di impatto effettuata, si era tenuto conto delle diverse tipologie di accessi al pronto soccorso, escludendone esplicitamente alcune dal servizio (ad es., gravità delle condizioni cliniche o possibilità che queste siano derivate da episodi di violenza) e si era scelto di non indicare nel dettaglio la tipologia di visita specialistica effettuata in pronto soccorso (cfr. *Newsletter* 6 aprile 2020, n. 464, doc. web n. 9307234).

5.12. *Stratificazione della popolazione per rischio sanitario*

5.12.1. Iniziative di livello nazionale

Particolare rilievo assume il parere reso dal Garante al Consiglio di Stato in merito alle nuove modalità di ripartizione del Fondo sanitario nazionale (Fsn) tra le regioni proposte dal Ministero della salute e basate sulla stratificazione della popolazione (parere 5 marzo 2020, n. 43, doc. web n. 9304455).

In tale parere, l'Autorità, nel riconoscere l'importanza di una ripartizione più equa del Fsn, basata su un'effettiva definizione dei diversi fabbisogni regionali, ha richiamato l'attenzione sulla necessità che i trattamenti di dati personali connessi a tale nuovo sistema di determinazione del Fsn siano previsti, sulla base di quanto richiesto dal Regolamento, da una specifica disposizione di legge. L'articolata attività di raccolta di categorie particolari di dati e l'interconnessione degli stessi anche con informazioni di carattere reddituale, volta alla creazione di un *database* di livello individuale quale base informativa per procedere alla cd. stratificazione di tutti gli utenti del Ssn da un punto di vista clinico e sociale, comporterebbe infatti un'analisi dei dati relativi alla salute dell'intera popolazione italiana, da condurre periodica-

5

mente, all'esito della quale verrebbero prese decisioni i cui effetti si riverberano su tutti gli assistiti.

Secondo il Garante, l'utilizzo di dati dell'intera popolazione, ancorché in una non compiutamente descritta forma pseudonimizzata, ai fini della determinazione dei predetti pesi, dovrebbe essere, in ogni caso, suffragata da una compiuta analisi circa i rischi che ne potrebbero derivare per i diritti e le libertà fondamentali degli interessati, alla luce dei principi di responsabilizzazione e di protezione dei dati personali fin dalla progettazione, nonché dall'obbligo di condurre una valutazione di impatto per i trattamenti (artt. 5, par. 2; 25, 35 e 36, par. 4, del RGPD) da effettuarsi anche in via generale nel contesto dell'adozione della base giuridica del trattamento prospettato (cfr. art. 36, par. 10, del RGPD).

In tale parere il Garante ha poi ricordato che la necessità di un'adeguata base giuridica che preveda in capo al Ministero la possibilità di procedere alla cd. attività di stratificazione della popolazione per il raggiungimento di specifiche finalità istituzionali, assume ancor maggior rilievo in considerazione dell'intenzione, manifestata dallo stesso Dicastero, di utilizzare tale sistema di profilazione della popolazione anche per il raggiungimento di finalità ulteriori rispetto a quella in esame: in particolare, quella relativa alla creazione di modelli legati alla cd. medicina predittiva o di iniziativa.

A tale riguardo, l'Autorità ha avviato confronti istituzionali con alcune regioni interessate a intraprendere iniziative legate alla cd. medicina predittiva o di iniziativa, fondate su un'attività di stratificazione della popolazione residente, sostanzialmente analoga a quella proposta dal Ministero della salute.

L'Autorità ha pertanto ritenuto che, all'atto della richiesta di parere, non fosse possibile rinvenire una base giuridica anche per la cd. attività di stratificazione di tutti gli utenti del Ssn, volta a definire un profilo sanitario individuale legato alla presenza di patologie croniche e connesso a un profilo reddituale individuale (*status* sociale). Più puntualmente, il Garante ha rilevato che, con la proposta sottoposta al parere del Consiglio di Stato, il Ministero della salute intenderebbe procedere ad una ripartizione del Fsn ancorata ai criteri di cui all'art. 1, comma 34, l. n. 662/1996, attraverso una modalità nuova, che prevede l'uso di dati personali individuali e la stratificazione degli utenti del Ssn, che non risulta però disciplinata dalla richiamata legge n. 662/1996 e dal rinnovato sistema per la determinazione dei costi e dei fabbisogni standard per le regioni (nel settore sanitario previsto, a partire dal 2013, dal decreto legislativo n. 68/2011), né da specifiche disposizioni normative, come invece richiesto dalla disciplina sulla protezione dei dati personali.

Successivamente all'adozione del parere, il legislatore ha introdotto la possibilità per il Ministero della salute, nell'ambito delle funzioni relative a indirizzi generali e di coordinamento in materia di prevenzione, diagnosi, cura e riabilitazione delle malattie, nonché di programmazione tecnico sanitaria di rilievo nazionale e indirizzo, coordinamento, monitoraggio dell'attività tecnico sanitaria regionale, di trattare dati personali, anche relativi alla salute degli assistiti, raccolti nei sistemi informativi del Ssn, per lo sviluppo di metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione (art. 7, d.l. n. 34/2020).

Con regolamento adottato con decreto del Ministro della salute, previo parere del Garante, saranno individuati i dati personali che possono essere trattati a tal fine, le operazioni eseguibili, le modalità di acquisizione dei dati dai sistemi informativi dei soggetti che li detengono e le misure appropriate e specifiche per tutelare i diritti degli interessati, nonché i tempi di conservazione dei dati trattati. In questa prospettiva è stato istituito un tavolo interistituzionale presso il Ministero della salute ai cui lavori partecipa anche l'Autorità.

5.12.2. Iniziative di livello regionale nell'ambito della cd. medicina di iniziativa

Come accennato, l'Ufficio ha continuato ad affrontare la tematica del rispetto della disciplina in materia di protezione dei dati personali nell'ambito della cd. medicina di iniziativa, vale a dire di 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 proprio percorso di cura (cfr., tra i molti richiami, Ministero della salute, Assemblea generale del Consiglio Superiore di Sanità, "Telemedicina – linee guida nazionali", 10 luglio 2012, cfr. par. 2.3.2, decreto 2 aprile 2015, n. 70).

Al riguardo il Garante, nell'ambito di un parere reso alla Provincia autonoma di Trento sul disegno di legge provinciale concernente ulteriori misure di sostegno per le famiglie, i lavoratori e i settori economici connesse all'emergenza epidemiologica da Covid-19 e conseguente variazione al bilancio di previsione della Provincia autonoma di Trento per gli esercizi finanziari 2020-2022, ha fornito indicazioni in merito alla base giuridica dei trattamenti di dati personali effettuati nell'ambito della medicina di iniziativa (pareri 8 maggio 2020, n. 84, doc. web n. 9344635 e 1° ottobre 2020, n. 275, doc. web n. 9469372). In particolare, l'Autorità ha evidenziato che, al fine di realizzare tale modello assistenziale, la disposizione in parola avrebbe previsto che l'Azienda provinciale per i servizi sanitari potesse operare la stratificazione del rischio degli assistiti e degli assistibili attraverso l'analisi statistica, l'interconnessione, l'elaborazione dei dati gestiti nell'ambito dei diversi archivi del servizio informativo sanitario provinciale e dell'Azienda stessa, ivi inclusi i dati forniti dai soggetti accreditati o convenzionati con il servizio sanitario provinciale. La disposizione, secondo l'Autorità, presentava non poche criticità in quanto perseguiva una pluralità di finalità (statistiche, di cura e amministrative) che si fondano su diversi presupposti di liceità, che la disposizione, così come formulata, non consente di rispettare. Ciò in violazione dei principi di liceità, correttezza, limitazione della finalità, minimizzazione e sicurezza dei dati, in quanto si accomunano, senza le necessarie distinzioni, trattamenti effettuati per scopi statistici, finalità amministrative e di cura.

Il Garante ha poi evidenziato che l'attività di stratificazione pone elementi di riflessione sia di tipo giuridico che etico. Il modello assistenziale proposto dalla disposizione comporta infatti una profilazione dell'utente del servizio sanitario provinciale, in quanto consiste in un trattamento automatizzato di dati personali volto a valutarne determinati aspetti sanitari, sulla base dei dati registrati nei diversi archivi del servizio informativo provinciale, in particolare per analizzarne e prevederne la situazione sanitaria, con specifico riferimento alle patologie croniche. Sul punto, il Regolamento prevede requisiti specifici e garanzie adeguate per i diritti degli interessati, specie ove si faccia ricorso alla profilazione per adottare decisioni che incidano su singoli individui (cfr. artt. 13, par. 1, lett. *f*); 14, par. 2, lett. *g*), 15, par. 1, lett. *h*), 21, par. 1 e 35, par. 3, lett. *a*), del RGPD).

Sono stati evidenziati gli specifici vincoli, in termini di protezione dei dati e trasparenza, che dovrebbero essere rispettati nel caso in cui tale attività di profilazione fosse realizzata attraverso l'uso di algoritmi. Al riguardo, l'Autorità ha richiamato la sentenza del Consiglio di Stato (sez. VI, 13 dicembre 2019, n. 8472) secondo la quale "dal diritto sovranazionale emergono tre principi, da tenere in debita considerazione nell'esame e nell'utilizzo degli strumenti informatici. In primo luogo, il principio di conoscibilità, per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino ed in questo caso a ricevere informazioni significative sulla logica utilizzata […] il principio di non esclusività della decisione algoritmica […]. In terzo luogo, dal cons. 71 del regolamento 679/2016, il diritto europeo trae un ulteriore principio fondamentale, di non discriminazione

algoritmica, secondo cui è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti". Tale attività di stratificazione dovrebbe essere, in ogni caso, suffragata da una compiuta analisi circa i rischi per i diritti e le libertà fondamentali degli interessati che ne potrebbero derivare, alla luce dei principi di responsabilizzazione e di protezione dei dati personali fin dalla progettazione, nonché preceduta da una valutazione di impatto per i trattamenti che presentano rischi significativi per i diritti degli interessati (artt. 5, par. 2; 25 e 35 del RGPD).

L'Autorità ha evidenziato pertanto la necessità di procedere a una revisione delle disposizioni sottoposte al parere, al fine di tenere conto dei principi di liceità, correttezza, limitazione della finalità, minimizzazione e sicurezza, e ha poi ricordato gli specifici vincoli, in termini di protezione dei dati e trasparenza, che devono essere rispettati nel caso in cui la medicina di iniziativa sia basata sulla profilazione degli assistiti attraverso l'uso di un algoritmo. In tale contesto è stato evidenziato che la raccolta e l'elaborazione di dati sanitari al fine di realizzare, con riferimento a specifiche patologie, un profilo sanitario di rischio dell'interessato configura un trattamento autonomo rispetto a quello principale finalizzato alla cura dell'assistito; esso deve essere pertanto effettuato sulla base del consenso dell'interessato, in quanto trattamento automatizzato non strettamente necessario per finalità di cura (artt. 9, par. 2, lett. *h*) e 22 del RGPD).

Tali considerazioni sono state ribadite anche nel parere reso dall'Autorità su uno schema di regolamento relativo alle disposizioni attuative della ricordata legge provinciale per la medicina di iniziativa nel servizio sanitario provinciale trentino (parere 1° ottobre 2020, n. 175, doc. web n. 9469372).

Analoghe considerazioni sono state espresse nei confronti della Regione Friuli Venezia Giulia. In particolare, l'Ufficio, oltre ad evidenziare quanto sopra rappresentato in ordine alla base giuridica del trattamento effettuato attraverso la medicina di iniziativa, ha sollevato profili di criticità in ordine alle tecniche di anonimizzazione dei dati descritte dalla Regione per la realizzazione di una analoga iniziativa, all'individuazione del titolare del trattamento e alle informazioni da rendere agli interessati, con particolare riferimento agli obblighi connessi alla descrizione della logica applicata al trattamento dei dati (artt. 24 e 25, 32, 13 e 14 del RGPD).

Con riguardo ai trattamenti di dati personali effettuati nell'ambito della medicina di iniziativa, l'Autorità ha sanzionato un'azienda sanitaria della Regione Toscana per avere promosso un modello organizzativo-assistenziale al fine di favorire "un approccio metodologico alla presa in carico e al processo di cura del paziente" che si traduceva in un "richiamo attivo e periodico del paziente per sottoporlo ad attività educative e clinico assistenziali, volte alla correzione dei stili di vita, all'*empowerment*, alla diagnosi precoce" (provv. 17 dicembre 2020, n. 278, doc. web n. 9529527). Tale modello è stato promosso con alcune delibere della Regione, ma ciascuna azienda sanitaria lo aveva avviato di propria iniziativa nell'ambito territoriale di competenza. In particolare, è stato contestato all'azienda in questione di non aver istituito il registro delle attività di trattamento previsto dall'art. 30 del RGPD, di non avere effet-

tuato un'adeguata designazione a responsabile del trattamento di un ente esterno alla stessa al quale era stato affidato il compito di procedere a numerosi e complessi trattamenti per conto dell'azienda, ivi compresi quelli relativi alla medicina di iniziativa, di aver individuato modalità attuative di quest'ultima in contrasto con i principi e criteri di sicurezza descritti dagli artt. 5, par. 2, lett. *f*) e 32 del RGPD. Tali modalità di trattamento hanno messo in luce l'assenza di una valutazione dei rischi del trattamento che si sarebbe dovuta effettuare nell'ambito della valutazione di impatto che invece non risulta essere stata condotta. È stato altresì contestato all'azienda sanitaria che il modello di informativa realizzato per le finalità di monitoraggio, valutazione e qualità dell'assistenza erogata attraverso il modello assistenziale della cd. sanità di iniziativa, fornito ai medici di medicina generale affinché ne venissero messi a parte i pazienti all'atto dell'arruolamento, era privo di alcuni degli elementi essenziali previsti dalla disciplina vigente.

5.13. *Codici di condotta in ambito sanitario*

Nel dare seguito ad alcune iniziative volte alla stesura di codici di condotta con riferimento a specifici trattamenti in ambito sanitario, sono state avviate interlocuzioni con organismi rappresentativi che si sono concentrate sul rispetto dei requisiti di ammissibilità dei progetti di codici in fase di redazione indicati, in particolare, nelle linee guida del Cepd sui codici di condotta e sugli organismi di monitoraggio (linee guida 1/2019, adottate il 4 giugno 2019, cfr. par. 5, punti da 19 a 31 e par. 7).

Al riguardo, merita di essere segnalata l'istruttoria relativa alla proposta di codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica (approvato con provv. 14 gennaio 2021, n. 7, doc. web n. 9535354): nel caso in esame, la Regione Veneto e un'azienda sanitaria, a seguito di una analisi della disciplina del Regolamento e delle difficoltà applicative della stessa rispetto allo specifico ambito di trattamento considerato, hanno elaborato la proposta di codice poi sottoposta all'approvazione del Garante.

La fase di approvazione è stata preceduta dall'esame del documento per verificare il pieno soddisfacimento dei requisiti di ammissibilità del progetto di codice, come declinati nelle linee guida del Cepd sui codici di condotta e sugli organismi di monitoraggio. In particolare, i profili che hanno richiesto specifici approfondimenti istruttori hanno riguardato il requisito della rappresentatività, l'entità delle consultazioni svolte e il rispetto della disciplina nazionale e regionale di settore.

Il codice *de quo*, che rappresenta il primo codice di condotta approvato dal Garante in relazione ai trattamenti di dati sulla salute in ambito sanitario, intende disciplinare le modalità attraverso le quali tali dati possono essere utilizzati per fini didattici e di pubblicazione scientifica da parte dei professionisti sanitari. Esso è volto a garantire, settorialmente, in funzione delle specifiche esigenze dei partecipanti, l'applicazione efficace, coerente ed omogenea del Regolamento, individuando un set di regole concrete e un corretto bilanciamento tra ciò che è richiesto dalla disciplina vigente e gli interessi dei soggetti coinvolti nel trattamento. Gli aderenti potranno utilizzarlo per dimostrare la conformità del trattamento alla disciplina sulla protezione dei dati personali, in omaggio al principio di *accountability* di cui i codici di condotta sono espressione.

Nello specifico, il codice prevede che l'utilizzo dei dati personali per fini didattici e di pubblicazione scientifica possa avvenire solo previa adozione di specifiche misure di anonimizzazione e pseudonimizzazione a tutela dei diritti e delle libertà degli interessati, declinate in un allegato *ad hoc*.

Particolarmente significativi, in chiave di tutela degli interessati e di chiarezza del disposto codicistico, gli allegati che recano il modello di richiesta di autorizzazione che il professionista sanitario deve rivolgere al titolare del trattamento per poter utilizzare i dati per scopi didattici e di pubblicazione scientifica (n. 3); il modello di informativa da rendere agli interessati, il quale, oltre a contenere tutti gli elementi previsti dagli artt. 13 e 14 del RGPD, individua chiaramente le finalità e i mezzi del trattamento e lo specifico periodo di conservazione dei dati (n. 4); il modello di consenso (n. 5).

Pur non essendo previsto in ambito pubblico il controllo del codice da parte di organismi in possesso di adeguate competenze e necessariamente accreditati dall'Autorità (art. 41, par. 6, del RGPD), nel codice sono stati individuati specifici meccanismi che consentono di effettuare un efficace controllo sul rispetto dello stesso da parte degli aderenti che si impegnano ad applicarlo (art. 40, par. 2, del RGPD).

5.14. *I trattamenti per finalità di cura e amministrative correlate alla cura: ulteriori istruttorie*

Una Ausl è stata sanzionata per aver effettuato un trattamento di dati personali degli interessati che hanno aderito alla campagna di prevenzione precoce dei tumori in violazione del diritto degli interessati di ricevere, al momento della raccolta dei dati, le informazioni di cui all'art. 13 del RGPD e degli obblighi del titolare in ordine alla corretta designazione del responsabile del trattamento di cui all'art. 28 del RGPD (provv. 6 febbraio 2020, n. 26, doc. web n. 9299150). L'azienda aveva infatti fornito agli interessati informazioni parziali in merito al trattamento dei dati che sarebbe stato effettuato nell'ambito della campagna di *screening* riportando anche finalità che non erano di fatto perseguite; campagna che veniva effettuata per il tramite di un istituto specializzato non designato responsabile del trattamento.

Si è definito un procedimento sanzionatorio a carico di un'azienda sanitaria in relazione ad una segnalazione, avente ad oggetto la messa a disposizione a una società, di copie di immagini acquisite tramite apparecchiatura TAC riferite ad alcuni pazienti; la società le aveva poi rielaborate e prodotte nell'ambito della documentazione necessaria a partecipare ad una gara d'appalto. Era stato riscontrato in proposito un trattamento illecito consistente nella comunicazione, da parte dell'azienda sanitaria, di informazioni sulla salute di alcuni pazienti identificati, in assenza di un'adeguata base normativa (cfr. Relazione 2019, p. 84-85 e *Newsletter* 23 settembre 2019, n. 457). Non è stato infatti accolto l'argomento difensivo consistente nell'asserito errore in cui era incorso l'operatore sanitario, dipendente dell'azienda, che in buona fede aveva consentito la predetta operazione sui dati rilevati dalle apparecchiature TAC, pur non essendo stato a ciò autorizzato dal titolare del trattamento. Sul punto, l'Autorità ha ritenuto che l'azienda avrebbe potuto diligentemente accertare, attraverso il personale preposto, se la società fosse legittimata all'accesso ai dati sanitari rilevati attraverso le apparecchiature mediche evitando di comunicare i dati a soggetti non autorizzati; la circostanza che la società fosse responsabile del trattamento designata dall'azienda sanitaria, non ha rilevato nel caso di specie, in quanto i dati acquisiti erano destinati a trattamenti effettuati per finalità proprie della società, non riconducibili a quelli oggetto della designazione quale responsabile del trattamento (provv. 24 giugno 2020, n. 106, doc. web n. 9444819).

In un'altra occasione, nell'ambito di un reclamo avente ad oggetto una valutazione del contenuto del verbale di pronto soccorso redatto da un'azienda sanitaria e

del documento di richiesta di consulenza da parte del pronto soccorso ad altra unità operativa (contenente riferimenti alla vita e al comportamento sessuale dell'interessato), è stato evidenziato che la valutazione circa la pertinenza e la necessità delle informazioni presenti all'interno della documentazione ufficiale sanitaria e del verbale di pronto soccorso spetta esclusivamente al personale sanitario e non all'Autorità. Ciò anche in considerazione dell'orientamento giurisprudenziale (cfr., da ultimo, Cass. civ., sez. III, 24 settembre 2015, n. 18868) secondo cui il verbale di pronto soccorso va qualificato come atto pubblico e, come tale, fa piena prova fino a querela di falso relativamente alla provenienza dal pubblico ufficiale che lo ha formato, alle dichiarazioni al medesimo rese, oltre agli altri fatti dal medesimo compiuti o che questi attesti essere avvenuti in sua presenza (nota 23 novembre 2020).

Si è conclusa l'istruttoria relativa al trattamento dei dati personali effettuato da una regione nell'ambito delle attività connesse alla gestione del centro unico di prenotazione regionale (Cup); in particolare, l'attività istruttoria ha riguardato il tema della fornitura del servizio di *call center*, che comporta il trattamento dei dati personali anche relativi alla salute (servizio di prenotazione di prestazioni sanitarie) da parte di un soggetto terzo rispetto al titolare del trattamento. Al riguardo, il Garante ha evidenziato la necessità di provvedere alla designazione del soggetto terzo quale responsabile del trattamento, anche a mente di quanto ribadito dal Cepd (cfr. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR-Version 1.0 adopted on 02 September 2020*, punto 101, nota 35), atteso che l'assenza di una chiara definizione del rapporto tra il titolare e il responsabile può sollevare il problema della mancanza di base giuridica su cui ogni trattamento dovrebbe basarsi (ad es., per quanto riguarda la comunicazione dei dati tra il titolare e il presunto responsabile). Il Garante ha quindi adottato un provvedimento sanzionatorio nei confronti della regione e uno di ammonimento nei confronti di una società cooperativa in relazione alla mancata designazione a responsabile del trattamento di quest'ultima in merito ai trattamenti effettuati attraverso il servizio Cup regionale (provv.ti 14 gennaio 2021, nn. 10 e 11, rispettivamente doc. web n. 9542136 e 9542155). In particolare l'Autorità ha ritenuto priva di effetti una designazione a responsabile del trattamento effettuata nei confronti della cooperativa da parte di un soggetto che era stato a sua volta designato responsabile dalla regione.

L'opportunità di affrontare alcune tematiche in via generale e coordinata è stata rappresentata alla direzione generale per la tutela della salute ed il coordinamento del sistema sanitario regionale di una giunta regionale in relazione al trattamento dei dati personali dei detenuti nell'ambito delle prestazioni di cura loro offerte dalle aziende sanitarie. Interpellato dalla direzione su un documento contenente disposizioni per il corretto trattamento dei dati personali nelle attività di assistenza sanitaria a favore dei detenuti nell'ambito dei servizi di sanità penitenziaria, l'Ufficio ha raccomandato di orientare l'attività al necessario rispetto dei principi generali di cui all'art. 5 del RGPD, con particolare riferimento al principio di *accountability*, e di rispettare le indicazioni fornite dall'Autorità su alcuni dei temi affrontati nel documento trasmesso, con particolare riferimento al *dossier* sanitario, al Fse, alla cd. medicina predittiva e all'attività di telemedicina. Considerato che il Garante è stato interessato anche da altre regioni sulla tematica relativa al trattamento dei dati personali dei detenuti, si è ritenuto di condividere i citati chiarimenti anche con il Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia, perché possa valutare l'opportunità di promuovere iniziative volte a fornire indicazioni in tale ambito agli istituti penitenziari sull'intero territorio nazionale, in considerazione della rilevanza, della portata e dell'impatto che tale trattamento dei dati può determinare sui diritti e le libertà degli interessati (nota 19 aprile 2020).

5

5.15. *Esercizio dei diritti*

Il Regolamento ha innovato profondamente l'istituto in esame sia considerando il reclamo quale unico e generale strumento per la tutela dell'interessato sia configurando il mancato o inidoneo riscontro alle richieste formulate dall'interessato quale violazione soggetta alla sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 5, lett. *b*), del RGPD.

Con riferimento ai reclami proposti in tema di esercizio dei diritti successivamente alla piena applicazione del Regolamento (artt. 12, 15 ss.), l'Autorità ha concluso le prime istruttorie basate sul rinnovato quadro normativo in materia di protezione del dati personali, adottando alcuni provvedimenti di ammonimento per la violazione dell'art. 12, par. 3 in relazione all'art. 15 del RGPD, avendo i titolari fornito riscontro agli interessati solo a seguito dell'invito ad aderire alle richieste di questi ultimi formulato dall'Ufficio. L'applicazione dell'ammonimento è da porre in relazione alla non intenzionalità della condotta, determinata in alcuni casi da un errore dell'operatore preposto alla gestione delle comunicazioni di posta certificata in arrivo, nonché alla sporadicità dell'accadimento e alle misure correttive adottate dal titolare (provv. ti 13 febbraio 2020, n. 33, doc. web n. 9305174; 12 marzo 2020, n. 55, doc. web n. 9365178 e 29 luglio 2020, n. 146, doc. web n. 9453071).

Nella maggior parte dei casi i mancati o inidonei riscontri alle istanze avanzate dall'interessato hanno avuto ad oggetto il diritto di accesso ai dati di cui all'art. 15 del RGPD. Tale diritto è stato spesso esercitato dagli interessati come strumento propedeutico per richiedere – a fronte di eventuali criticità presenti nel trattamento – interventi correttivi (rettifica/integrazione), inibitori (limitazione o opposizione) o eliminatori (cancellazione).

In più di un caso si è evidenziato che, sebbene talune istanze non riscontrate dai titolari fossero state formulate dagli interessati con richiami alla disciplina di protezione dei dati personali, in realtà esse erano finalizzate ad accedere alla documentazione amministrativa (spesso corposa). L'Autorità ha al riguardo ribadito, come in passato già rappresentato anche con riferimento ad ambiti diversi da quello sanitario, l'alterità tra il diritto di accesso ai dati personali e il diritto di accesso alla documentazione esercitato ai sensi della legge n. 241/1990 (v. Relazione 2019, p. 150).

6 La ricerca scientifica

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

Nel campo della ricerca scientifica merita evidenziare due provvedimenti con i quali il Garante, ai sensi degli artt. 110 del Codice e 36 del RGPD, ha espresso parere favorevole in ordine al trattamento dei dati personali per finalità di ricerca medica, biomedica e epidemiologica, in ragione dell'impossibilità di acquisire il consenso al trattamento dei dati personali da parte degli interessati.

Il primo provvedimento fa seguito a una istanza di consultazione preventiva relativa a uno studio clinico multicentrico, osservazionale, retrospettivo concernente il trattamento di particolari categorie di dati riferiti anche a pazienti per i quali la raccolta del consenso sarebbe stata possibile solo con uno sforzo sproporzionato rispetto alle finalità perseguite (provv. 29 ottobre 2020, n. 202, doc. web n. 9517401).

Ai fini della valutazione dell'istanza, il titolare del trattamento (promotore dello studio) ha trasmesso, come richiesto dall'art. 110 del Codice, la valutazione di impatto, redatta ai sensi dell'art. 35 del RGPD, nella quale ha dato evidenza di misure appropriate per tutelare i diritti e le libertà degli interessati coinvolti nel progetto di ricerca, della designazione, quale responsabile del trattamento dei dati, della società incaricata della creazione e dello sviluppo del *database* necessario per l'inserimento dei dati prelevati dalle cartelle cliniche dei pazienti e di quella incaricata di supportare il titolare del trattamento in qualità di CRO (*Clinical Reasearch Organization*). Il titolare ha altresì trasmesso il parere favorevole del comitato etico del centro di ricerca coordinatore, rappresentando l'esigenza, al fine di evitare ritardi che avrebbero irrimediabilmente inciso sulla fattibilità e sulle risultanze dello studio, di avviarlo immediatamente presso il centro coordinatore, subordinando l'inizio dei trattamenti presso gli altri centri sperimentali solo all'ottenimento dei pareri dei comitati etici territorialmente competenti.

Il Garante ha espresso parere favorevole ritenendo sufficiente la documentazione disponibile e sottolineando che il titolare del trattamento, in qualità di *sponsor*, e i centri di sperimentazione potranno dare inizio ai trattamenti dei dati personali necessari per la realizzazione dello studio solo dopo l'ottenimento dei pareri favorevoli dei rispettivi comitati etici territorialmente competenti in conformità al menzionato art. 110 del Codice. Sotto altro profilo, tenuto conto che lo studio in esame vede coinvolto un elevato numero di interessati che, ancorché in vita, non sono singolarmente raggiungibili, al fine di assicurare l'effettiva applicazione dei principi di correttezza e trasparenza (art. 5, par. 1, lett. *a*), del RGPD), ha ingiunto allo *sponsor* di rendere pubbliche le informazioni da fornire agli interessati, ai sensi dell'art. 14 del RGPD, attraverso qualsiasi modalità ritenuta efficace e idonea quale, a titolo meramente esemplificativo, una specifica inserzione sul sito internet della società medesima e/o, laddove possibile, dei centri di sperimentazione coinvolti nonché tramite l'Associazione italiana malati del sonno (in ragione dell'oggetto dello studio), ovvero attraverso l'installazione di appositi pannelli informativi presso i centri di sperimentazione.

Il secondo provvedimento muove anch'esso da un'istanza di consultazione preventiva, presentata ai sensi degli artt. 110 del Codice e 36 del RGPD, concernente uno studio clinico multicentrico osservazionale basato sul trattamento dei dati sulla

salute riferiti sia a soggetti in vita sia a defunti (provv. 10 dicembre 2020, n. 266, doc. web n. 9520597).

La fondazione promotrice dello studio aveva acquisito presso un altro titolare, successivamente posto in liquidazione, la banca dati dei pazienti arruolati nella prima versione dello studio al fine di proseguire la ricerca sospesa (cfr. cons. 50 e art. 5, par. 2, lett. *b*), del RGPD). Successivamente il titolare ha inteso modificare lo studio originario al fine di aggiornare, grazie alla collaborazione con alcuni centri di sperimentazione che avevano partecipato alla prima fase del progetto, i dati dei pazienti arruolati acquisendo ulteriori informazioni e analizzando altresì il tasso di mortalità per la patologia osservata in un determinato arco temporale.

A tal fine, il titolare del trattamento ha trasmesso, oltre al parere favorevole del comitato etico competente, la valutazione di impatto resa ai sensi dell'art. 35 del RGPD rispetto alla quale il Garante ha ritenuto di poter condividere le valutazioni circa l'idoneità delle misure di sicurezza, tecniche e organizzative ivi previste, volte a ridurre i rischi di esposizione degli interessati a minacce concrete di violazione dei propri diritti e libertà fondamentali connessi ai trattamenti di dati personali effettuati nell'ambito dello studio.

Il titolare del trattamento ha dato evidenza della designazione della società fornitrice dei servizi IT, quale responsabile del trattamento dei dati ai sensi dell'art. 28 del RGPD, rappresentando altresì di aver designato, ai sensi dell'art. 29 del RGPD e dell'art. 2-*quaterdecies* del Codice, i soggetti autorizzati ad accedere al *database* dello studio; è stato inoltre prodotto in atti il testo aggiornato dell'informativa predisposta in relazione allo studio in esame, che tiene conto dei rilievi formulati dall'Ufficio in fase istruttoria. L'Ufficio ha infatti ritenuto necessario verificare se e come il titolare del trattamento abbia garantito l'effettività del principio di trasparenza e adempiuto agli obblighi informativi connessi alla raccolta di dati personali presso soggetti terzi per scopi di ricerca scientifica, a seguito dell'acquisizione della banca dati, relativa all'originario progetto, dal cedente titolare in liquidazione (artt. 5, par. 1, lett. *a*) e 14, par. 5, lett. *b*), del RGPD).

La normativa in materia di protezione dei dati personali infatti prevede espressamente che, qualora i dati siano ottenuti presso terzi, come nel caso in esame, il titolare del trattamento possa non rendere le informazioni di cui ai parr. da 1 a 4 dell'art. 14 del RGPD se la comunicazione di tali informazioni risulti impossibile o implichi uno sforzo sproporzionato. Ciò, in particolare, nell'ambito dei trattamenti svolti per finalità di ricerca scientifica, ferme restando le condizioni e le garanzie di cui all'art. 89, par. 1, del RGPD. In tali casi, il titolare del trattamento è comunque tenuto ad adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni (art. 14, par. 5, lett. *b*), del RGPD).

Il Garante, nell'esprime parere favorevole sulla richiamata istanza di consultazione preventiva, ha dichiarato illecita la condotta omissiva del titolare che non aveva fornito l'informativa connessa alla raccolta di dati personali presso terzi e con il medesimo provvedimento ha ammonito il titolare per la violazione degli artt. 5, par. 1, lett. *a*), 14, par. 5, lett. *b*), del RGPD e 6, comma 3 delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, all. A5 al Codice.

Un'altra istanza di consultazione preventiva ha riguardato il trattamento di dati personali relativi alla salute di cinque pazienti deceduti, svolto nell'ambito di uno studio aggiuntivo teso a dimostrare l'efficacia e la sicurezza di un farmaco e a consentire alle autorità competenti (europee e statunitensi) di valutarne la sicurezza e l'efficacia per concludere la relativa procedura di approvazione.

Sulla base degli elementi acquisiti nel corso dell'istruttoria, il parere del Garante

non si è reso necessario in quanto il consenso prestato dagli interessati atteneva anche al menzionato studio aggiuntivo e a tutti i dati contenuti nelle cartelle cliniche, il cui esame si è reso necessario per l'approvazione del farmaco da parte delle autorità competenti (nota del 19 febbraio 2020).

6.2. *Registro impianti protesici mammari, Registro nazionale della talassemia e delle altre emoglobinopatie e Registro nazionale tumori*

Numerose sono state le interlocuzioni informali con il Ministero della salute sulle bozze di regolamento per l'istituzione di alcuni registri di mortalità, di tumori e di altre patologie (l'art. 12, d.l. 18 ottobre 2012, n. 179 e d.P.C.M. 3 marzo 2017), segnatamente concernenti il Registro nazionale degli impianti protesici mammari, il Registro nazionale della talassemia e delle altre emoglobinopatie e il Registro nazionale tumori.

In via generale, è stata evidenziata la necessità che il Ministero accompagni questi atti di natura regolamentare con una relazione illustrativa e una valutazione d'impatto. Sono poi seguite alcune preliminari osservazioni che hanno riguardato, in particolare, la base giuridica dei trattamenti svolti attraverso i Registri, i diversi ruoli dei soggetti che intervengono nelle operazioni di trattamento che devono essere definiti ai sensi della normativa in materia di protezione dei dati personali (artt. da 27 a 29 del RGPD), le metodologie applicate per evitare il rischio di reidentificazione degli interessati e le misure tecniche implementate ai sensi dell'art. 32 del RGPD nonché l'opportunità di richiamare espressamente l'art. 110 del Codice, in quanto sulle ricerche previste *ex lege* non è necessaria la consultazione preventiva ma solo l'obbligo di pubblicare la valutazione di impatto.

Il Garante è in attesa di ricevere la richiesta formale di parere sulle bozze definitive dei richiamati schemi di regolamento al fine di formulare il parere di competenza.

7 La statistica

L'Istat costituisce un *unicum* nel panorama delle p.a. per la straordinaria concentrazione di dati personali trattati in vista del perseguimento della propria funzione istituzionale tesa alla realizzazione dell'informazione statistica ufficiale. L'Istituto, infatti, duplica e, all'occorrenza, interconnette quasi tutte le banche dati pubbliche, quelle di soggetti privati acquisite per la realizzazione della statistica ufficiale e raccoglie informazioni presso gli interessati, nell'ambito delle cd. indagini dirette.

Coerentemente con l'evoluzione della statistica ufficiale a livello europeo, l'Istat è passato da una prevalenza di rilevazioni dirette presso gli interessati a costanti e massive duplicazioni delle fonti amministrative, anche per la creazione di cd. *repository*, ovvero sistemi informativi statistici tematici che raccolgono, per la creazione di campioni statistici, informazioni sui singoli, analizzate sotto diversi profili (come ad es. assistiti, lavoratori, contribuenti, vittime di determinati reati, studenti, ecc.). Ciò anche al fine di ridurre il cd. fastidio statistico.

Nel corso dell'anno di riferimento, l'Autorità è intervenuta affinché il trattamento di dati personali per la realizzazione della statistica ufficiale si conformi alla normativa vigente così come rinnovata a seguito dell'entrata in vigore del Regolamento e del Codice novellato, tenendo in debita considerazione le eccezioni e le deroghe previste per il perseguimento di scopi statistici. Si evidenzia, infatti, che i trattamenti di dati personali per fini statistici (come quelli di ricerca scientifica e di archiviazione nel pubblico interesse), in presenza di adeguate garanzie a tutela dei diritti e delle libertà fondamentali degli interessati, tra cui in particolare rileva l'impiego di adeguate tecniche di pseudonimizzazione, possono essere svolti anche in deroga ad alcuni dei principi applicabili al trattamento (artt. 5, par. 1, lett. *b*) e *e*) e 89, par. 1, del RGPD) e, come detto, dei diritti spettanti agli interessati (artt. 15, 16, 18, 21 e 89, par. 2, del RGPD).

7.1. *Autorizzazione allo svolgimento dei trattamenti di dati personali necessari per la realizzazione del censimento permanente*

Come ricordato nelle precedenti Relazioni, con provvedimento del 9 maggio 2018, n. 271 (doc. web n. 9001732), il Garante, nel formulare il parere di competenza sullo schema di Programma statistico nazionale 2017-2019, aggiornamento 2018-2019, si era espresso negativamente sui lavori statistici connessi all'attuazione del cd. censimento permanente, di cui alla legge 27 dicembre 2017, n. 205 (art. 1, comma 227, lett. *a*). Successivamente, con provvedimento del 4 ottobre 2018, n. 459 (doc. web n. 9047672), il Garante, seppur con specifiche prescrizioni, ha autorizzato l'Istat ad avviare le operazioni censuarie di raccolta dei dati sul campo, ma ha, al tempo stesso, ritenuto necessario proseguire gli approfondimenti istruttori al fine di conformare alla normativa in materia di protezione dei dati personali siffatti trattamenti su larga scala, attesi gli elevati rischi che presentano per le libertà e i diritti degli interessati.

Con provvedimento del 23 gennaio 2020, n. 10 (doc. web n. 9261093), il Garante ha concluso il processo di autorizzazione dei trattamenti di dati personali necessari per la realizzazione del censimento permanente. In tale ambito, si è tenuto

conto delle peculiarità relative alla rinnovata modalità operativa di svolgimento del censimento permanente, che non solo prevede l'interconnessione di numerosi archivi amministrativi, ma altresì tempi di conservazione dei dati molto estesi. Specifici avvertimenti e prescrizioni sono stati formulati nei confronti dell'Istituto per la corretta applicazione dei principi relativi al trattamento dei dati personali e per assicurare, nel rispetto del principio di proporzionalità (cons. 4 del RGPD), adeguata tutela ai diritti e alle libertà fondamentali degli interessati.

In primo luogo, l'Autorità ha formalmente avvertito l'Istituto, ai sensi dell'art. 58, par. 2, lett. *a*), del RGPD, della necessità che, nel pieno rispetto del principio di responsabilizzazione (*accountability*) e dell'obbligo di protezione dei dati fin dalla progettazione (artt. 5, par. 2; 24 e 25, par. 1, del RGPD), esso non solo ponga in atto misure tecniche e organizzative adeguate a garantire che i trattamenti siano conformi alla disciplina vigente, ma sia anche in grado di darne dimostrazione. L'Autorità ha fatto riferimento, in modo particolare, all'elaborazione della documentazione, alla motivazione delle scelte effettuate e alla descrizione e analisi dei rischi connessi ai trattamenti. Il rinnovato quadro normativo richiede, infatti, al titolare del trattamento una valutazione ponderata di tutte le scelte connesse ai trattamenti di dati personali che risultino supportate da idonee motivazioni che, anche attraverso indicatori qualitativi e quantitativi, dimostrino l'efficacia delle misure implementate (cfr. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, adottate il 13 novembre 2019 dal Cepd).

L'Autorità ha poi rilevato specifiche criticità in relazione ai principi di minimizzazione dei dati, limitazione della finalità e della conservazione, con riferimento ai trattamenti connessi alle operazioni censuarie e ai successivi trattamenti svolti per ulteriori finalità statistiche derivanti dalla tecnica di pseudonimizzazione adottata (art. 5, par. 1, lett. *b*), *c*) e *e*), del RGPD). In particolare, l'Istituto aveva considerato come adeguata forma di pseudonimizzazione dei dati quella che conduce all'attribuzione di un codice univoco che identifica l'individuo nell'ambito di tutte le banche dati Istat provenienti da fonti amministrative (cd. codice SIM). L'Autorità ha invece ritenuto che, seppure l'attribuzione di tale codice alle singole unità statistiche nella fase di raccolta e prima elaborazione dei dati per le operazioni censuarie possa essere considerata una misura adeguata a garantire la confidenzialità dei dati trattati e a ricondurre ad un unico interessato i dati raccolti attraverso diverse fonti amministrative (a garanzia dell'accuratezza del dato), tale attribuzione si riveli tuttavia inidonea a garantire un'efficace attuazione degli altri principi applicabili al trattamento dei dati personali (minimizzazione, limitazione della finalità e della conservazione dei dati), a causa delle staticità del codice.

Tenuto conto dello specifico contesto dei trattamenti, l'adozione di un meccanismo statico di codifica dei dati evidenzia significative criticità.

In primo luogo, tale meccanismo di codifica conferisce ai dati personali una struttura rigida, schiudendo il rischio che, nel selezionare i dati personali necessari per un qualsiasi lavoro statistico, vengano trattate anche informazioni riferite a un singolo interessato non pertinenti rispetto allo specifico scopo perseguito. Ciò in quanto l'assegnazione di un codice invariante nelle diverse basi dati, non è in grado di offrire quella flessibilità necessaria a selezionare, di volta in volta, solo le informazioni effettivamente pertinenti rispetto alla specifica finalità statistica perseguita.

In secondo luogo, il mantenimento di tale codice univoco nel tempo impedisce di differenziare i tempi di conservazione dei dati in relazione alle diverse finalità statistiche perseguite. L'invarianza del codice infatti condiziona le scelte del titolare rispetto alla conservazione o alla cancellazione del dato offrendogli esclusivamente due opzioni: quella del mantenimento del codice univoco, con tutte le informazio-

ni ad esso associate, ovvero la cancellazione di tali informazioni. Viceversa, l'introduzione di plurimi codici pseudonimi consentirebbe un'attuazione più efficace del principio di limitazione della finalità e della conservazione. Ciò in quanto a ciascuno di essi potrebbe essere associato uno specifico periodo di validità, allo scadere del quale si potrebbe, in ragione delle esigenze statistiche, provvedere alla loro rigenerazione o alla cancellazione dei codici e dei dati ad esso associati.

Su tali basi, il Garante, con il provvedimento in esame, ha prescritto all'Istat l'adozione di specifiche misure di pseudonimizzazione idonee a prevenire i richiamati rischi attraverso l'assegnazione di diversi codici pseudonimi, ciascuno con una validità limitata alla specifica finalità perseguita, secondo una logica gerarchica che consenta, ove se ne ravvisi la necessità, di ricongiungere i vari pseudonimi al medesimo interessato. Tali codici dovranno avere tempi di validità differenziati in ragione dei diversi scopi perseguiti, allo scadere dei quali, essi dovranno essere rigenerati o cancellati unitamente ai dati ad essi associati.

Ulteriori criticità hanno riguardato la definizione delle garanzie per la diffusione dei dati. Sul punto il Garante ha prescritto di integrare il Piano generale del censimento (Pgc) con l'indicazione delle modalità di restituzione ai comuni, in forma aggregata, delle informazioni raccolte nell'ambito del censimento, come stabilito dall'art. 1, comma 233, l. 27 dicembre 2017, n. 205 (legge di bilancio), così come modificato dall'art. 22, comma 7, d.lgs. n. 101/2018, e che le tecniche di aggregazione dei dati siano supportate da adeguate argomentazioni (misure e indicatori di prestazione) circa la probabilità di reidentificazione degli interessati.

Sul punto l'Istituto ha chiarito di operare una rappresentazione dei dati per classi (cd. rappresentazione per ipercubi) che consente in ogni momento di individuare con certezza tutti i casi di rivelazione dell'identità (*identity disclosure*) e di stimare la probabilità che si verifichino casi di divulgazione degli attributi (*attribute disclosure*). Questa conoscenza permette all'Istituto di intervenire, con opportune aggregazioni tra classi, per ridurre l'incidenza del rischio di reidentificazione degli interessati.

Con riguardo ai livelli di aggregazione dei dati destinati ai comuni, l'Istituto ha rappresentato che le variabili sono aggregate a livello comunale e che, ai fini della valutazione della probabilità di reidentificazione degli interessati, utilizzerà le stesse metriche sopra descritte. L'Istat si è infine formalmente impegnato ad applicare tali tecniche per ogni settore, adeguandole rispetto al contesto specifico relativo ai diversi lavori statistici presenti nel programma statistico nazionale.

Con riferimento alle tecniche di pseudonimizzazione che l'Istituto intende applicare per conformarsi al provvedimento, l'Istat ha trasmesso un documento recante "Soluzioni tecnologiche ed organizzative per realizzare la piena compliance del Sistema di Integrazione dei Microdati" (SIM, acronimo dal quale deriva la denominazione del codice pseudonimo utilizzato in tale contesto) rispetto al quale, in ragione della complessità delle tematiche illustrate, sono tuttora in corso specifici approfondimenti.

Si segnala, infine, che il Garante ha dato atto delle criticità superate in relazione alle operazioni di trattamento concernenti la realizzazione del censimento permanente a suo tempo rilevate con il provvedimento del 4 ottobre 2018, n. 459 (doc. web n. 9047672).

7.2. *Provvedimenti correlati al Programma statistico nazionale*

Nell'anno di riferimento l'Autorità ha adottato diversi provvedimenti correlati alla programmazione statistica triennale che l'Istat è istituzionalmente chiamato a predisporre (art. 15, d.lgs. n. 322/1989).

7.2.1. Parere sullo schema di Programma statistico nazionale 2017-2019 – Aggiornamento 2019 del 13 febbraio 2020

Con provvedimento del 13 febbraio 2020, n. 29 (doc. web n. 9283929), il Garante ha reso parere favorevole sullo schema di Programma statistico nazionale 2017-2019 – Aggiornamento 2019 (Psn), pur esprimendosi negativamente rispetto a taluni specifici lavori statistici.

In via preliminare, è stato evidenziato come, dopo l'entrata in vigore del Regolamento, sia seguita una modifica rilevante all'art. 6-*bis*, d.lgs. n. 322/1989, il quale ora richiede che nel Psn siano indicati, in particolare:

- i tipi di dati;
- le operazioni eseguibili;
- le misure adottate per tutelare i diritti fondamentali e le libertà degli interessati;
- le misure tecniche e organizzative idonee a garantire la liceità e la correttezza del trattamento, con particolare riguardo al principio di minimizzazione dei dati. Inoltre, per ciascun trattamento, vanno indicati: a) le modalità; b) le categorie dei soggetti interessati; c) le finalità perseguite; d) le fonti utilizzate; e) le principali variabili acquisite; f) i tempi di conservazione; g) le categorie dei soggetti destinatari dei dati.

Occorre considerare che il Psn funge da informativa agli interessati in riferimento ai dati raccolti presso soggetti terzi (come previsto dall'art. 6, comma 2 delle menzionate regole deontologiche) e che, in base al Regolamento, sono più ampi gli elementi informativi che i titolari del trattamento devono rendere noti agli interessati in fase di raccolta (cfr. art. 13 del RGPD).

Il Garante ha fornito ulteriori e specifiche indicazioni affinché, nei Psn futuri, i prospetti informativi relativi ai singoli lavori statistici siano più chiari e comprensibili e quindi sia assicurata l'effettiva applicazione del principio di trasparenza; anzitutto prevedendo che ciascun prospetto informativo debba recare le indicazioni riguardanti il tempo di conservazione (o i criteri utilizzati per definirli) rispetto a ciascun lavoro statistico (art. 13, par. 2, lett. *a*), del RGPD).

Il Garante ha altresì ritenuto fuorviante l'indicazione, per ciascun lavoro statistico, di tempi di conservazione differenti in ragione della fonte di provenienza dei diversi dati trattati, rappresentando l'esigenza che, per ogni lavoro, sia indicato il tempo di conservazione necessario al proseguimento dello specifico scopo statistico dichiarato e l'eventuale ulteriore periodo di conservazione nel caso del perseguimento di ulteriori scopi statistici con i medesimi dati (artt. 5, par. 1, lett. *b*) ed *e*) e 89 del RGPD e 6-*bis*, comma 4, d.lgs. n. 322/1989).

L'Autorità si è espressa anche sulle modalità con le quali l'Istat ha inteso adempiere alla nuova prescrizione in base alla quale il Psn deve contenere anche specifiche indicazioni in ordine alle misure adottate per tutelare i diritti fondamentali e le libertà degli interessati e alle misure tecniche e organizzative idonee a garantire la liceità e la correttezza del trattamento, con particolare riguardo al principio di minimizzazione dei dati (art. 6-*bis*, d.lgs. n. 322/1989). Sul punto, è stata apprezzata l'impostazione individuata dall'Istituto in base alla quale ogni titolare fornisce specifiche indicazioni rispetto alle misure tecniche e organizzative implementate (riportate in un'apposita appendice). L'Autorità ha sottolineato però come non risulti a tal fine necessario dare evidenza ad adempimenti già previsti dal Regolamento (si pensi ad es. alla compilazione del registro dei trattamenti ex art. 30 del RGPD o all'adesione a codici di condotta, tenuto in considerazione che, allo stato, non risultavano ancora approvati ai sensi dell'art. 40 del RGPD). In secondo luogo, rilevando una certa eterogeneità nella descrizione delle misure in esame fornita dai diversi soggetti Sistan, titolari dei

7

lavori statistici inseriti nel Psn, il Garante ha invitato l'Istituto a conferire maggiore coerenza e omogeneità al paragrafo in esame (artt. 6-*bis* e 15, comma 1, lett. *a*) e *d*), d.lgs. n. 322/1989).

Nel corso dell'istruttoria relativa allo schema di Psn in esame, l'Ufficio ha svolto taluni ulteriori approfondimenti istruttori sul SIM (Sistema integrato di microdati amministrativi), oggetto di parere negativo nell'ambito del provvedimento del 9 maggio 2018 e di specifiche prescrizioni nel provvedimento del 23 gennaio 2020, n. 271 (rispettivamente docc. web nn. 9261093 e 9001732).

Nel provvedimento del 2020, il Garante si è nuovamente soffermato sul Sistema integrato di microdati amministrativi, consistente in un'infrastruttura tecnologica costruita in base a specifiche logiche statistiche e contrassegnata nel Psn dal codice IST-02270; più precisamente, si tratta di un'infrastruttura "intermedia" di supporto ai lavori statistici, deputata alla centralizzazione dell'acquisizione di fonti amministrative e alla gestione dei dati. In tal modo l'Istat mira a creare un ambiente unico e sicuro per l'acquisizione, la gestione e l'archiviazione dei dati amministrativi raccolti per finalità statistiche. A ogni singola unità statistica è attribuito un codice SIM che consente il collegamento di varie basi di dati attraverso specifiche operazioni (*record linkage*). I dati così strutturati sono quindi resi accessibili agli utenti interni autorizzati. Su tali basi l'Autorità, tenuto conto delle misure già prescritte con il citato provvedimento, ha ritenuto che non vi siano elementi ostativi al suo utilizzo.

Nel rilevare un incremento di registri statistici all'interno del Psn, il Garante ha ribadito la necessità che vengano adottate specifiche misure di pseudonimizzazione secondo le indicazioni già fornite per il trattamento e la conservazione dei dati in tali contesti; ciò in quanto in tali registri spesso si cumulano trattamenti primari e secondari di dati personali per scopi statistici. L'Autorità si è quindi espressa negativamente in relazione ai seguenti lavori statici: IST-2729-Registro degli edifici e delle unità abitative; IST-02721-Registro base degli individui delle famiglie e delle convivenze, IST-02742-Registro del lavoro, IST-01382-Registro annuale su retribuzioni, ore e costo del lavoro individuale, IST-02638-Integrazione dati e registro redditi, consumi e ricchezza; IST-02638-Integrazione dati e registro redditi, consumi e ricchezza; IST-02634-Sistema informativo sull'occupazione - Registro Asia Occupazione.

Statistiche da indagine

Specifica attenzione è stata prestata anche alle cd. statistiche da indagine, che prevedono la raccolta di informazioni direttamente presso gli interessati. La rinnovata modalità di realizzazione dei lavori statistici, attraverso l'utilizzo di molteplici fonti amministrative, ha inciso in maniera determinante anche su tali lavori in quanto sovente i dati rilevati presso gli interessati sono successivamente collegati con altri, già in possesso dell'Istituto. Al fine di assicurare l'effettività dei principi di correttezza e trasparenza, l'Autorità ha formalmente avvertito l'Istituto, ai sensi dell'art. 58, par. 2, lett. *a*), del RGPD, della necessità che tale logica di trattamento sia rappresentata agli interessati nell'ambito delle informazioni rese ai sensi dell'art. 13 del RGPD.

Tra i lavori oggetto di parere non favorevole da parte del Garante rilevano, in particolare, quelli per i quali è stata prevista la diffusione delle variabili in forma disaggregata in quanto, in base al principio di responsabilizzazione, il Garante ha ritenuto necessario che, per avvalersi della deroga ai limiti posti dalla disciplina in materia di segreto statistico di cui all'art. 13, comma 3-*bis*, d.lgs. n. 322/1989, i titolari del trattamento debbano comunque specificare che i risultati verranno diffusi in modo da escludere l'identificazione di singoli interessati secondo i parametri di cui al cons. 26 del RGPD o, in subordine, fornire adeguate e circostanziate motivazioni che giustifichino una tale forma di disaggregazione dei dati alla luce del principio di proporzionalità richiamato al cons. 4 del RGPD.

7.2.2. Pareri su alcuni lavori statistici sospesi

Con provvedimento del 19 maggio 2020, n. 87 (doc. web n. 9370217), il Garante si è espresso favorevolmente sui lavori statistici IST-02607 Indagine su bambini e ragazzi: comportamenti, atteggiamenti e progetti futuri, e IST-02732 Modulo dell'indagine sulla immagine sociale della violenza nelle scuole e IST-01858 Multiscopo sulle famiglie (lavori sospesi a seguito del parere 9 maggio 2018 sullo schema di Psn 2017-2019, aggiornamento 2018-2019 (doc. web n. 9001732).

Le principali criticità rilevate avevano riguardato il coinvolgimento di soggetti minori di età, anche infraquattordicenni, e l'assenza di garanzie idonee a tutelare la dignità di rispondenti particolarmente giovani d'età e, per ciò solo, estremamente vulnerabili, specie nelle ipotesi di raccolta di dati connessi a temi particolarmente delicati oltre che di informazioni sensibili (quali le difficoltà nelle attività quotidiane, la contraccezione e la vita sessuale, i determinanti della salute, l'abitudine al fumo, i problemi di peso, l'attività fisica, il consumo di alcol e la storia migratoria). Il Garante ha ritenuto pertanto necessario acquisire ulteriori elementi istruttori, con particolare riguardo alle valutazioni d'impatto ai sensi dell'art. 35 del RGPD.

Con riferimento all'indagine IST-02607 Indagine su bambini e ragazzi: comportamenti, atteggiamenti e progetti futuri, al cui interno è inserito il lavoro IST-02732 Modulo dell'indagine sulla immagine sociale della violenza nelle scuole, il principale elemento di osservazione del Garante ha riguardato la residuale previsione di applicare l'obbligo di risposta per i minorenni di età compresa tra i 14 e i 18 anni; già a seguito del provvedimento del 9 maggio 2018, infatti, era stato eliminato tale obbligo per gli infraquattordicenni, indicando tale circostanza nel relativo prospetto informativo. Ciò premesso, pur non essendo l'obbligo di risposta previsto per i minori tra i 14 e i 18 anni corredato da una sanzione amministrativa in caso di violazione, il Garante ha ritenuto tale previsione sproporzionata, tenuto conto dell'invasività dei quesiti sottoposti rispetto alla finalità perseguita di promuovere l'adesione all'indagine da parte dei rispondenti. Ciò anche alla luce di quanto previsto dalla Convenzione sui diritti dell'infanzia e dell'adolescenza nella parte in cui richiede che gli Stati garantiscano "al fanciullo capace di discernimento il diritto di esprimere liberamente la sua opinione su ogni questione che lo interessa" (art. 12).

Anche in relazione al lavoro IST-01858 Multiscopo sulle famiglie: uso del tempo l'Autorità si è, in primo luogo, soffermata sull'obbligo di risposta, ritenendolo proporzionato per gli ultraquattordicenni, soprattutto in ragione della minore invasività della tipologia di dati raccolti rispetto al lavoro IST-02607. Tuttavia, affinché la previsione dell'obbligo di risposta per i soggetti ultraquattordicenni possa costituire una misura rispettosa della sfera privata degli interessati, si è ritenuto necessario, anche in considerazione del principio di correttezza e trasparenza del trattamento, prescrivere all'Istituto di evidenziare chiaramente nell'informativa, resa all'atto della rilevazione (tramite una lettera inviata alle famiglie a firma del Presidente), nonché nel relativo prospetto informativo, che al mancato conferimento dei dati per i quali è previsto un obbligo di risposta non corrisponde l'applicazione di una sanzione amministrativa da parte dell'Istituto (artt. 5, par. 1, lett. *a*) e 13, par. 2, lett. *e*), del RGPD).

A tale riguardo, si segnala che il Garante ha preso favorevolmente atto della scelta di considerare come quesiti di natura sensibile, non soggetti quindi all'obbligo di risposta, anche quelli relativi allo stress (sez. 5.2 e 5.3 del modello denominato Istat IMF-13B), che toccano la sfera della salute psico-fisica dei rispondenti. Nel provvedimento in esame, con riferimento ad entrambi i lavori statistici, l'Autorità si è espressa in relazione ai tempi di ulteriore conservazione dei dati, ritenendo che in entrambi i casi lo scopo dell'ulteriore trattamento – previsto per il lavoro IST-02607 in 20 anni e per il lavoro IST-01858 in 10 anni – non fosse ben determinato (art. 5,

par. 1, lett. *e*), del RGPD).

Sul punto rileva altresì la disciplina di settore in base alla quale i dati personali raccolti specificatamente per uno scopo statistico possono essere trattati dai soggetti che fanno parte o partecipano al Sistan per altri scopi statistici di interesse pubblico e previsti da una specifica base normativa quando questi ultimi sono chiaramente determinati e di limitata durata. Tale eventualità è chiaramente rappresentata agli interessati al momento della raccolta o, quando ciò non è possibile, è resa preventivamente nota al pubblico e al Garante nei modi e nei termini previsti dalle regole deontologiche (art. 6-*bis*, comma 4, d.lgs. n. 322/1989).

Su tali basi, nelle more della revisione delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistan (All. A.4 al Codice), il Garante ha quindi prescritto che eventuali ulteriori trattamenti con i dati raccolti per la realizzazione dei lavori statistici in esame siano preventivamente resi noti all'Autorità. Ciò al fine di consentire una verifica circa la compatibilità degli stessi rispetto allo scopo della raccolta, soprattutto laddove siano previste operazioni di collegamento (*record linkage*) con archivi amministrativi, tenuto anche conto dell'adeguatezza delle misure implementate ai sensi dell'art. 89 del RGPD. Sul punto il Garante ha prescritto che ai lavori in esame siano applicate le tecniche di pseudonimizzazione che verranno adottate dall'Istituto per conformarsi al provvedimento del 23 gennaio 2020, n. 10 (doc. web n. 9261093).

L'Autorità si è poi concentrata sulla verifica dell'effettiva applicazione del principio di esattezza del dato all'atto della composizione dei campioni statistici necessari alla realizzazione delle indagini. Un campione è esattamente composto quando risulta adeguatamente rappresentativo della popolazione oggetto di rilevazione, con tutte le sue variabili. Tale circostanza incide in maniera determinate sul corretto trattamento di dati personali nella misura in cui il fine di ogni rilevazione statistica è quello di raggiungere una migliore comprensione di un fenomeno sociale, allo scopo di far discendere da tale nuova conoscenza idonei interventi da parte dei decisori pubblici.

Ciò premesso, l'Autorità, pur ritenendo astrattamente non critici i criteri per la definizione del campione definiti dall'Istat, ha rilevato come l'Istituto non avesse adeguatamente rappresentato, attraverso specifici indicatori, l'efficacia della metodologia applicata per la definizione del campione (cfr. in particolare i punti 64, 65, da 72 a 74, delle *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, adottate il 13 novembre 2019, dal Cepd). È stato quindi prescritto di integrare le valutazioni di impatto con tali elementi e l'Istituto ha provveduto in tal senso.

L'Autorità ha rilevato specifiche criticità anche in relazione alle tecniche di aggregazione applicate in fase di diffusione dei dati per escludere il rischio di reidentificazione degli interessati, riguardanti per lo più le modalità di aggregazione dei dati. In particolare, è stato evidenziato come, in primo luogo, l'Istat non supportasse attraverso specifiche metriche l'indicazione delle probabilità di reidentificazione degli interessati; in secondo luogo, si è rilevato come la sola applicazione *ex ante* di tecniche di aggregazione non consentisse sempre di prevenire casi di singolarità all'interno di un campione.

Infatti, possono verificarsi situazioni nelle quali la disponibilità di un'informazione ausiliaria da parte di un soggetto terzo (cd. attaccante) può consentire la reidentificazione di un interessato presente in un campione sottoposto a preventive tecniche di aggregazione. Questa evenienza (cd. attacco) è tanto più probabile quanto più rare sono le caratteristiche del campione. È stato quindi prescritto all'Istat di evidenziare in termini numerici la probabilità di reidentificazione degli interessati tenendo conto dei richiamati rilievi.

Anche a tale prescrizione l'Istituto ha ottemperato fornendo le indicazioni metodologiche richieste.

7.2.3. Schema di Programma statistico nazionale 2020-2022

Con provvedimento del 10 dicembre 2020, n. 261 (doc. web n. 9520567), il Garante si è espresso sullo schema di Programma statistico nazionale 2020-2022 (Psn). In particolare, ne è stata apprezzata la razionalizzazione grazie alla quale risulta più chiaro il riferimento alle modalità con le quali gli interessati possono esercitare i loro diritti e alla logica applicata ai trattamenti svolti, in particolare, attraverso l'uso di grandi banche dati.

Criticità sono state rilevate, invece, in relazione ai prospetti identificativi dei singoli lavori statistici, ancora troppo eterogenei e disarmonici tra loro, nonché di difficile comprensione, con ciò disattendendosi sia le aspettative del legislatore europeo – per cui la base giuridica o la misura legislativa su cui si fonda un trattamento di dati personali dovrebbe essere chiara e precisa e la sua applicazione prevedibile per le persone che vi sono sottoposte (cons. 41 del RGPD) – sia il principio di trasparenza, giacché il Psn funge da informativa agli interessati in relazione ai dati raccolti presso soggetti terzi (art. 6, comma 2, delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistan, all. A4 al Codice).

Le questioni di seguito affrontate sono quindi state oggetto di formali avvertimenti da parte del Garante, ai sensi dell'art. 58, par. 2, lett. *a*), del RGPD, affinché, già a partire dai prossimi aggiornamenti, l'Istituto proceda a revisionare il Psn, anche secondo una logica di gradualità, al fine di potersi pervenire, per la prossima programmazione triennale (2023-2025), a un documento maggiormente in linea con la disciplina di protezione dei dati personali. Si è evidenziato che la descrizione delle finalità del trattamento nei richiamati prospetti continui a non essere sempre chiara e intellegibile e i riferimenti normativi ivi riportati imprecisi e fuorvianti.

È stata altresì rilevata la presenza nel Psn di numerosi lavori statistici di titolarità dell'Istituto Superiore di Sanità e di talune regioni che, nel descrivere lo specifico obiettivo statistico perseguito, evidenziano anche l'intenzione di costituire un osservatorio, un sistema di sorveglianza, un registro ovvero di realizzare uno studio epidemiologico o di svolgere attività di verifica *a posteriori* (*follow up*). Il Garante ha precisato che il trattamento di dati personali per la realizzazione di ricerche scientifiche in ambito medico, biomedico e epidemiologico debba essere effettuato nel rispetto della specifica disciplina di cui all'art. 110 del Codice, delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, all. A5 al Codice, e delle prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (all. n. 5 al provvedimento che individua le prescrizioni contenute nelle autorizzazioni generali che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice, del 13 dicembre 2018, doc. web n. 9068972). Parimenti, è stato ribadito che l'istituzione di nuovi sistemi di sorveglianza e registri può avvenire solo nel rispetto della specifica normativa di settore per le finalità ivi richiamate (art. 12, commi da 10 a 14, d.l. 18 ottobre 2012, n. 179, d.P.C.M. 3 marzo 2017), potendo il Psn indicare unicamente i trattamenti di dati personali svolti per il perseguimento di scopi statistici (art. 6-*bis*, comma 1-*bis*, d.lgs. n. 322/1989).

Specifica attenzione è stata rivolta alla presenza nel Psn di taluni dei registri e dei sistemi di sorveglianza già istituiti presso l'Iss ai sensi del richiamato d.P.C.M. 3 marzo 2017 affinché, nelle more del completamento della disciplina relativa all'istituzione dei registri di patologia e dei sistemi di sorveglianza, vengano chiaramente distinte le finalità di statistica ufficiale, le uniche da doversi indicare all'interno del

Psn, da quelle di cui al richiamato art. 12, comma 10, d.l. n. 179/2012 e all'art. 1, d.P.C.M. 3 marzo 2017. Ciò tenuto anche conto che ciascuna di queste differenti finalità può richiedere differenti modalità di trattamento dei menzionati registri, in conformità al principio di minimizzazione dei dati e di limitazione della finalità.

Il Garante ha quindi formalmente avvertito l'Istituto, ai sensi dell'art. 58, par. 2, lett. *a*), del RGPD, della necessità che i prospetti informativi indichino con chiarezza gli scopi statistici (e non quelli di altra natura) perseguiti per la realizzazione dei lavori inseriti nel Psn, facendo riferimento a pertinenti basi normative.

I diritti degli interessati

L'Autorità ha poi affrontato il tema dei diritti spettanti agli interessati di cui agli artt. 15, 16, 18 e 21, che possono essere in ambito statistico oggetto di specifiche deroghe ai sensi dell'art. 89 del RGPD, evidenziando come la sede appropriata per definire la portata di tali deroghe e le garanzie poste a tutela dei diritti e delle libertà fondamentali degli interessati siano le regole deontologiche (artt. 2-*quater* e 105 del Codice).

In tale quadro, il Garante ha sottolineato la peculiarità correlata al diritto di opposizione, che non spetta agli interessati se il trattamento statistico è necessario (come quelli in esame) per l'esecuzione di un compito di interesse pubblico (art. 21, par. 6, del RGPD). L'Autorità ha tuttavia posto l'accento sulla circostanza che tale eccezione non ha carattere assoluto ma sia, per esplicito dettato normativo, subordinata alla presenza di garanzie adeguate per i diritti e le libertà dell'interessato, con particolare riferimento a misure di pseudonimizzazione, ai sensi dell'art. 89, par. 1, del RGPD.

Il Garante ha precisato, infine, formulando sul punto un formale avvertimento all'Istituto, che la deroga al diritto di opposizione, in omaggio ai principi di correttezza e trasparenza, comporta specifici oneri informativi nei confronti degli interessati i quali devono, al fine di poter correttamente esercitare il proprio diritto all'autodeterminazione informativa, poter essere a conoscenza del fatto che, aderendo ad una rilevazione inserita nel Psn, non è loro riconosciuto il diritto di opposizione.

Conservazione dei dati

Il Garante si è soffermato sulla complessa questione dell'indicazione, nei prospetti informativi, del tempo di conservazione dei dati raccolti per uno scopo statistico e del tempo di ulteriore conservazione correlato ad eventuali usi secondari.

Tenuto conto del principio di limitazione della conservazione (art. 5, par. 1, lett. *e*), del RGPD), il Garante ha preso favorevolmente atto dell'intenzione dell'Istituto di indicare, nei prospetti informativi, unicamente il tempo di conservazione delle informazioni ritenuto di volta in volta necessario al perseguimento dello scopo statistico rappresentato nella sezione "obiettivo" del medesimo prospetto, secondo quanto già evidenziato dall'Autorità nel parere sullo schema di Psn 2017-2019 – Aggiornamento 2019 (doc. web n. 9283929).

In secondo luogo, è stato precisato che il Regolamento consente la conservazione dei dati per periodi più lunghi rispetto a quelli necessari al raggiungimento dello scopo posto a fondamento della raccolta, a condizione che siano trattati solo per alcune specifiche finalità, tra le quali quelle statistiche, conformemente all'art. 89, par. 1, del RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato (art. 5, par. 1, lett. *e*), del RGPD). Sul punto, anche in questa sede è stata richiamata la specifica disciplina di settore in base alla quale i dati personali raccolti specificatamente per uno scopo statistico possono essere trattati dai soggetti che fanno parte o partecipano al Sistan per altri scopi statistici di interesse pubblico e previsti da una specifica base normativa, quando questi ultimi sono chiaramente determinati e di limitata durata. Tale eventualità deve essere chiaramente rappresentata agli interessati al momento della raccolta o, quando ciò non sia possibile, resa preventivamente nota al pubblico e al Garante nei

modi e nei termini previsti dalle regole deontologiche (art. 6-*bis*, comma 4, d.lgs. n. 322/1989; cfr. provv. 19 maggio 2020, n. 87, doc. web n. 9370217).

Il Garante ha poi evidenziato che l'ulteriore conservazione dei dati per scopi statistici debba trovare una più compiuta disciplina nelle regole deontologiche di settore che verranno adottate ai sensi dell'art. 2-*quater* del Codice; ciò in quanto, nel provvedimento recante le regole deontologiche, l'Autorità ha ritenuto incompatibile con il Regolamento l'art. 11 del previgente codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifici effettuati nell'ambito del Sistema statistico nazionale (all. A.3 al Codice), che indicava i casi in cui si ritenevano ammissibili ulteriori periodi di conservazione dei dati (art. 106, par. 2, lett. *b*), del Codice). Pertanto è stato rilevato che, nella maggior parte dei casi, le motivazioni relative all'ulteriore conservazione indicate nei prospetti informativi, che fanno ancora riferimento all'art. 11 dell'abrogato codice di deontologia, non sempre soddisfano i requisiti di specificità richiesti dal rinnovato quadro normativo.

Su tali basi è stato quindi formulato un formale avvertimento ai sensi dell'art. 58, par. 2, lett. *a*), del RGPD, affinché, nelle more del completamento del richiamato quadro normativo di riferimento, la definizione e la conseguente corretta rappresentazione dei tempi di ulteriore conservazione siano espressamente indicati nelle informative agli interessati, nel Psn o, quando ciò non sia possibile, rese preventivamente note al Garante.

Nel provvedimento in esame, con riferimento all'utilizzo dei sistemi informativi e dei registri, è stato rilevato che nel Psn si continua a fare riferimento al cd. Sistema integrato dei registri (Sir) (che dovrebbe comporsi di almeno 4 registri statistici di base) senza però specificare cosa si intenda con tale locuzione. Sul punto, il Garante ha evidenziato come il riferimento a sistemi e modalità di trattamento dei dati in nessun modo esplicitati costituisca un ulteriore elemento di criticità rispetto alla necessaria chiarezza espositiva dell'atto che sovente rende imprevedibili per gli interessati le tipologie di trattamenti di dati personali effettuati (cons. 41 del RGPD), avvertendo formalmente l'Istat della necessità che le modalità di trattamento dei dati nell'ambito dei sistemi informativi statistici siano rappresentate nei richiamati prospetti informativi in maniera chiara e comprensibile per gli interessati.

Nel corso dell'istruttoria è stato nuovamente affrontato il tema del cd. obbligo di risposta. Al riguardo il Garante ha evidenziato come la corretta rappresentazione della sussistenza dell'obbligo di risposta incida in maniera determinante sull'effettiva applicazione dei principi di trasparenza e correttezza che devono informare i trattamenti di dati personali (art. 5, par. 1, lett. *a*), del RGPD).

Su tali basi, l'Autorità ha preso favorevolmente atto, in primo luogo, della scelta dell'Istituto di omettere l'indicazione dell'obbligo di risposta nei prospetti informativi relativi ai singoli lavori statistici che prevedono la raccolta di dati presso tutte le amministrazioni, enti e organismi pubblici, essendo tale obbligo previsto per legge e rappresentato nella sezione introduttiva del Psn (cfr. art. 7, d.lgs. n. 322/1989; punto 1.5, capitolo 1, volume 2 del Psn). In secondo luogo, è stata condivisa l'intenzione dell'Istat di indicare, nei prospetti informativi destinati ai soggetti privati, la sussistenza o meno dell'obbligo di risposta, accompagnata dall'indicazione dell'eventuale applicazione di una sanzione amministrativa in caso di mancato riscontro. Si è preso atto, infine, del fatto che i prospetti informativi correttamente indichino le ipotesi in cui, per esplicito dettato normativo, l'interessato è obbligato a fornire anche dati inerenti alle particolari categorie di cui agli artt. 9 e 10 del RGPD, laddove in linea generale, come pure indicato nei prospetti, in assenza di una specifica previsione normativa, tale obbligo per queste categorie di dati non sussiste.

Sempre nell'ottica della corretta applicazione del principio di trasparenza, l'Au-

torità, in coerenza con quanto già sottolineato nel richiamato provvedimento del 13 febbraio 2020 (cfr. *supra* punto 1.2.1), si è riservata di svolgere specifici approfondimenti sulle modalità di realizzazione delle cd. statistiche da indagine, al fine di garantire l'effettiva applicazione del principio di autodeterminazione informativa, soprattutto nei casi in cui la rilevazione sia accompagnata dall'obbligo di risposta o preveda il trattamento di particolari categorie di dati.

È stata osservata con favore, infine, la scelta di rimuovere dalle schede informative la distinzione tra dati pseudonimizzati, dati personali e dati identificativi diretti (talvolta recante la precisazione che "I dati che identificano direttamente gli interessati sono cancellati al termine del trattamento"). A tale riguardo, l'Autorità ha precisato che il concetto di dato personale è riferibile tanto a dati cd. in chiaro quanto a quelli pseudonimizzati e che i criteri per la valutazione del rischio di reidentificazione degli interessati, indicati nel cons. 26 del RGPD, rendono di fatto superata la distinzione tra dato personale e dato identificativo diretto. In questi termini, peraltro, si è già espresso il Garante al punto 2 della premessa del provvedimento recante le regole deontologiche per i trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (all. A4 al Codice).

7.2.4. Parere su ulteriori lavori statistici sospesi con il provvedimento del 9 maggio 2018

Con provvedimento del 17 dicembre 2020, n. 270 (doc. web n. 9523274), il Garante ha reso parere favorevole sui lavori IST-02742 Registro del lavoro; IST-02634 Registro esteso dell'occupazione nelle imprese (Asia occupazione); IST-01382 Registro Annuale su retribuzioni, ore e Costo del Lavoro Individuale; IST-02748 Archivio disabilità; IST-02726 Indagine sulle discriminazioni; l'IST-02645 Quantificazione delle popolazioni in ambiti territoriali potenzialmente a rischio, precedentemente sospesi con il parere sullo schema di Psn 2017-2019, Aggiornamento 2018-2019, del 9 maggio 2018. Sulla base della documentazione trasmessa, l'Autorità ha potuto verificare la necessità e proporzionalità dei trattamenti di dati personali previsti per la realizzazione di tali lavori nonché l'adeguatezza – salve talune specifiche prescrizioni relative alle tecniche di pseudonimizzazione – delle misure implementate a tutela dei diritti e delle libertà fondamentali degli interessati.

Nel provvedimento in esame il Garante si è soffermato sul tema della conservazione nel pubblico interesse di dati raccolti per fini statistici. Al riguardo l'Istituto aveva manifestato l'intenzione di protrarre *sine die* la conservazione di alcune delle informazioni, anche di carattere personale, raccolte per i predetti scopi, riversandole in un archivio storico, per finalità sia di ricerca scientifica dell'Istat sia di archiviazione nel pubblico interesse. Ciò anche alla luce della presunzione di non incompatibilità dell'ulteriore trattamento a fini di ricerca scientifica e di archiviazione nel pubblico interesse con lo scopo della raccolta (art. 5, par. 1, lett. *b*), del RGPD).

In base alle normative rilevanti in materia di statistica ufficiale e di protezione dei dati personali, sono state rilevate specifiche criticità.

In primo luogo, è stato evidenziato come, in virtù del segreto statistico e del divieto di trattare i dati raccolti per scopi statistici per finalità differenti, "i dati raccolti nell'ambito di rilevazioni statistiche comprese nel programma statistico nazionale da parte degli uffici di statistica non possono essere esternati se non in forma aggregata, in modo che non se ne possa trarre alcun riferimento relativamente a persone identificabili e possono essere utilizzati solo per scopi statistici" (art. 9, d.lgs. n. 322/1989). Nel rispetto del richiamato divieto, la normativa statistica assicura in ogni caso la massima conoscibilità a "dati elaborati nell'ambito delle rilevazioni statistiche comprese nel programma statistico nazionale" definendoli come "patrimonio della collettività" e prevedendo che siano "distribuiti per fini di studio e di ricerca

a coloro che li richiedono secondo la disciplina del presente decreto" e nel rispetto dei richiamati divieti (art. 10, commi 1 e 2, d.lgs. n. 322/1989 e art. 5-*ter*, d.lgs. 14 marzo 2013, n. 33).

In secondo luogo, è stata richiamata la disciplina vigente, in base alla quale il trattamento dei dati per uno scopo ulteriore rispetto a quello della raccolta si presume in generale con esso non incompatibile se volto al perseguimento di finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, par. 1, del RGPD. In maniera speculare, i dati possono essere conservati per periodi più lunghi rispetto a quelli necessari al perseguimento dello scopo primario della raccolta, a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nel rispetto di adeguate garanzie (artt. 5, par. 1, lett. *b*) e *e*) e 89 del RGPD).

Infine, è stato richiamato l'art. 105 del Codice che esclude espressamente, coerentemente con la disciplina di settore, che i dati personali trattati a fini statistici o di ricerca scientifica possano essere utilizzati per scopi di altra natura. In altri termini, se è vero che i dati personali raccolti per un determinato scopo si presume che possano essere ulteriormente trattati per finalità statistiche, di ricerca statistica e di archiviazione nel pubblico interesse, è invece vietato trattare i dati personali raccolti per finalità statistiche e di ricerca scientifica, per il perseguimento di finalità differenti, ivi incluse quelle di archiviazione nel pubblico interesse e di ricerca storica.

Su tali basi, il Garante ha precisato come, seppure l'Istat, quale istituto pubblico, in base al codice dei beni culturali (d.lgs. 22 gennaio 2004, n. 42, codice dei beni culturali e del paesaggio, ai sensi dell'art. 10, legge 6 luglio 2002, n. 137), abbia l'obbligo di conservare i propri documenti, secondo quando quanto ivi indicato, tale obbligo non può, tuttavia, riguardare anche i dati di carattere personale raccolti per scopi statistici che possono però essere conservati in forma anonima e aggregata tale per cui non sia possibile in alcuno modo risalire all'identità dei soggetti interessati.

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

8.1. *I trattamenti in ambito giudiziario*

Produzione di dati in giudizio

Diversi reclami hanno riguardato la conformità alla normativa in materia di protezione dei dati della produzione in giudizio delle informazioni personali. Secondo un consolidato orientamento, l'Ufficio ha precisato che spetta al Giudice, ove ritualmente richiesto, la competenza a valutare la liceità del trattamento in giudizio dei dati personali dell'interessato. Ciò in quanto l'art. 160-*bis* del Codice stabilisce che la validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non 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* del Codice: provv.ti 23 settembre 2010, doc. web n. 1756065; 4 novembre 2010, doc. web n. 1770943 e 17 novembre 2010, doc. web n. 1779765).

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

L'Autorità è stata interessata della vicenda di un invio, da parte dell'avvocato dell'ex coniuge del reclamante, della costituzione in mora riguardante gli assegni per il nucleo familiare, anche al datore di lavoro dell'interessato. All'esito dell'istruttoria svolta, l'Autorità ha precisato che tale invio è avvenuto sulla base di valutazioni professionali proprie del legale, al quale occorre riconoscere, in principio, un diritto di scelta della strategia difensiva da utilizzare, tenuto conto che una troppo rigida restrizione finirebbe per contrastare il libero svolgimento dell'attività di assistenza legale. Pertanto, anche in base al RGPD che legittima il trattamento persino di particolari categorie di dati se "necessario per accertare, esercitare o difendere un diritto in sede giudiziaria" (cfr. art. 9, par. 2, lett. *f*), del RGPD), non si sono ravvisati, allo stato degli atti, gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali (nota 21 luglio 2020).

In altra vicenda si è lamentato l'invio da parte di un avvocato, per conto di un erede legittimo, di copia integrale di un testamento concernente anche un immobile ad un soggetto poi risultato acquirente dell'immobile medesimo. Anche in questo caso, dall'esame della documentazione prodotta dinanzi all'Autorità e tenuto conto altresì di quanto sancito dall'art. 168 del Codice (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante), la comunicazione del testamento in questione è risultata essere avvenuta sulla base di valutazioni professionali del legale e, pertanto, anche in considerazione di quanto sancito dall'art. 9, par. 2, lett. *f*), del RGPD, non si sono ravvisati gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali (nota 3 agosto 2020).

Consegna di documentazione a seguito di revoca del mandato professionale

È pervenuto un reclamo a mezzo del quale si lamentava che, a seguito di revoca e rinuncia al mandato professionale, mediante una persona terza un avvocato aveva tentato di riconsegnare ad un familiare della reclamante la documentazione relativa ai giudizi seguiti, ivi compreso un elenco della documentazione contenuta nelle relative buste, in cui erano visibili le procedure penali con numeri, gli RG, gli RGNR, le denunce penali presentate, gli atti di precetto, le opposizioni, le esecu-

zioni immobiliari, etc. Con il medesimo reclamo l'interessata ha altresì lamentato l'invio da parte del medesimo professionista di un messaggio privato indirizzato a persona terza in cui si riportavano informazioni personali riferite alla stessa. Nel corso dell'istruttoria, l'avvocato ha dichiarato e documentato di essersi impegnato alla restituzione tramite corriere della documentazione suddetta, che non è stata ritirata né dall'interessata né dai suoi familiari, di talché ha provveduto a consegnarla presso l'Ordine professionale. Il professionista ha altresì rappresentato che il corriere era un operatore professionale che cura le consegne a domicilio e che aveva tentato di consegnare la documentazione di ogni singola posizione racchiusa in plichi sigillati, ognuno indirizzato al proprio destinatario e che l'elenco era stato redatto per ogni singola posizione e consegnato in busta chiusa al corriere per farlo sottoscrivere ad ogni singolo destinatario. Dall'esame della documentazione prodotta e tenuto conto di quanto sancito dall'art. 168 del Codice, non sono stati ravvisati gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali. Inoltre, quanto all'invio del messaggio privato da parte dell'avvocato a persona terza, esso non configura alcuna violazione della disciplina in materia di protezione dei dati personali, tenuto conto che ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività esclusivamente personale non si applicano le disposizioni contenute nel RGPD (cfr. art. 2, par. 2, lett. *c*), del RGPD) (nota 22 ottobre 2020).

Comunicazioni tra avvocato e assistito

L'Autorità si è occupata di un reclamo a mezzo del quale si è lamentato l'invio da parte dell'Avvocatura dello Stato ad un comune di osservazioni presentate all'Avvocatura medesima dal reclamante, dopo esser venuto a conoscenza che il consiglio comunale aveva respinto l'opposizione ad una precedente delibera sulla base di un parere espresso dall'Avvocatura dello Stato. Nella vicenda in esame si è rappresentato che la corrispondenza tra l'avvocato ed il proprio assistito, sottoposta a segreto professionale e sottratta al diritto di accesso (v. art. 2, d.P.C.M. n. 200/1996, recante le norme per la disciplina di categorie di documenti formati o comunque rientranti nell'ambito delle attribuzioni dell'Avvocatura dello Stato sottratti al diritto di accesso), legittimamente può avere ad oggetto informazioni ricevute dall'avvocato – anche se contenute in una nota "riservata", ciò che peraltro non si è potuto verificare dagli atti trasmessi all'Autorità – in relazione ad una vicenda che vede coinvolto il proprio assistito. Nella fattispecie, pertanto, la lamentata comunicazione con cui l'Avvocatura avrebbe messo a disposizione del comune le osservazioni del reclamante è risultata pertinente e legittima e non si sono ravvisati gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali (nota 26 ottobre 2020).

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

Il Garante ha adottato un provvedimento di limitazione provvisoria nei confronti di un comune con riferimento al progetto di un sistema di videosorveglianza con funzioni di riconoscimento facciale da installare presso l'area verde antistante la principale stazione ferroviaria cittadina; tale sistema mirava a consentire al Nucleo di polizia giudiziaria della polizia locale l'individuazione sia di persone oggetto di indagine e/o scomparse al passaggio nell'area sottoposta a controllo, sia di situazioni sospette (*loitering*) o potenzialmente pericolose (abbandono di oggetti), come pure la rilevazione automatica di furti di oggetti o, ancora, il monitoraggio di ingressi/uscite da aree di interesse per attività di indagine. Premesso che il trattamento in questione riguardava dati biometrici – ossia dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali

di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale – e che per le finalità indicate tale trattamento rientra nel campo di applicazione del d.lgs. 18 maggio 2018, n. 51, il Garante ha precisato che la raccolta di dati biometrici può effettuarsi solo in presenza di un'idonea previsione normativa, come stabilito dall'art. 7 del menzionato decreto legislativo, allo stato, non sussistente (provv. 26 febbraio 2020, n. 54, doc. web n. 9309458).

Il Garante ha adottato un provvedimento prescrittivo e sanzionatorio nei confronti del Ministero dell'interno per l'illecito trattamento di dati personali da parte di una questura che, nelle comunicazioni istituzionali relative all'adozione di un provvedimento di ammonimento per atti persecutori (ex art. 8, d.l. 23 febbraio 2009, n. 11), aveva erroneamente indicato che l'interessato era stato destinatario di un ammonimento orale per condotta violenta. Nonostante le ripetute richieste di rettifica da parte dell'interessato e la richiesta di informazioni formulata dal Garante, il questore pro tempore ha ritenuto di non provvedere alla rettifica dei dati errati, considerando sufficiente che le informazioni inserite presso il Ced del Dipartimento della pubblica sicurezza fossero corrette, con la conseguenza della perdurante erroneità dei dati presso i destinatari delle comunicazioni, come accertato in sede istruttoria. Solo a distanza di oltre un anno dalla richiesta di rettifica dell'interessato e successivamente alla comunicazione dell'avvio del procedimento del Garante, il questore nel frattempo subentrato nell'incarico ha provveduto ad inviare ai destinatari delle predette comunicazioni una nota di rettifica dei dati. Il Garante ha pertanto accertato per il pregresso la violazione degli artt. 3, comma 1, lett. *a*) e *d*) (che stabiliscono che i dati personali devono essere trattati in modo lecito e corretto, esatti e, se necessario, aggiornati e devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati), 4, comma 3 (secondo cui, quando i dati personali sono stati trasmessi illecitamente o sono inesatti, il destinatario ne è tempestivamente informato e i dati personali devono essere rettificati o cancellati o il trattamento deve essere limitato) e 12, comma 1 (che riconosce all'interessato il diritto di ottenere dal titolare del trattamento, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che lo riguardano), del d.lgs. n. 51/2018. Di conseguenza, ha ingiunto al Ministero dell'interno, in qualità di titolare del trattamento, di pagare la somma di euro 50.000 a titolo di sanzione amministrativa pecuniaria e ha prescritto, ai sensi dell'art. 37, comma 2, lett. *b*), d.lgs. n. 51/2018, di valutare l'opportunità di promuovere adeguate iniziative formative nei confronti del personale, anche periferico, della Polizia di Stato, per assicurare il rispetto dei diritti degli interessati e la tempestiva rettifica dei dati inesatti, nonché di riferire al Garante l'esito di tale valutazione (provv. 29 ottobre 2020, n. 205, doc. web n. 9493020).

Divulgazione di immagini autolesionistiche all'interno di un commissariato

L'Autorità ha adottato un provvedimento prescrittivo e sanzionatorio nei confronti del Ministero dell'interno per l'illecito trattamento di dati personali da parte di un commissariato di polizia a seguito della diffusione in internet delle immagini di un episodio di violenta reazione autolesionistica da parte di un uomo in evidente stato di alterazione psico-fisica mentre era sottoposto ad arresto all'interno del medesimo commissariato. Dall'istruttoria svolta è emerso che la diffusione è stata resa possibile dalla mancanza di ogni misura idonea a proteggere i dati in questione, risultando così violate le disposizioni relative alla loro conservazione, alla compatibilità del trattamento con le finalità per cui erano stati raccolti, alla non eccedenza, all'adeguata sicurezza e protezione da trattamenti non autorizzati ed alle adeguate garanzie per i diritti e le libertà dell'interessato richieste per le particolari categorie di dati (artt. 3 e 7, d.lgs. n. 51/2018). È stato pertanto ingiunto al Ministero dell'interno, in qualità di titolare del trattamento, di pagare la somma di euro 60.000 a titolo

di sanzione amministrativa pecuniaria e prescritto, ai sensi dell'art. 37, comma 2, lett. *b*), d.lgs. n. 51/2018, di valutare l'opportunità di promuovere adeguate iniziative formative nei confronti del personale, anche periferico, della Polizia di Stato, per assicurare il rispetto dei diritti degli interessati, nonché di valutare se intraprendere ulteriori iniziative in materia di protezione dei dati personali, in conformità agli artt. 3 del decreto del capo della polizia del 23 luglio 2019 e 14, comma 3, d.P.R. n. 15/2018 (provv. 26 novembre 2020, n. 236, doc. web n. 9522206).

8.3. *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 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 continuata l'attività relativa all'attuazione delle raccomandazioni ricevute in esito alla valutazione sui trattamenti di dati personali effettuati in applicazione dell'*acquis* di Schengen svoltasi nel 2016 e sono state altresì poste in essere le prime iniziative finalizzate alla prossima nuova valutazione che si svolgerà nel mese di settembre del 2021, seppur con i limiti imposti dalle restrizioni disposte ai fini di contrasto della pandemia da Covid-19.

Esercizio dei diritti per i dati registrati nel SIS II

Come noto, il Codice ha introdotto nuove modalità di esercizio dei diritti rispetto ai dati registrati nel SIS II, in virtù dei quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale dell'archivio Schengen, ossia al Dipartimento della pubblica sicurezza (cd. accesso diretto). Al riguardo, il Ministero invia trimestralmente *report* statistici, privi di dati di natura personale, contenenti 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, in conformità con la raccomandazione formulata all'esito della precedente valutazione sull'applicazione dell'*acquis* di Schengen.

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

Nel corso del 2020, con ogni evidenza anche in ragione della pandemia da Covid-19, si è assistito ad un parziale calo del numero delle richieste degli interessati indirizzate direttamente al Garante rispetto all'anno precedente; tra queste poi sono risultate costanti in termini percentuali quelle di interessati i quali lamentano un insoddisfacente o erroneo riscontro alle proprie richieste da parte dell'autorità nazionale di polizia e, pertanto, ricorrono al Garante al fine di vederle soddisfatte.

Infine, anche qui con ogni probabilità in conseguenza della pandemia, si è assistito ad un moderato ma costante calo delle richieste di accesso da parte di autorità nazionali di controllo di altri Stati UE, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane.

Le relative informazioni vengono comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni di cui all'art. 62 della decisione 2007/533/GAI del Consiglio e all'art. 46 del regolamento (CE) n. 1987/2006.

9 L'attività giornalistica

9.1. *Premessa*

L'attività dell'Autorità, con riguardo ai profili attinenti alla tematica della libertà di manifestazione del pensiero, si è arricchita di nuovi spunti e riflessioni, in parte legate alle contingenze connesse alla pandemia, che hanno consentito di valutare il livello di adeguatezza dei trattamenti di dati personali in ambito giornalistico con riferimento ai principi dettati dalle norme che ne contengono la disciplina.

Anzitutto l'emergenza sanitaria ha inciso sui diritti fatti valere innanzi al Garante, traducendosi in molteplici reclami e segnalazioni diretti a lamentare l'avvenuta diffusione, sia attraverso articoli di giornale che tramite *social network*, di informazioni eccedenti riguardanti persone risultate positive al Covid-19. In considerazione della delicatezza dei dati trattati si è provveduto, oltreché ad avviare un'istruttoria nei casi nei quali si sono ravvisati gli estremi di una violazione, anche a predisporre un comunicato stampa – poi pubblicato nel sito istituzionale con il titolo "Coronavirus: Garante *privacy*, su *social* e *media* troppi dettagli sui malati" – al fine di arginare un fenomeno che sembrava destinato ad assumere proporzioni molto ampie, anche in considerazione del clima di forte preoccupazione destata dalla particolare situazione. Attraverso il comunicato si è voluto evidenziare che, anche nel contesto emergenziale, debbano comunque essere preservate alcune garanzie a tutela della riservatezza e della dignità delle persone e che tale obbligo riguardi non solo i giornalisti professionisti, ma anche gli utenti dei *social network*, a partire da alcuni amministratori locali che, pensando forse di fornire informazioni utili per la collettività di riferimento, hanno spesso diffuso i dati personali di persone decedute o contagiate senza valutare compiutamente le conseguenze per gli interessati e per le loro famiglie.

Un *focus* specifico si è poi aperto con riguardo al trattamento di dati contenuti all'interno di immagini, reali o frutto di manipolazione (come nel caso dei *fake*), ed ai limiti che la libera pubblicazione incontra sia nell'ambito della cronaca giornalistica – approfondendo, in particolare, le questioni connesse alla diffusione di immagini di persone ritratte in uno stato di costrizione e/o di alterazione – sia, ancora una volta, nel mondo dei *social network*, nel quale si è assistito alla proliferazione di episodi di pubblicazione di fotografie in assenza di consenso o comunque in conflitto con i principi desumibili dalle norme vigenti in materia di libertà di manifestazione del pensiero, come si è in particolare potuto rilevare con riguardo all'ampio utilizzo di immagini riferite a minori.

9.2. *Dati statistici ed aspetti procedurali*

Le richieste pervenute all'Autorità hanno incluso in modo pressoché equivalente, in termini numerici, reclami e segnalazioni. Queste ultime raccolgono sia richieste riguardanti in via diretta gli interessati, analogamente a quanto avviene con i reclami, sia denunce di condotte illecite dai contorni più ampi rispetto alle quali compete all'Autorità la valutazione circa la sussistenza dei presupposti per l'avvio di un'istruttoria. Ciò si è verificato, ad esempio, con riferimento a segnalazioni riguardanti la

diffusione di dati riferiti a minori, in particolare tramite i *social network*, spesso usati strumentalmente nell'ambito di contese familiari ovvero per il perseguimento di scopi non sempre in linea con la necessità di promuovere uno sviluppo equilibrato dei medesimi secondo le indicazioni contenute all'interno della Carta di Treviso, aspetto quest'ultimo spesso rilevato anche da associazioni che svolgono attività dirette alla tutela di cittadini e consumatori.

L'esame dei reclami invece, in larga parte orientati all'esercizio dei diritti di cui agli artt. 15-22 del RGPD, ha consentito, in alcuni casi, di consolidare orientamenti già propri dell'Autorità – in particolare, nell'ambito delle richieste di *delisting* da motore di ricerca – e in altri di ampliare i confini della tutela riconosciuta all'interessato attraverso un'interpretazione più stringente di ciò che può essere ritenuto essenziale al fine di soddisfare la finalità informativa insita nell'esercizio del diritto di cronaca giornalistica.

Si tratta di un approccio che, dato l'alto numero di adesioni spontanee alle richieste manifestato dai titolari del trattamento, risulta presumibilmente condiviso anche da parte di questi ultimi benché in alcune ipotesi possa rilevarsi un disallineamento con il riscontro fornito dagli stessi agli interessati in fase di interpello preventivo, anche nei casi in cui quest'ultimo preceda di poco, da un punto di vista temporale, la proposizione del reclamo. Sulla base delle casistiche emerse, l'Autorità ha curato, con specifico riguardo ad alcuni titolari, attività di approfondimento finalizzate a stimolare una più puntuale conformità, con riguardo ai tempi ed alle modalità di risposta, alle indicazioni contenute nel Regolamento.

Una parte dei reclami, pari a circa un quarto delle richieste pervenute, ha invece portato all'adozione di decisioni collegiali che, attraverso l'esame degli elementi specifici di ogni vicenda, si sono espresse sulla fondatezza della doglianza prospettata, ricorrendo spesso ad un bilanciamento tra le istanze del singolo e l'interesse pubblico generale all'informazione e facendo ricorso ai poteri correttivi, ivi incluso quello sanzionatorio, riconosciuto dal Regolamento alle autorità di controllo. Nei casi più gravi il Garante ha ritenuto di applicare, a fini dissuasivi rispetto alla reiterazione della condotta giudicata illecita, anche misure sanzionatorie di tipo pecuniario (provv. 6 febbraio 2020, n. 28, doc. web n. 9283121); tale scelta è stata determinata dalla particolare gravità delle violazioni contestate, oltreché dalla durata delle stesse, pur dovendosi tenere conto del fatto che, in generale, è necessario calibrare con attenzione questo nuovo potere in un settore particolare quale quello della libertà di manifestazione del pensiero.

Le doglianze presentate dagli interessati hanno riguardato, in continuità con il 2019, l'avvenuta 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; 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; infine 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, sia stata ritenuta non più rispondente alla situazione attuale della medesima ed al conseguente interesse del pubblico a disporre delle relative informazioni.

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

9.3.1. Dati giudiziari

Il trattamento di dati giudiziari nel contesto dell'informazione, da intendersi in tutte le sue declinazioni, è uno dei temi sui quali maggiormente si è concentrato l'impegno dell'Autorità e ciò in ragione della particolare delicatezza dei dati in questione – la cui tutela è stata peraltro rafforzata dall'art. 10 del RGPD – e del fatto che in tale ambito siano state frequentemente riscontrate condotte palesemente illecite o verosimilmente tali.

Occorre ricordare che il giornalista ed il suo editore sono chiamati, anteriormente alla pubblicazione di informazioni, a condurre una valutazione in ordine alla correttezza del relativo trattamento sulla base delle norme che regolano il settore e che, proprio al fine di non comprimere l'esigenza informativa connessa alla circolazione di certi contenuti, già contengono in sé una maggiore flessibilità rispetto a quanto invece avviene con riguardo ad altre tipologie di trattamento. Ma ciò non consente la diffusione di notizie senza alcun filtro, adducendo quale giustificazione, come spesso si è verificato, la circostanza che le medesime notizie siano già state rese disponibili in rete da altre testate giornalistiche o *blog* o che siano state comunque divulgate da fonti qualificate, come nel caso degli appartenenti alle Forze di polizia.

A tale riguardo, nel corso dell'anno l'Autorità ha concluso un'istruttoria avviata nel 2019 a seguito dell'adozione, in via d'urgenza, di una serie di provvedimenti di limitazione provvisoria del trattamento attraverso i quali è stata inibita ai titolari coinvolti l'ulteriore propalazione 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 (*ex multis*, provv. 25 marzo 2019, n. 73, doc. web n. 9114416). In tale occasione è stata in particolare contestata la diffusione di immagini avvenuta 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, e quindi in presumibile violazione della disciplina applicabile (cfr. art. 137, comma 3, del Codice e art. 8, comma 1, delle regole deontologiche). Tale valutazione è stata confermata anche a seguito dello svolgimento dell'istruttoria e dell'esame delle difese prodotte dagli editori dalle quali è emerso che la ragione ricorrentemente dedotta da questi ultimi quale presupposto del trattamento effettuato fosse la necessità di documentare quanto realmente avvenuto all'interno del commissariato al fine di tutelare gli agenti presenti da eventuali successive accuse di maltrattamenti da parte del protagonista, tenuto conto di diversi gravi fatti verificatisi in epoca recente con riguardo ad interazioni avvenute tra cittadini ed appartenenti alle Forze di polizia.

L'Autorità, pur riconoscendo l'utilità per la collettività di conoscere la vicenda considerata nel suo complesso, ha comunque ritenuto che, nel caso specifico, si fosse verificata un'eccedenza informativa, lesiva dei diritti dell'interessato; di qui il divieto di ulteriore trattamento dei dati del medesimo con modalità tali da consentirne un'agevole identificazione – eccettuata la mera conservazione degli stessi per fini giudiziari – ed il provvedimento di ammonimento dei titolari coinvolti in relazione all'esigenza di adeguarsi integralmente alle disposizioni previste in materia di trattamento dei dati in ambito giornalistico, con particolare riguardo alle misure da adottare per salvaguardare la riservatezza e la dignità degli interessati (*ex multis*, provv. 26 novembre 2020, n. 246, doc. web n. 9531858). L'Autorità ha in parallelo agito, tramite iniziative del competente Dipartimento, indagando sulle modalità e finalità di trattamento dei medesimi dati da parte delle Forze di polizia – che spesso costituiscono la fonte primaria delle informazioni poi veicolate tramite gli organi di

stampa – al fine di stigmatizzare eventuali condotte non rispettose delle norme di settore, peraltro molto stringenti, che indicano le ragioni tassative in funzione delle quali la diffusione di categorie particolari di dati possa reputarsi lecita.

In considerazione del significativo impatto che la divulgazione di dati riguardanti le vicende giudiziarie di una persona può avere sulla sua identità personale e sociale, risulta importante garantire che l'aggiornamento delle notizie veicolate all'opinione pubblica sia effettuato con modalità appropriate. Tale profilo è stato esaminato nell'ambito di una decisione adottata dall'Autorità su reclamo dell'interessata che, pur avendo in origine circoscritto la doglianza all'avvenuta pubblicazione delle sue generalità all'interno di un articolo di giornale che offriva un resoconto riguardo ad un procedimento penale nel quale era stata coinvolta, ha successivamente rilevato la carenza di aggiornamento delle notizie relativamente all'evoluzione giudiziaria avuta dal procedimento in questione. Il titolare del trattamento ha argomentato le proprie difese asserendo di aver assicurato la correttezza dell'informazione mediante la pubblicazione di articoli più recenti che risultavano correlati, all'interno del proprio sito, a quelli precedenti tramite apposito richiamo. Tuttavia il Garante ha ritenuto che un sistema archivistico di correlazione operante solo nel motore di ricerca interno al sito non fosse sufficiente a garantire un trattamento rispettoso dei principi di liceità, richiedendosi invece, in capo al titolare del trattamento, la predisposizione di un sistema idoneo a segnalare, nel corpo o a margine dell'articolo, la sussistenza di un seguito e di uno sviluppo della notizia (provv. 9 aprile 2020, n. 71, doc. web n. 9426173).

In questo settore c'è stato poi spazio per approfondire, alla luce degli effetti connessi alla diffusione di informazioni di tipo giudiziario, i limiti entro i quali può ritenersi consentita la perdurante reperibilità di notizie al di fuori dell'archivio *online* presente all'interno del sito web di un editore. Si tratta di un profilo che richiede un'attenta valutazione delle finalità originarie del trattamento effettuato tramite la pubblicazione di un articolo di giornale e del loro rapporto con le diverse finalità di archiviazione che ne giustificano la successiva conservazione. Anche tenendo conto delle indicazioni contenute nel RGPD, in particolare nell'art. 89, l'Autorità ha avuto modo di aggiungere nuovi spunti di riflessione rispetto a questo argomento che assume una connotazione particolare laddove le informazioni diffuse in rete riguardino un personaggio pubblico. Ciò è quanto avvenuto con riguardo ad alcuni reclami proposti da un medesimo interessato, noto personaggio del mondo politico ed imprenditoriale, che ha chiesto la rimozione e, in subordine, l'aggiornamento e la deindicizzazione di alcuni articoli che riportavano informazioni riguardanti una vicenda giudiziaria conclusasi con la sua assoluzione per insussistenza dei fatti contestati. Il Garante, pur non ritenendo integrati i presupposti per la rimozione degli articoli dagli archivi *online* degli editori – in quanto aventi valore di testimonianza documentale –, ha tuttavia ritenuto che l'originaria finalità connessa all'esercizio del diritto di cronaca, e dunque la perdurante ed indiscriminata diffusione dell'informazione al di fuori dei predetti archivi, non fosse più sussistente in considerazione del lasso di tempo decorso e dell'esito giudiziario avuto dalla vicenda (*ex multis*, provv. 10 dicembre 2020, n. 287, doc. web n. 9575055). Il diverso trattamento consistente nella conservazione degli articoli all'interno dell'archivio *online* del giornale risulta infatti specificatamente sorretto da una finalità di tipo documentaristico ed archivistico per perseguire la quale non si è ritenuto necessario consentire la perdurante diffusione delle informazioni tramite i motori di ricerca generalisti in quanto le stesse, pur se aggiornate, sono apparse pregiudizievoli per l'interessato. La protezione normativa dell'archivio storico giornalistico ha formato oggetto di specifica disciplina anche nell'ambito del RGPD che, pur ponendo a salvaguardia della sua integrità

alcune limitazioni con riguardo ai diritti esercitabili dagli interessati relativamente ai dati personali che li riguardino contenuti al suo interno, ha comunque previsto l'adozione di garanzie adeguate per i diritti e le libertà degli stessi mediante la predisposizione di misure tecniche ed organizzative che possano assicurare il rispetto del principio della minimizzazione dei dati (cfr. art. 89, par. 1, del RGPD).

9.3.2. Dati relativi a minori

Il rispetto delle garanzie a salvaguardia dei diritti dei minori previste dalle regole deontologiche (art. 7) e dalla Carta di Treviso continua a costituire una delle priorità del Garante nell'esame delle segnalazioni e dei reclami sottoposti alla sua attenzione.

Non di rado le richieste pervenute si inseriscono nell'ambito di vicende attinenti a rapporti conflittuali tra genitori o tra questi ultimi e istituzioni pubbliche – come nel caso di minori allontanati dal proprio ambiente familiare e affidati ai servizi sociali, rispetto ai quali la valutazione dell'Autorità richiede un attento bilanciamento tra il diritto alla riservatezza del minore e il diritto di critica riguardo ai provvedimenti giurisdizionali adottati e spesso evidenzia una sovrapposizione di competenze tra la propria e quella dell'Autorità giudiziaria. L'Autorità ha garantito in ogni caso la massima attenzione nell'effettuare verifiche e nel fornire indicazioni riguardo alle questioni che le sono state rappresentate.

Specifici provvedimenti contenenti un ammonimento nei confronti degli editori titolari del trattamento sono stati adottati dal Garante a fronte di pubblicazioni ritenute in contrasto con le disposizioni a tutela dei minori e accomunate dalla circostanza di riferirsi a minori la cui esposizione era collegata alla notorietà di un genitore in ragione del ruolo pubblico ricoperto. In tale occasione il Garante ha ricordato che le garanzie previste dalle regole deontologiche e dalla Carta di Treviso devono essere salvaguardate a prescindere dalla notorietà e rilevanza pubblica del genitore, anche nell'eventualità che sia lo stesso a rivelare informazioni relative ai figli (provv. 24 giugno 2020, n. 112, doc. web n. 9471155).

9.3.3. Inchieste giornalistiche

L'Autorità ha continuato a misurarsi con una complessa opera di bilanciamento tra i diritti della persona e la libertà di informazione, con particolare riguardo al cd. giornalismo di inchiesta e all'applicazione dell'art. 2 delle regole deontologiche nella parte in cui prevede alcune eccezioni alla regola dell'informativa – seppur semplificata – da rendere all'interessato al momento della raccolta dei dati, delimitando i confini nell'attività di acquisizione delle notizie ("il giornalista […] rende note la propria identità, la propria professione e le finalità della raccolta salvo che ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa; evita artifici e pressioni indebite") .

È su questa disposizione che in questi anni, si è basata la valutazione del Garante in merito ai sempre più diffusi servizi giornalistici, soprattutto televisivi, fondati su riprese e dichiarazioni raccolte con dispositivi nascosti, da parte di soggetti che celano la qualifica di giornalista o comunque la finalità giornalistica perseguita. Così è avvenuto per due servizi televisivi riconducibili alla stessa trasmissione televisiva in cui l'operatore, fingendo di richiedere la prestazione riconducibile alla professione dei reclamanti, ne ha raccolto le dichiarazioni, volte a documentare inchieste ritenute di interesse generale, la cui successiva diffusione è avvenuta – in virtù delle informazioni personali divulgate e delle modalità di ripresa – senza l'adozione di misure idonee a garantire l'anonimato degli intervistati.

In entrambi i casi (in uno dei quali, peraltro, i dati trattati attenevano alla sfera sessuale dell'interessata ed erano stati diffusi unitamente ad immagini riconducibili

ad un'attrice, ma con la voce della reclamante), oltre alla dichiarazione di illiceità del trattamento, è stata comminata una sanzione amministrativa pecuniaria (provv.ti 6 febbraio 2020, n. 28, doc. web n. 9283121 e 26 novembre 2020, n. 241, doc. web n. 9509558).

9.4. *Diffusione di dati personali sui* social network

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

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

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

Facebook

A tal riguardo si segnala il reclamo con cui un comandante della polizia locale di un piccolo comune ha lamentato una violazione della normativa in materia di protezione dei dati personali in relazione alla diffusione, tramite la pagina Facebook di una associazione, di due fotografie che lo ritraevano in servizio durante un evento pubblico. Il reclamante ha evidenziato, in particolare, che, benché gli scatti fotografici fossero stati effettuati durante una manifestazione in area pubblica e ritraessero una persona in divisa che riveste un ruolo pubblico, la loro diffusione su Facebook aveva una finalità denigratoria, finalizzata a strumentalizzazione politica, suscitando commenti ironici e allusivi. Ha chiesto perciò all'Autorità di ingiungere al titolare del trattamento di eliminare le suddette immagini.

Il titolare della pagina Facebook interessata dal reclamo ha replicato eccependo che le foto pubblicate nel *post* si inserivano nell'ambito di una serie di critiche rivolte all'amministrazione comunale ed alla gestione della polizia locale, ritraendo il comandante di quest'ultima mentre prestava servizio in divisa durante un evento ludico.

Il Garante, alla luce di quanto emerso nel corso dell'istruttoria e visto l'art. 97 della legge 22 aprile 1941, n. 633 (legge sulla protezione del diritto d'autore), ha dichiarato infondato il reclamo, ritenendo che nel caso in esame risultasse sussistente l'interesse pubblico, in quanto nelle foto è stato ritratto il reclamante, in divisa e nel corso di una manifestazione pubblica, in ragione del ruolo pubblico ricoperto, al fine di comprovare una critica nei confronti dell'amministrazione comunale quanto alla gestione della polizia locale (provv. 9 luglio 2020, n. 137, doc. web n. 9446627).

Segnalazioni e reclami sono pervenuti nei confronti di Facebook, in quanto in molti profili sono state riportate fotografie e video relativi a notizie già pubblicate da quotidiani e da altri organi di stampa. In particolare, la presidente di un comitato referendario nazionale ha chiesto di ordinare a Facebook la rimozione di un URL

9

contenente un'intervista rilasciata dalla stessa ad una rete televisiva. Sull'assunto che il video diffuso tramite la piattaforma *social* nel 2016 violasse i principi della normativa vigente in materia di protezione dei dati, in quanto frutto di una manipolazione e di un'alterazione dei contenuti dell'intervista, con scopi e intenti lesivi e denigratori nei suoi confronti.

Il Garante, alla luce di quanto emerso nel corso dell'istruttoria, ha dichiarato il reclamo infondato, ritenendo rientrante nella libertà di manifestazione del pensiero e, in particolare, nel diritto di critica, la riproduzione dei contenuti di tale intervista, anche con l'inserimento di commenti, senza che peraltro in essi si siano ravvisati elementi lesivi della dignità della persona o in contrasto con i principi dell'essenzialità dell'informazione (provv. 24 giugno 2020, n. 108, doc. web n. 9444496).

TikTok

In seguito a segnalazioni inviate all'Autorità da alcune associazioni di tutela dei consumatori relative a possibili problemi di sicurezza del *social media* TikTok, il Garante, nel gennaio 2020, ha segnalato al Comitato l'esigenza di un intervento coordinato fra le varie autorità europee. A seguito di tale richiesta, è stata istituita un'apposita *Task force* al fine di coordinare l'attività delle autorità europee nei confronti della società, la cui sede era all'epoca stabilita negli USA.

Allo stesso tempo, a livello nazionale, l'Autorità, dopo aver avviato a marzo una istruttoria volta a evidenziare una serie di trattamenti ritenuti non conformi alla normativa in materia di protezione dei dati personali, il 15 dicembre 2020 ha inviato una formale contestazione nei confronti di TikTok Inc. (USA) e di TikTok Technology Lt. (Ireland), contestando a quest'ultima la violazione di alcune disposizioni del Regolamento. Forti criticità sono state rinvenute quanto alle modalità di iscrizione al *social network*, le quali non assicurano adeguate forme di tutela dei minori; il divieto di iscrizione al di sotto dei 13 anni, stabilito dal *social network*, risulta infatti facilmente aggirabile una volta che si inserisca una data di nascita falsa. TikTok, di conseguenza, non impedisce ai più piccoli di iscriversi, né verifica che vengano rispettate le disposizioni nazionali che prevedono per l'iscrizione ai *social network* il consenso dei genitori o di chi ha la responsabilità genitoriale del minore che non abbia compiuto 14 anni. Inoltre, l'Autorità ha contestato le modalità con le quali l'informativa è fornita, il trasferimento dei dati all'estero, il periodo di conservazione degli stessi e il rispetto dei principi di *privacy by design* e *by default*.

Riguardo al profilo della competenza, va considerato che, solo in tempi successivi all'avvenuta contestazione, l'Autorità irlandese ha comunicato che TikTok Ireland debba essere considerato stabilimento principale ai sensi dell'art. 4, n. 16), del RGPD.

Anche in considerazione di un tragico evento che ha coinvolto una bambina di 10 anni – che avrebbe perso la vita dopo aver partecipato ad una "sfida" sul *social network* – ed ha suscitato grande allarme sociale, con interrogazioni parlamentari e richieste di informazioni rivolte anche al Garante, è stato adottato un provvedimento d'urgenza ai sensi dell'art. 66 del RGPD, contenente un ordine di limitazione del trattamento dei dati personali degli utenti di cui non è possibile accertare l'età ex art. 58, par. 2, lett. *f*), del RGPD (provv. 22 gennaio 2021, n. 20, doc. web n. 9524194).

TikTok Ireland, a seguito del provvedimento, ha instaurato una collaborazione con l'Autorità e ha dichiarato di adeguarsi all'ordine ricevuto, anche mediante apposita campagna mediatica di sensibilizzazione. In particolare, la Società ha deciso di inviare un messaggio "in *app*" a tutti gli utenti italiani, chiedendo loro di indicare di nuovo la data di nascita prima di continuare ad utilizzare il servizio. Sempre secondo quanto dichiarato da TikTok, una volta identificato un utente al di sotto dei 13 anni, la Società si è impegnata a rimuoverne l'*account* senza consentire l'effettuazione di nuovi tentativi. TikTok ha provveduto ad un miglioramento della funzione di se-

gnalazione che permette agli utenti di indicare la presenza sulla piattaforma di utenti minori di 13 anni (o presunti tali) e si è impegnata a prendere in considerazione, in prospettiva, la possibilità di ricorrere all'intelligenza artificiale come strumento aggiuntivo per supportare la verifica dell'età dell'utente.

Il provvedimento del Garante ha carattere temporaneo, essendo stato emanato secondo la procedura d'urgenza prevista dall'art. 66, par. 1, del RGPD. La data di scadenza inizialmente fissata al 15 febbraio 2021, è stata prorogata al 15 marzo 2021 al fine di consentire la valutazione delle misure predisposte da TikTok (provv. 11 febbraio 2021, n. 61, doc. web n. 9554603); a tale atto ha fatto poi seguito un nuovo provvedimento d'urgenza motivato dalle criticità rilevate con riguardo all'adeguatezza dei meccanismi previsti per la verifica dell'età anagrafica, concedendo anche in tal caso alla Società un termine, fissato al 22 aprile 2021, per ottemperare alle indicazioni fornite dall'Autorità (provv. 25 marzo 2021, n. 126, doc. web n. 9574709).

In seguito a tale provvedimento, l'Autorità ha richiesto indicazioni in ordine alle modalità di iscrizione e alle verifiche dell'età degli utenti anche rispetto ad altre piattaforme.

9.5. *Il trattamento dei dati da parte dei gestori dei motori di ricerca*

Il settore del trattamento di dati effettuato dai gestori dei motori di ricerca ha mantenuto un andamento costante, benché bilanciato da un incremento, rispetto all'analogo dato riferito all'anno 2019, dei reclami proposti direttamente nei confronti degli editori degli articoli oggetto di richiesta di deindicizzazione, circostanza indicativa di un rinnovato interesse dei reclamanti ad interagire direttamente con chi *ab origine* pubblica i dati al fine di ottenere misure idonee a limitare a monte la diffusione di informazioni personali.

La maggior parte delle richieste di *delisting* pervenute hanno riguardato trattamenti posti in essere tramite il motore di ricerca gestito da Google LLC, società nei confronti della quale l'Autorità può assumere decisioni autonome in quanto, nonostante la relativa attività sia ascrivibile ai trattamenti di tipo transfrontaliero (cfr. art. 4, n. 23), del RGPD), non opera nei suoi riguardi, per lo specifico settore del motore di ricerca, il meccanismo dello sportello unico (cfr. Relazione 2019, p. 111).

Diversa la situazione con riguardo invece a società che gestiscono altri motori di ricerca, quali Microsoft Corporation e Verizon Media – rispettivamente titolari dei motori di ricerca Bing e Yahoo! –, avendo le stesse individuato uno stabilimento principale nel territorio dell'Unione; ciò determina l'applicabilità del meccanismo di cooperazione, laddove non sia possibile definire la vicenda in una fase di preliminare contatto con il titolare e ferma restando 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.

Questa strada è stata intrapresa, in particolare, con riguardo ad un reclamo proposto da un'interessata per la rimozione di alcuni risultati reperibili in associazione al suo nominativo tramite il motore di ricerca Yahoo!; Verizon Media EMEA Ltd., rispetto alla quale l'Autorità ha provveduto ad inviare, analogamente a quanto avviene con gli altri gestori, una richiesta preliminare finalizzata a valutare la possibilità di definire la questione anteriormente all'attivazione del meccanismo di cooperazione, ha riscontrato la stessa invocando per la trattazione del reclamo la competenza della *Lead Authority* (qui l'Autorità irlandese), circostanza alla quale ha fatto seguito l'apertura della relativa procedura nell'apposita piattaforma utilizzata per la condivisione dei casi nel sistema IMI. Trattandosi di una fattispecie che, sulla base della

previsione contenuta nell'art. 56, par. 2, del RGPD, presentava specifici elementi di collegamento con la dimensione nazionale, l'Autorità ha avanzato la proposta di definire il reclamo a livello locale; tale proposta non ha trovato tuttavia accoglimento da parte dell'Autorità irlandese che ha invece rappresentato la necessità di valutare unitariamente i reclami aventi ad oggetto le richieste di rimozione, motivando la scelta alla luce dell'impatto che le relative decisioni producono sui criteri generali applicati per la valutazione. La posizione così assunta, sebbene possa trovare fondamento nel Regolamento, può tuttavia sollevare qualche problema nel caso di reclami "plurimi", ovvero proposti nei confronti di diversi gestori di motori di ricerca, la decisione dei quali sia rimessa ad autorità di controllo diverse, pur essendo identica la questione sottostante.

Con riguardo invece alle richieste avanzate nei confronti di Google occorre rilevare che circa la metà di esse sono state soddisfatte a seguito di un'adesione spontanea del titolare del trattamento successiva alla trasmissione del reclamo da parte dell'Autorità, mentre nei restanti casi si è provveduto tramite provvedimento collegiale. Le decisioni assunte dall'Autorità nel periodo di riferimento (circa 35) presentano, come tipologia, un numero più o meno equivalente di valutazioni di infondatezza – attraverso le quali sono stati per lo più confermati principi già enucleati nell'ambito di precedenti provvedimenti adottati con riguardo a questioni analoghe (provv.ti 2 luglio 2020, n. 127, doc. web n. 9445898 e n. 129, doc. web n. 9445947; 15 ottobre 2020, n. 193, doc. web n. 9513091 e n. 196, doc. web n. 9513224; 12 novembre 2020, n. 226, doc. web n. 9522184) – e di accoglimento, anche solo parziale, delle istanze avanzate dagli interessati.

Queste ultime hanno registrato la maggiore varietà di profili trattati – dai dati giudiziari ad informazioni personali riferite a periodi della vita passata ritenuti dall'interessato non più rispondenti alla sua attuale identità sociale – nell'affrontare i quali è stato fatto ricorso, in alcuni casi, anche alle indicazioni fornite dalla CGUE in alcune recenti decisioni (in particolare nella sentenza del 24 settembre 2019, causa C-136/17, GC, AF, BH, ED c. *Commission nationale de l'informatique et des libertés*, relativa al trattamento delle particolari categorie di dati di cui agli artt. 9 e 10 del RGPD).

Parte delle doglianze ha riguardato la perdurante reperibilità in rete di informazioni relative a vicende giudiziarie che hanno interessato il reclamante e che, in epoca successiva alla pubblicazione degli articoli indicati, hanno assunto contorni diversi in virtù dell'evoluzione dei relativi procedimenti. Il mancato aggiornamento degli articoli reperibili in rete è apparso idoneo a causare un particolare pregiudizio in capo al reclamante, in molti casi ritenuto non bilanciato da un interesse del pubblico alla perdurante conoscibilità dell'informazione. Ciò è quanto avvenuto nel caso di una richiesta di rimozione di URL collegati ad articoli riguardanti un procedimento giudiziario nel quale il reclamante era stato coinvolto nel 2010 conclusosi con una parziale assoluzione del medesimo con riferimento ad uno dei reati contestati e con la concessione del beneficio della sospensione condizionale della pena relativamente alla restante imputazione. Di tali circostanze sopravvenute non era stata tuttavia fatta alcuna menzione nei predetti articoli, né informazioni aggiornate in merito risultavano altrimenti reperibili in rete. Il Garante ha, in tal caso, accolto l'istanza (provv. 13 febbraio 2020, n. 34, doc. web n. 9308726) ritenendo che la specificità della vicenda meritasse un'attenta considerazione delle ragioni dell'interessato, benché sotto il profilo giudiziario vi fosse stata una parziale condanna del medesimo. Le notizie presenti all'interno degli articoli in questione erano infatti risalenti a diversi anni prima e descrivevano solo la fase inziale dell'indagine senza dare conto degli sviluppi successivi favorevoli al reclamante del quale emergeva pertanto una rappre-

sentazione inesatta e fuorviante. Ai fini della decisione si è tenuto particolare conto della posizione espressa dalla CGUE nella menzionata sentenza 24 settembre 2019, causa C-136/17, nella quale è contenuta un'attenta disamina dell'approccio che anche il gestore di un motore di ricerca deve adottare nel trattamento delle particolari categorie di dati individuate nel RGPD, tra le quali quelle riferite ai dati giudiziari di cui all'art. 10. Nell'ambito delle finalità per le quali è consentito il trattamento di dati personali da parte del gestore di un motore di ricerca rientra sicuramente quella di rendere possibile il reperimento di informazioni giudicate di interesse per il pubblico, ma tale aspetto dovrebbe essere necessariamente bilanciato con i diritti fondamentali dell'individuo, specie laddove si verta su profili particolarmente sensibili della sua vita. Quest'ultimo è l'aspetto sul quale si è incentrata maggiormente l'attenzione della Corte che, con riguardo ai dati giudiziari, ne ammette la divulgazione purché la stessa si riveli strettamente necessaria, precisando che, qualora la reperibilità di informazioni relative a fasi ormai superate di un procedimento giudiziale che abbia coinvolto l'interessato sia da ritenersi giustificata alla luce dell'interesse prevalente del pubblico, il motore di ricerca dovrà "sistemare l'elenco dei risultati in modo tale che l'immagine globale che ne risulta per l'utente di Internet rifletta la situazione giudiziaria attuale", ordinandoli quindi sulla base dei risultati di ricerca più recenti.

Tale indicazione risulta coerente con le caratteristiche del trattamento di dati personali effettuato dai motori di ricerca in quanto basato sull'aggregazione di informazioni che, per conformarsi ai principi di liceità del trattamento e per rispondere ad una reale utilità informativa, dovrebbero trovare corrispondenza con l'identità attuale della persona alla quale di riferiscono. Questa necessità ha portato l'Autorità ad effettuare, con riguardo a richieste di rimozione comprensive di contenuti collegati a vicende diverse relative ad un medesimo interessato, una valutazione multipla e differenziata in esito alla quale è stato disposto, in alcuni casi, un accoglimento parziale della relativa istanza, benché l'interesse pubblico alla conoscibilità delle informazioni complessivamente reperibili tramite i corrispondenti URL non potesse dirsi interamente superato. Ciò è quanto si è verificato nel caso di richieste riguardanti la rimozione di URL collegati ad articoli che davano conto di diverse vicende giudiziarie riferite alla stessa persona e non ancora completamente esaurite, per alcune delle quali non veniva tuttavia offerto un quadro completo ed aggiornato della situazione attuale della medesima. Si è rivelata determinante, ai fini della decisione, la presenza in rete di articoli ulteriori rispetto a quelli indicati dall'interessato che, riportando notizie integrate con informazioni riferite agli sviluppi giudiziari successivi, risultavano idonei a consentire una corretta ricostruzione dello svolgimento dei fatti, assicurando in tal modo anche l'interesse degli utenti della rete ad una corretta informazione (provv.ti 15 ottobre 2020, n. 195, doc. web n. 9513208 e 12 novembre 2020, n. 223, doc. web n. 9522159).

Quest'ultima finalità, in quanto connaturata alla fruibilità *online* di un'ampia quantità di notizie da parte del pubblico, dovrebbe godere del giusto peso nell'ambito del giudizio di bilanciamento condotto in occasione della valutazione della fondatezza delle richieste di rimozione avanzate dagli interessati. E proprio l'opportunità di preservare, in termini di attendibilità, la valenza informativa delle notizie disponibili in rete ha indotto l'Autorità a pronunciarsi, in alcune ipotesi, in favore delle predette richieste laddove le informazioni desumibili dal contenuto degli articoli contestati non risultavano idonee a veicolare informazioni utili all'utenza e ciò anche a prescindere dalla questione di merito sottostante. L'attenta ponderazione di questo aspetto ha portato il Garante ad accogliere la richiesta di rimozione di alcuni URL collegati ad articoli che riportavano, in parte, informazioni riguardanti vicende personali dell'interessato – ritenute di interesse per la collettività in considerazione del delicato

ruolo pubblico rivestito dal medesimo – ma poi superate dalla definizione delle stesse in sede giudiziale senza che di tale circostanza fosse stato dato conto all'interno degli articoli individuati nel reclamo, ed in parte informazioni legate ai presunti guadagni percepiti in relazione a corsi di formazione da lui effettuati ed i cui contenuti erano stati oggetto di giudizi critici da parte della stampa. Ampia parte degli articoli contenenti queste ultime informazioni, benché in astratto potessero ritenersi di interesse pubblico in quanto collegate ad un'attività ancora esercitata dal reclamante, non risultavano tuttavia visibili per la generalità degli utenti, ma solo per gli abbonati. Nella prospettiva della finalità tipica del trattamento effettuato tramite motore di ricerca, che è quella di restituire un profilo della persona in relazione alla quale viene effettuata la ricerca, tale circostanza è apparsa idonea a privare le pagine corrispondenti di una valenza informativa utile per il pubblico, nonché ad elidere uno dei parametri necessari per poter condurre il giudizio di bilanciamento richiesto dagli artt. 17, par. 1, lett. *c*), e 21, par. 1, del RGPD, determinando con ciò la prevalenza delle ragioni dell'interessato (provv. 10 dicembre 2020, n. 265, doc. web n. 9529506). Ai fini della decisione si è comunque tenuto conto del fatto che l'interesse del pubblico a disporre delle relative notizie restava comunque salvaguardato dalla presenza in rete di articoli completi ed aggiornati riguardanti i medesimi fatti. Nell'ambito del medesimo procedimento non si è invece ritenuto di accogliere la richiesta dell'interessato volta ad ottenere una rimozione globale degli URL indicati, ovvero estesa alle versioni extraeuropee del motore di ricerca (sentenza CGUE 24 settembre 2019, C-507/17). L'Autorità non ha infatti riconosciuto la sussistenza, nel caso in esame, dei presupposti per l'esercizio del potere valutativo riconosciuto dalla sentenza in capo alle autorità di controllo, quale, ad esempio, la riconducibilità al reclamante di situazioni di interesse personale e/o economico di perimetro più ampio rispetto ai confini dell'Unione europea.

La possibilità di riconoscere una specifica valenza informativa alle notizie reperibili in rete è stata tenuta nel debito conto anche nelle decisioni con le quali il Garante ha ritenuto di accogliere alcuni reclami nei quali le doglianze degli interessati erano dirette a lamentare il pregiudizio loro derivante dalla reperibilità in rete di articoli riguardanti vicende giudiziarie nelle quali erano stati coinvolti solo in una fase iniziale o che comunque riguardavano in via diretta persone diverse, sebbene in alcuni casi aventi legami di parentela o professionali con i medesimi. Si può citare, a titolo esemplificativo, il caso di una persona il cui nominativo era stato riportato all'interno di alcuni articoli di stampa che riferivano di un collegamento tra la società nella quale la stessa aveva prestato la propria attività ed un'altra azienda direttamente coinvolta in un'inchiesta giudiziaria, nonché quello di un reclamante le cui generalità erano state associate ad una vicenda giudiziaria nella quale era stato indagato solo in una fase iniziale, ma che coinvolgeva in via principale il padre, in seguito condannato. In entrambi gli episodi i reclamanti hanno eccepito il fatto che, contrariamente a quanto poteva desumersi dalla lettura degli articoli, non erano mai stati sottoposti a provvedimenti giudiziari in relazione alle vicende descritte – come confermato dai certificati penali prodotti nel corso dei rispettivi procedimenti – ed in considerazione di ciò il Garante ha ritenuto che la perdurante reperibilità in rete degli articoli in associazione al nominativo degli interessati fosse idonea a creare un impatto sproporzionato sui loro diritti, non bilanciato da un interesse pubblico a conoscere notizie di procedimenti che non avevano avuto alcun seguito giudiziario a loro carico (provv.ti 15 ottobre 2020, n. 192, doc. web n. 9491061 e n. 194, doc. web n. 9491078).

Riabilitazione e non menzione

È stato confermato un orientamento consolidatosi negli anni e diretto ad attribuire particolare rilievo alla portata giuridica di alcuni istituti dell'ordinamento penale, tra i quali la riabilitazione ed il beneficio della non menzione della con-

danna nel casellario giudiziale. Quest'ultimo, in particolare, è finalizzato a limitare la conoscibilità della condanna subita da un determinato soggetto, beneficio che sarebbe, di fatto, vanificato ove fosse consentito al gestore di un motore di ricerca di trattare tale dato attraverso la reperibilità in rete di esso in associazione al nominativo dell'interessato, così come rischierebbe di essere vanificata la finalità di agevolare il reinserimento sociale del reo nelle ipotesi in cui venga disposta la riabilitazione, con notevole pregiudizio della sfera giuridica del medesimo.

Ciò è quanto avvenuto, ad esempio, nel caso della richiesta di rimozione di alcuni URL da parte di una persona coinvolta in una vicenda giudiziaria, conclusasi nel 2017, connessa al suo ruolo di dirigente pubblico con una sentenza di applicazione di una pena a richiesta delle parti inferiore a due anni di reclusione e con concessione del beneficio della sospensione condizionale della stessa, oltreché della non menzione della pena nel certificato del casellario giudiziale in attuazione di quanto previsto dalle disposizioni che ne regolano la formazione (in particolare l'art. 24, comma 1, lett. *e*), d.P.R. 14 novembre 2002, n. 313, recante 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 anche nella formulazione successiva alle modifiche introdotte con il d.lgs. 2 ottobre 2018, n. 122). In tale ipotesi, come già avvenuto per il passato, l'Autorità ha ritenuto prevalente sul fattore temporale il dato costituito dal mancato aggiornamento delle informazioni reperibili sul conto dell'interessato e, soprattutto, la finalità dalla quale è governato il beneficio della non menzione della pena nel casellario giudiziale (provv. 30 aprile 2020, n. 81, doc. web n. 9426491).

In altro reclamo l'interessato ha chiesto invece la rimozione di URL collegati ad articoli che, pur riportando informazioni di riconosciuto valore per la storia giudiziaria e politica del nostro Paese, risultavano, con riferimento alle vicende che lo avevano direttamente riguardato, ormai superate in virtù del tempo decorso e del percorso di ravvedimento nel frattempo intrapreso, grazie al quale aveva ottenuto la riabilitazione. L'Autorità ha riconosciuto la fondatezza delle ragioni dedotte dall'interessato tenuto conto del fatto che la permanente indicizzazione dei relativi articoli avrebbe avuto l'effetto di elidere i benefici connessi all'operatività del predetto istituto ed avrebbe fornito un profilo giudiziario dell'interessato non aggiornato con riguardo ai successivi sviluppi (provv. 23 gennaio 2020, n. 24, doc. web n. 9297610).

In alcuni procedimenti, si è posto poi il tema legato al trattamento da parte del gestore del motore di ricerca di dati personali contenuti all'interno di immagini. La questione è emersa in relazione ad un reclamo tramite il quale l'interessato, avente una carica di rilievo all'interno di un'associazione a tutela dei diritti dei cittadini nota a livello nazionale, ha lamentato il pregiudizio derivante dalla reperibilità, in associazione al suo nominativo, di articoli al contenuto dei quali l'editore aveva abbinato immagini decontestualizzate, riferibili ad un evento diverso e risalente nel tempo.

Il Garante ha tuttavia giudicato la richiesta non fondata tenuto conto del fatto che il contenuto degli articoli in questione, concernente fatti recenti connessi al ruolo pubblico ricoperto dall'interessato, fosse di interesse per la collettività, precisando che l'utilizzo delle immagini così diffuse – riprese anch'esse nell'ambito di una manifestazione pubblica promossa molti anni prima dall'associazione della quale fa parte il reclamante – esprimesse una scelta editoriale operata dalle testate giornalistiche alle quali erano riconducibili i contenuti oggetto di contestazione ed alle quali avrebbe dovuto essere eventualmente rivolta apposita istanza, non essendo possibile svolgere tale valutazione sulla base dei criteri generalmente utilizzati per i trattamenti posti in essere tramite i motori di ricerca (provv. 12 novembre 2020, n. 221, doc. web n. 9521918).

9

Analoga valutazione è stata condotta con riguardo alla richiesta di rimozione di un URL collegato ad un articolo di recente pubblicazione nel quale erano riportate notizie di interesse pubblico relative alla candidatura di alcuni esponenti di un movimento politico in occasione dello svolgimento delle elezioni amministrative avvenute nel 2016 nella Capitale. Le ragioni della doglianza risiedevano nel fatto che in associazione al contenuto dell'articolo era stata pubblicata una fotografia che ritraeva, tra gli altri, l'interessato ripreso nell'atto di fare un gesto (il cd. saluto romano) configurabile quale reato, immagine che era stata scattata in un'occasione conviviale svoltasi in luogo aperto al pubblico e divulgata poi sul profilo Facebook di uno dei presenti dal quale era stata ripresa dal giornalista senza consenso delle persone coinvolte. Anche in tal caso l'Autorità ha ritenuto che le richieste del reclamante non potessero essere accolte in quanto i contenuti riportati nell'articolo – ma anche l'immagine per il significato che la stessa acquisiva in associazione con essi – rivestivano interesse pubblico in quanto atti a dare conto di specifici orientamenti politici manifestati in un contesto pubblico (provv. 15 gennaio 2020, n. 13, doc. web n. 9284633).

10 Cyberbullismo

L'attività dell'Autorità nel settore del cyberbullismo è stata in prevalenza caratterizzata dalla gestione delle segnalazioni pervenute che, salve alcune fattispecie non rientranti in tale ambito (perché, ad esempio, non riferite a minorenni o a condotte riconducibili a quelle previste dalla l. n. 71/2017), hanno riguardato principalmente la rimozione di contenuti e/o immagini di carattere offensivo e denigratorio, nonché di fotografie, anche a carattere intimo, e la denuncia dell'esistenza di falsi profili attivati a nome del segnalante.

La prima parte del 2020 è risultata particolarmente proficua con riguardo alle occasioni di collaborazione e di intervento del Garante quale membro del tavolo tecnico interistituzionale istituito dall'art. 3 della ricordata legge in materia di prevenzione e contrasto al cyberbullismo. In questa prospettiva, l'Autorità ha preso parte al *Safer internet day* 2020 – evento organizzato nell'ambito del progetto Generazioni connesse e coordinato dal Ministero dell'istruzione – con lo scopo di sensibilizzare la collettività sul cyberbullismo. In tale circostanza si è richiamata l'attenzione sulle misure da attuare per rendere più sicuro l'utilizzo della rete da parte delle giovani generazioni, sottolineando la necessità di assicurare una rafforzata sinergia tra scuola e famiglia al fine di costituire una rete di supporto ai (più) giovani e favorire così un approccio consapevole e prudente nell'utilizzo di dispositivi che, se correttamente impiegati, costituiscono validi strumenti di conoscenza, partecipazione e crescita professionale. Nel suo intervento, l'Autorità ha richiamato l'attenzione sulla necessità di valutare in maniera adeguata le finalità del trattamento dei dati conferiti dai ragazzi ai titolari che operano *online* al fine di confinarne l'uso improprio, quando non addirittura illecito, ed ha altresì posto l'accento sui poteri riconosciuti al Garante riguardo alla rimozione di contenuti contrari alla disciplina di settore.

A tale evento ha poi fatto da corollario l'ausilio prestato dall'Ufficio alla redazione di un questionario collegato al progetto *Better Internet for Kids* promosso, a partire dal 2012, dalla Commissione europea e diretto a rendere internet un ambiente più sicuro per i ragazzi attraverso la cooperazione tra la Commissione europea, gli Stati membri e gli operatori del settore (per lo più piattaforme). La finalità perseguita dal questionario è stata essenzialmente quella di consentire la raccolta dei dati relativi ai progressi compiuti in questo specifico ambito dagli Stati membri e di favorire altresì la condivisione tra gli stessi delle esperienze, delle problematiche riscontrate e delle buone prassi: dalla divulgazione di materiale volto a migliorare la consapevolezza nell'uso di internet da parte dei giovani, alle tipologie d'intervento per rendere anche la scuola soggetto attivo nel fenomeno della digitalizzazione, alla creazione di sistemi per individuare, in base alla fascia d'età, i programmi ed i contenuti disponibili in rete.

Si sono infine avute occasioni di incontro con i componenti del tavolo tecnico interistituzionale e, nel corso di uno di essi, è stato affidato all'Autorità il compito di predisporre, in attuazione di quanto previsto da tale disposizione, una bozza del codice di co-regolamentazione destinato a disciplinare alcuni adempimenti posti a carico degli operatori della rete e dei gestori di *social network*, ivi inclusi i profili più specificatamente attinenti alla protezione dei dati personali. Lo schema predisposto dall'Autorità ha formato quindi oggetto di un confronto (il 14 ottobre 2020) con gli

10

altri soggetti istituzionali e offerto lo spunto per avviare una riflessione comune sui nodi problematici emersi anche attraverso un maggiore coinvolgimento dei ragazzi, destinatari privilegiati degli strumenti di tutela individuati dalla legge sul cyberbullismo.

11 *Marketing* e trattamento dei dati personali

11.1. Telemarketing

Le segnalazioni e i reclami in materia di *marketing* 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 che, in ragione della loro numerosità e della complessità delle operazioni necessarie per risalire alla (spesso articolata) filiera del trattamento, continuano a costituire il carico di lavoro assolutamente prevalente dell'Autorità.

Dall'analisi delle segnalazioni pervenute risulta che le telefonate indesiderate continuano ad interessare sia gli abbonati iscritti nel Registro pubblico delle opposizioni (Rpo) – circostanza dalla quale si devono quindi desumere comportamenti ancora poco virtuosi da parte dei soggetti operanti nella filiera del *telemarketing* –, 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 vengono lamentate (oltre alla mancata identificazione del committente) 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, come peraltro già segnalato (cfr. da ultimo Relazione 2019, p. 118). In particolare, vengono lamentate non solo la violazione del diritto di cancellazione o 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 informazioni richieste, ad esempio, circa l'origine dei medesimi.

In una prospettiva di costante attenzione alle doglianze dei segnalanti riguardo al *telemarketing*, comunicazioni puntuali sono state regolarmente inviate anche con riferimento alle numerose e reiterate segnalazioni relative a 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) essenziali ai fini di un'attività di controllo efficiente ed efficace da parte dell'Autorità.

Con riguardo a tali segnalazioni l'Ufficio ha effettuato sistematicamente una ricerca delle numerazioni chiamanti, indicate dagli interessati, sul Registro degli

operatori di comunicazione (Roc) pubblicato nel sito web dell'Agcom, comunicando l'esito delle verifiche svolte nelle comunicazioni destinate ai segnalanti e censendo le società rilevate in un *dossier* appositamente predisposto per monitorare il fenomeno del *marketing* indesiderato da parte di tali operatori telefonici, nella prospettiva di promuovere l'esame organico (e cumulativo) delle doglianze avanzate nei confronti dei singoli operatori economici.

Con riguardo, invece, al fenomeno delle telefonate cd. mute, è stata comunicata ai segnalanti una sintesi dei propri interventi di carattere ispettivo, prescrittivo e sanzionatorio (fra cui anzitutto il provvedimento generale a carattere prescrittivo in materia di cd. chiamate mute del 20 febbraio 2014, nonché le FAQ pubblicate nel sito istituzionale del Garante, nella sezione "Telefonate mute: le domande più frequenti").

Nella gestione delle varie lagnanze, spesso si è palesata l'irreperibilità di vari titolari extra UE che, pur avendo l'obbligo di nominare un rappresentante nell'Unione, non vi ottemperano; in alcuni casi, è stato necessario chiarire ai reclamanti che il Garante dispone di mezzi istruttori e d'indagine decisamente limitati al riguardo.

Sono stati forniti anche numerosi chiarimenti sull'attuale quadro normativo in materia di Registro pubblico delle opposizioni, del quale si attende ancora la concreta operatività mediante il decreto attuativo previsto dalla legge 11 gennaio 2018, n. 5, recante nuove disposizioni in materia di iscrizione e funzionamento del registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato. A tale atto, infatti, è rimessa l'attuazione delle misure di contenimento del fenomeno delle chiamate indesiderate, tra le quali la possibilità di inserire anche le numerazioni mobili nel Rpo e il contestuale azzeramento di tutti i pregressi consensi. Nell'ambito dell'*iter* regolamentare, il Garante ha espresso, su richiesta del Mise, il parere del 10 dicembre 2020, n. 260 (doc. web n. 9517462), fornendo chiarimenti in relazione al regime sanzionatorio applicabile. In tale occasione, il Garante si è espresso in merito all'ambito di applicazione del Rpo chiarendo le motivazioni per le quali non si ritiene ipotizzabile, nell'attuale quadro normativo, una sua estensione alle chiamate promozionali senza operatore (cfr. punto 3.2).

Dall'analisi dei riscontri forniti dai titolari del trattamento è stata talora rilevata la sussistenza di una pregressa interazione con l'interessato, tale da rendere applicabile l'art. 130, comma 4, del Codice, che disciplina il cd. *soft spam*, con la conseguente legittimità dell'invio di *e-mail* a contenuto promozionale a soggetti che siano entrati già in contatto con il titolare (ad es. clienti) anche in assenza di un preventivo consenso all'attività promozionale (v. linee guida 4 luglio 2013 in materia di attività promozionale e contrasto allo *spam*, doc. web n. 2542348).

In altri casi è emerso l'utilizzo di liste di dati personali per finalità promozionali acquisite da imprese terze che li avevano raccolti in assenza di un libero e specifico consenso degli interessati, determinando così un'illecita circolazione di tali dati con la necessità di intervenire con provvedimenti inibitori, prescrittivi e sanzionatori.

Le notificazioni di utilizzo di *call center* all'estero

Continuano a pervenire all'Ufficio le notificazioni previste dall'art. 24-*bis*, d.l. n. 83/2012 (28 nel corso del 2020), per le quali si sta valutando di adottare una procedura automatizzata di ricezione (come già accade per i *data breach*) al fine di poter analizzare e consultare agevolmente le informazioni comunicate all'Autorità e cooperare con le altre autorità destinatarie di analoghe comunicazioni.

Merita di essere segnalato che sono state effettuate tre contestazioni (due l'11 novembre 2020; una terza il successivo 18 dicembre) ad altrettanti operatori, per la violazione dell'art. 24-*bis* con riguardo alla omessa o ritardata notifica, contestando sanzioni pecuniarie, definite con pagamento in misura ridotta, per un importo complessivo pari a euro 150.000.

11.1.1. I trattamenti nel settore telefonico

Diverse delicate istruttorie che hanno riguardato in via preminente i principali operatori di telefonia sono giunte a conclusione.

La prima, chiusasi con provvedimento del 15 gennaio 2020, n. 7 (doc. web n. 9256486), ha portato all'adozione di numerose misure inibitorie e prescrittive nei confronti del principale operatore telefonico italiano, con riguardo anche alla corretta, consapevole e responsabile gestione dei *call center* utilizzati per le campagne di *marketing*. La sanzione irrogata, come rilevato già nella precedente Relazione (cfr. p. 122), pari a circa 28.000.000 euro, è risultata la più alta mai comminata dal Garante.

Relativamente alle misure impartire, la società ha inviato una documentata relazione, attentamente vagliata dall'Ufficio che ha riscontrato alcuni punti meritevoli di approfondimento. Sono stati pertanto richiesti chiarimenti, fornendo al contempo indicazioni utili alla piena comprensione di alcune prescrizioni del citato provvedimento (nonché della sottesa normativa) e della relativa portata applicativa, con particolare riguardo alle utenze *business* e a quelle eventualmente reperibili *online.*

L'istruttoria sopra descritta è risultata collegata – nel contesto complessivo di trattamenti per finalità di *marketing* – a quelle relative ad alcune società di *call center, partner* del medesimo operatore telefonico, anche in considerazione della necessità di prendere in esame ulteriori doglianze (successive agli accertamenti ispettivi effettuati), analoghe a quelle già affrontate nel menzionato provvedimento; ciò ha consentito di valutare aspetti del trattamento ulteriori rispetto a quelli già esaminati e di individuare le effettive modalità di esecuzione dei trattamenti. Il *focus* istruttorio è stato incentrato sulle liste di dati acquisite da soggetti terzi, trattate senza un'idonea base giuridica per finalità di *telemarketing*, in nome e/o per conto della citata compagnia telefonica nonché sulle utenze cd. referenziate, ossia asseritamente indicate dai soggetti legittimamente contattati. Per le menzionate società sono stati adottati dal Garante in data 11 marzo 2021 i relativi provvedimenti correttivi e sanzionatori (n. 98, doc. web n. 9577371; n. 99, doc. web n. 9577065 e n. 100, doc. web n. 9577042).

Si evidenzia il dispositivo articolato, soprattutto con riguardo alle misure organizzative e tecniche prescritte, finalizzato ad assicurare la piena conformità alla normativa vigente, con specifico riguardo: alla gestione corretta, nonché adeguatamente documentata, del fenomeno delle chiamate rivolte ad utenze cd. fuori lista; all'inserimento in *black list* dei dati degli interessati che, in qualunque modo, si oppongano al trattamento. Misure peraltro finalizzate a garantire modalità corrette e non invasive nello svolgimento delle campagne promozionali, a prescindere dal mezzo utilizzato.

Una seconda importante compagnia telefonica operante sul territorio nazionale è stata poi raggiunta da un altrettanto rilevante provvedimento correttivo e sanzionatorio (provv. 9 luglio 2020, n. 143, doc. web n. 9435753), portando così a termine un'articolata istruttoria durata oltre due anni. La sanzione erogata è stata fissata in circa 16.800.000 euro. Le condotte rilevate hanno riguardato, in primo luogo, il trattamento per finalità di *marketing* posto in essere dalla società, facendo emergere una persistente difficoltà nel controllo della filiera dei subagenti, nonostante le misure correttive apportate negli anni. In un procedimento parallelo è stato rilevato che l'acquisizione dei dati degli interessati da contattare per le promozioni, effettuata da un subagente sconosciuto alla medesima compagnia telefonica, era avvenuto mediante accesso abusivo al sistema informatico di un operatore concorrente. È emerso pertanto come gli interventi posti in essere dall'operatore non siano riusciti ad incidere in concreto su condotte che causano particolare disagio sociale (con conseguenti numerosissime segnalazioni al Garante); infatti, pur in presenza di procedure

formalmente rispondenti alle disposizioni normative, l'acquisizione del consenso è risultata non sempre corretta, condizionata dalla pressione rappresentata dai forti incentivi economici perseguiti dagli agenti. La stessa attività istruttoria ha messo altresì in evidenza come i meccanismi di progettazione dell'*app* di servizio sono risultati impostati in maniera inidonea, con la conseguenza di forzare il conferimento del consenso da parte degli utenti senza che questi ne abbiano piena contezza.

Tra gli aspetti più rilevanti emersi dall'istruttoria e contestati al titolare, si segnalano: a) il mancato o inidoneo controllo sulla filiera dei *partner* che ha condotto alla realizzazione di campagne commerciali nei confronti di soggetti che non avevano prestato (o avevano revocato) il proprio consenso, oltre ad attività illecite per l'acquisizione dei nominativi da contattare; b) l'acquisizione illecita dei consensi attraverso procedure, in negozio o tramite *app*, volte a condizionare la libertà dell'interessato; c) le inidonee modalità di riscontro delle richieste di esercizio dei diritti da parte degli interessati con l'adozione di procedure volte ad ostacolare la revoca del consenso; d) le carenze nell'informativa; e) la pubblicazione indesiderata dei dati negli elenchi telefonici.

Nei confronti di un'altra delle maggiori società telefoniche a livello europeo è stato adottato il provvedimento del 12 novembre 2020, n. 224 (doc. web n. 9485681), con riferimento al complesso dei trattamenti finalizzati alla promozione di propri servizi o offerte e all'acquisizione di nuovi clienti. Il provvedimento ha accertato che le piattaforme informatiche della compagnia per la gestione della clientela non consentivano di verificare se l'attivazione dei servizi e delle offerte avvenisse a seguito di contatti promozionali correttamente effettuati da agenzie censite al Roc e con l'utilizzo di liste di anagrafiche relative a interessati che avessero espresso il proprio consenso ai trattamenti promo-pubblicitari. Nel provvedimento è stato osservato che i sistemi della compagnia devono essere configurati in modo da poter bloccare le procedure di attivazione di offerte o servizi quando esse non siano certamente riconducibili ad attività promozionali svolte nel rispetto delle norme e dei diritti degli interessati, degli utenti e dei consumatori fin dal momento del primo contatto; pertanto è stato ingiunto alla compagnia telefonica di modificare i propri sistemi informatici al fine di recepire tali prescrizioni. Il Garante ha anche accertato l'illiceità delle modalità di acquisizione delle liste anagrafiche utilizzate dalla rete di vendita della compagnia telefonica per il contatto dei potenziali clienti: tale acquisizione è risultata avvenire attraverso plurimi passaggi fra diversi titolari del trattamento in assenza del consenso degli interessati alla comunicazione dei dati. Il Garante ha altresì richiamato precedenti provvedimenti (provv. 11 dicembre 2019, n. 232, doc. web n. 9244365), evidenziando che il necessario controllo che a ciascun interessato deve essere garantito in ordine ai trattamenti per i quali ha prestato il consenso sarebbe del tutto irrealizzabile se le comunicazioni potessero avvenire in assenza di una propria manifestazione di volontà e fossero ancorate esclusivamente ad un consenso iniziale capace di dispiegare effetti a catena del tutto imprevedibili. È stato pertanto disposto il divieto dei trattamenti effettuato con l'utilizzo delle liste di anagrafiche così acquisite ed è stata applicata alla compagnia telefonica una sanzione di circa 12.250.000 euro.

All'esito di un accertamento ispettivo, è stato predisposto un provvedimento correttivo anche nei confronti di una compagnia telefonica di più recente emersione sul mercato nazionale (provv. 9 luglio 2020, n. 138, doc. web n. 9435807), peraltro comminando una sanzione pari a euro 800.000. In tale occasione, il Garante ha ammonito la società in merito alla necessità di presentare un'informativa chiara e pertinente rispetto alle finalità per cui i dati sono raccolti sul proprio sito web (cfr. par. 12.1); inoltre, sono state impartite apposite prescrizioni in merito al rispetto delle distanze di cortesia in fase di sottoscrizione del contratto mediante appositi

terminali. Infine, sono state rilevate violazioni nella conservazione e nell'accesso a dati di traffico da parte di soggetti non autorizzati, con la conseguente adozione di ulteriori misure correttive.

Con nota 20 novembre 2020, l'Ufficio ha avviato il procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del RGPD nei confronti di un'altra rilevante società telefonica. Il procedimento in questione si collega alla complessa istruttoria avviata dall'Autorità a seguito della ricezione di centinaia di segnalazioni e reclami inviati da interessati che lamentavano, e ancora lamentano, continui contatti telefonici indesiderati per promuovere i servizi di telefonia e internet.

Tra i vari aspetti contestati al titolare, si sono evidenziate: a) la mancata implementazione da parte della società di controlli della filiera dei dati personali acquisiti nella fase di promozione dei servizi idonei ad escludere che da contatti provenienti da numerazioni sconosciute siano stati poi perfezionati contratti o attivate utenze; b) alcune criticità in merito al processo di acquisizione da parte della società delle liste anagrafiche provenienti dai fornitori o *partner*; c) le carenze nell'informativa e nelle procedure adottate dalla società in merito al servizio cd. *call me back*; d) la vulnerabilità generale dei sistemi societari in relazione alla complessiva vicenda dei contatti rivolti alla clientela, diretti ad acquisire documenti di riconoscimento ovvero a proporre migrazioni delle utenze telefoniche, nonché l'omessa notificazione di alcuni *data breach* all'Autorità; e) le inidonee modalità di riscontro alle richieste di esercizio dei diritti da parte degli interessati a causa di un'inadeguata strutturazione dei sistemi della società; f) l'illecita attività promozionale svolta in *partnership* con un altro operatore economico (del settore energetico), in assenza del prescritto consenso e utilizzando, in modo non corretto, la base giuridica del legittimo interesse. Sulla base di tali violazioni, è stato adottato il provvedimento correttivo, inibitorio e sanzionatorio, per un importo di circa 4.500.000 euro (provv. 25 marzo 2021, n. 112, doc. web n. 9570997).

11.1.2. I trattamenti di dati nel settore energetico

Nel gennaio 2020 sono state esaminate le misure adottate in esecuzione del provvedimento dell'11 dicembre 2019, n. 232 (doc. web n. 9244365) da parte di una società operante nel settore energetico alla quale con il detto provvedimento è stata comminata una sanzione di 8.500.000 euro.

È stata altresì organizzata ed attuata, per un'analisi complessiva dei trattamenti in rilievo, una minuziosa attività di raccolta di tutti i reclami e delle segnalazioni pervenute nei confronti di un'altra società energetica, riguardanti soprattutto il *telemarketing* nei confronti di interessati titolari di utenze riservate che non hanno manifestato il consenso o di utenti iscritti nel Rpo, nonché il ricorso a modalità automatizzate di contatto, in particolare attraverso un disco preregistrato, per promuovere prodotti e servizi in vista del passaggio al mercato libero; pur in misura decisamente inferiore, si sono registrati altri fenomeni relativi, in particolare, alla fruizione dei servizi *online*.

Rispetto ad altro operatore attivo nel settore energetico ulteriori profili sono stati esaminati con riguardo all'effettuazione di telefonate promozionali nei confronti di soggetti i cui dati personali non risultavano forniti direttamente alla società ma acquisiti da altre fonti. In particolare, i dati risultavano acquisiti sulla base di liste di anagrafiche di interessati che avevano inizialmente acconsentito alla comunicazione dei relativi dati a terzi per finalità promozionali, ma non avevano rilasciato un consenso libero, specifico ed informato a successive comunicazioni tra autonomi titolari.

La complessa attività di verifica avviata in entrambi i casi è in via di definizione.

11.1.3. Il "sottobosco" delle agenzie incaricate delle attività di telemarketing *e* teleselling

Nell'ambito del contrasto alle attività di *telemarketing* selvaggio l'Autorità ha adottato un provvedimento correttivo e sanzionatorio (provv. 9 luglio 2020, n. 144, doc. web n. 9435774) nei confronti di un'importante agenzia, impegnata a promuovere l'attivazione di servizi nel segmento *business* del mercato telefonico e internet. L'adozione del provvedimento è stata preceduta da una complessa istruttoria che ha portato all'individuazione di un *call center* abusivo che aveva instaurato e consolidato forme di acquisizione di liste di potenziali clienti nonché modalità di contatto dei medesimi in palese violazione della normativa sulla protezione dei dati personali. In particolare, le liste di contatti venivano utilizzate senza aver acquisito dagli interessati il consenso al trattamento dei propri dati per finalità di *marketing* nonché per la comunicazione a terzi; inoltre il *call center* operava senza essere stato preventivamente designato dall'agenzia quale responsabile del trattamento, contattando i potenziali clienti mediante numerazioni mobili non censite al Registro degli operatori di comunicazione. I contratti acquisiti dal *call center* abusivo venivano poi inviati all'agenzia che, in ragione del consolidato rapporto con il committente, li registrava nella piattaforma di gestione dei clienti di quest'ultima procedendo all'attivazione di offerte e servizi. Il Garante, oltre ad aver applicato all'agenzia in questione una sanzione di 200.000 euro, ha imposto alla stessa di provvedere alla designazione dei propri *partner* quali responsabili del trattamento e, nelle more di tale adempimento, ha disposto il divieto di ulteriori trattamenti.

11.1.4. Gli eventuali profili penali

Per alcune delle istruttorie amministrative condotte, in ragione della ravvisabilità di profili di rilevanza penale, si è ritenuto opportuno predisporre e trasmettere alle Procure competenti la relazione motivata ex art. 167, comma 5, del Codice, unitamente ai documenti più significativi in atti. Si è così dato seguito all'appunto informativo inviato alla Procura della Repubblica presso il Tribunale di Roma da questa Autorità il 19 aprile 2019 e finalizzato a tracciare il complessivo quadro normativo in materia di comunicazioni promozionali ed offrire una panoramica delle attività inibitorie, prescrittive e sanzionatorie costantemente svolte dall'Autorità per contrastare il fenomeno del *marketing* indesiderato, riconducibile, in particolare, alle società operanti nel settore delle telecomunicazioni, anche nella prospettiva di un opportuno intervento dell'Autorità giudiziaria con i propri mezzi d'indagine per un più ampio contrasto al fenomeno del *telemarketing* selvaggio.

12 Internet e servizi di comunicazione elettronica

12.1. *Raccolta di dati* online

Continuano a pervenire segnalazioni relative alla liceità della raccolta dei dati *online*, con particolare riguardo alle formule di acquisizione del consenso e alla presenza di un'idonea informativa. Al riguardo si menziona il provvedimento correttivo e sanzionatorio del 9 luglio 2020, n. 138 (doc. web n. 9435807; cfr. par. 11.1.1), con cui l'Autorità, fra le varie prescrizioni, ha ingiunto alla società telefonica destinataria dello stesso l'implementazione di un'informativa chiara in relazione alle finalità per le quali i dati sono raccolti sul proprio sito web, rilevando altresì la presenza di una formula di richiesta del consenso per finalità di *marketing* che risultava non pertinente, non essendo indicata tale finalità tra i trattamenti effettuati.

12.2. *L'invio di* e-mail *indesiderate*

È stato adottato un provvedimento di ammonimento (provv. 19 maggio 2020, n. 90, doc. web n. 9443795) a seguito del reclamo pervenuto da un cliente che lamentava la ricezione di *e-mail* promozionali da parte di una società in tempi successivi rispetto al recesso dal programma fedeltà ed alla opposizione a ricevere ulteriori comunicazioni promozionali. Da quanto emerso all'esito di un'articolata istruttoria, la società, pur avendo dato atto dell'avvenuta cancellazione dei dati dell'interessato e riscontrato la specifica richiesta di accesso pure formulata dal reclamante, ha continuato ad inviare ulteriori comunicazioni promozionali in base ad un asserito errore dovuto al volume di richieste da gestire nello stato di amministrazione straordinaria in cui si è venuta a trovare nonché a causa della carenza di personale. È stato contestato anche il mancato rispetto dei principi di liceità e correttezza del trattamento nonché dei principi di *privacy by design* e *by default* ed è stata prescritta l'implementazione di adeguate procedure e di sistemi interni di gestione.

È stato adottato un articolato provvedimento (27 gennaio 2021, n. 37, doc. web n. 9561833), a contenuto anche sanzionatorio, a seguito dell'invio di comunicazioni commerciali indesiderate e in ragione dell'omessa informativa sul sito web della società titolare del trattamento, carente anche in relazione alle informazioni relative al Rpd (nonché per la mancata nomina e correlata comunicazione al Garante dei dati di contatto del medesimo).

12.3. *L'acquisizione del consenso e la circolazione di liste di dati per finalità promozionali*

Con provvedimento del 15 ottobre 2020, n. 181 (doc. web n. 9486485), l'Autorità si è espressa in merito all'idoneità di un consenso per finalità promozionali raccolto dieci anni addietro. Nel rilevare specifiche violazioni con riguardo al modulo di raccolta del consenso, è stato chiarito che il solo fattore temporale non è un parametro sufficiente, di per sé, per ritenere illecito il trattamento. Si è affermato che il consenso al trattamento dei dati personali per finalità promozionali, in quanto

espressione dell'autodeterminazione individuale, deve innanzitutto considerarsi autonomo e non condizionato dall'esistenza o meno di un rapporto contrattuale e deve ritenersi valido, indipendentemente dal tempo trascorso, finché non venga revocato dall'interessato, a condizione però che sia stato correttamente acquisito in origine e che sia ancora valido alla luce delle norme applicabili al momento del trattamento nonché dei tempi di conservazione stabiliti dal titolare.

Con provvedimento del 10 dicembre 2020, n. 267 (doc. web n. 9557571) è stato dichiarato illecito, disponendo la misura dell'ammonimento, il trattamento posto in essere da una società che aveva inviato *e-mail* promozionali utilizzando dati acquisiti da banche dati di soggetti terzi senza effettuare preventive verifiche sulla corretta composizione delle stesse. In tale sede, è stata ribadita la necessità di effettuare opportune valutazioni di conformità alla normativa in caso di acquisto di banche dati dal momento che siffatta acquisizione non esonera il titolare del trattamento dal dovere di verificare e documentare la presenza di un idoneo consenso degli interessati (v. in questo senso già provv. 29 maggio 2003 in materia di *spam* nonché il più recente provv. 18 aprile 2019, n. 96, doc. web n. 9105201, in materia di propaganda elettorale). In considerazione del riverbero dell'illiceità della raccolta sui successivi ulteriori trattamenti, si è pertanto reso necessario vietare l'ulteriore utilizzo dei dati acquisiti in assenza di un idoneo consenso, oltre a censurare l'omessa informativa a favore degli interessati.

In base a una segnalazione proveniente da un'associazione di categoria, alcuni iscritti, ex clienti di una società fornitrice di servizi energetici (risultata in stato di liquidazione e dichiaratasi estranea all'accaduto), avrebbero ricevuto telefonate promozionali indesiderate per conto di altri fornitori sulla base di dati raccolti da una società moldava. Sulla base delle dichiarazioni dell'Autorità di protezione dati moldava, è emerso che detta società si occupa della raccolta dati via internet attraverso la compilazione di apposita modulistica e che la raccolta dei dati di contatto di potenziali clienti (*lead generation*) sarebbe comunque preceduta dalla visualizzazione di una informativa e sarebbe fondata su un consenso libero ed informato degli interessati. L'impresa moldava non è stata tuttavia in grado di fornire un preciso riscontro a quanto richiesto, negando qualunque rapporto con la società in questione nonché la detenzione di un *database* dei clienti di quest'ultima. Nonostante i trattamenti effettuati dalla stessa siano risultati sottratti all'applicazione del Regolamento, si è comunque ottenuta l'assicurazione, da parte dell'Autorità moldava, di continuare a monitorare il fenomeno segnalato, aggiornando il Garante.

In tema di esercizio dei diritti degli interessati in relazione a trattamenti di dati svolti con finalità promozionali, il Garante ha adottato un provvedimento (23 gennaio 2020, n. 12, doc. web n. 9284622) con il quale ha rivolto un avvertimento, ai sensi dell'art. 58, par. 2, lett. *a*), del RGPD, ad una società di servizi di *marketing*, individuando nei trattamenti svolti dalla stessa un *fumus* di illiceità, con riferimento a possibili violazioni degli artt. 5, 6, 7 e 13 del RGPD. Con riferimento al mancato riscontro ad una richiesta di esercizio del diritto di accesso di un interessato, garantito dall'art. 15 del RGPD, il Garante, con lo stesso provvedimento, ha applicato una sanzione amministrativa pecuniaria alla società, ingiungendo alla medesima di dare seguito alle richieste dell'interessato.

12.4. *Le linee guida in materia di* cookie

In considerazione del tempo trascorso dal provvedimento del 2014 sulle regole da seguire per l'impiego di *cookie* e altri strumenti di tracciamento, tenuto anche

conto dell'entrata in vigore del Regolamento che ha rafforzato il potere dispositivo della persona sulle sue informazioni personali ed ha introdotto l'obbligo del rispetto dei principi di protezione dati sin dalla fase della progettazione e per impostazioni predefinite (*privacy by design* e *by default*), nonché a seguito del monitoraggio effettuato sulla implementazione delle regole da parte dei siti web, il Garante ha adottato (e posto in consultazione pubblica) lo schema delle linee guida in materia di *cookie* e altri strumenti di tracciamento (provv. 26 novembre 2020, n. 255, doc. web n. 9498472).

Tra le principali indicazioni fornite si segnalano quelle riguardanti: la distinzione tra *cookie* tecnici e *cookie* di profilazione; la piena estensione della disciplina ai sistemi di tracciamento cd. passivi; le condizioni di liceità dello *scrolling* e del *cookie wall*; l'esigenza di standardizzazione e di categorizzazione semantica dei *cookie*; le modalità per l'acquisizione del consenso tramite *banner*; il trattamento dei dati per finalità di profilazione in caso di impiego di *cookie* di terze parti.

Come anticipato, il documento è stato posto in consultazione pubblica per un periodo di 30 giorni e l'Autorità sta valutando i vari e talora articolari contributi ricevuti per addivenire all'adozione del testo definitivo.

12.5. *L'attività riguardante i* data analytics

È stata avviata un'istruttoria, con richieste di informazioni ed esibizione di documenti nei confronti delle principali compagnie telefoniche e di altri soggetti, in ordine all'uso dei cd. *data analytics*, al fine di tracciare un quadro complessivo di tale attività e individuare e valutare i trattamenti di dati correlati, anche nella prospettiva del fenomeno dei *big data*, nonché verificare il rispetto dei principi ed obblighi della vigente normativa.

Gli elementi fino ad oggi acquisiti sembrano evidenziare un salto di qualità nei processi di *data analytics*, un tempo confinati nell'alveo delle attività di *marketing* di ciascuna impresa. Il quadro che emerge è quello di un'attività complessa che si caratterizza come *business* autonomo messo a disposizione di piccole, medie e grandi imprese e p.a., con offerte differenziate e specifici campi di elaborazione rispetto alla segmentazione del mercato. Ciò impone una puntuale valutazione anche in ordine alla base giuridica dei trattamenti svolti, posto che la mera indicazione di un legittimo interesse del titolare non sembra poter più accomunare attività di profilazione che traggono la loro ragion d'essere dalle necessità aziendali legate alle strategie di *marketing* e trattamenti di dati effettuati mediante sistemi di *data analytics* finalizzati alla commercializzazione verso l'esterno. Nell'ambito del bilanciamento degli interessi in gioco, sarà necessario valutare: il livello di dettaglio e la completezza dei profili elaborati; l'impatto della profilazione sull'interessato; le misure di sicurezza volte ad assicurare la qualità dei dati nel processo di profilazione nonché le necessarie garanzie ai sensi dell'art. 22, par. 2, del RGPD.

12.6. *Conservazione ed accesso ai dati di traffico telematico e telefonico*

A seguito di una complessa istruttoria è stato adottato il provvedimento del 14 maggio 2020, n. 85 (doc. web n. 9442587) relativo ad un reclamo presentato da una persona indagata per alcuni reati e concernente la lamentata violazione – da parte di un operatore telefonico (che non risulta aver dato riscontro e peraltro non ha ritenuto di aderire all'invito formulato dall'Ufficio) – del diritto di accesso ai dati di traffico in

entrata e in uscita, di cui i suoi difensori necessitavano per condurre le investigazioni difensive. Si evidenzia la delicatezza di tale fattispecie, anche in ragione degli interventi della CGUE in materia di conservazione dei dati di traffico (cfr. cap. 24) e del fatto che si è trattato della prima applicazione della normativa in vigore dopo la piena operatività del RGPD, che, come noto, ha comportato, mediante il d.lgs. n. 101/2018, alcune modifiche anche all'art. 132 del Codice. Ciò, peraltro, in costanza della *lex specialis* di riferimento in materia di comunicazioni elettroniche (di recepimento della direttiva 2002/58/CE), rimasta immutata in attesa del nuovo regolamento *e-privacy.*

Con il citato provvedimento l'Autorità ha anzitutto richiamato la persistente validità ed operatività del provvedimento generale del 3 novembre 2005 (doc. web n. 1189488), precisando che, in via di eccezione, le richieste di esercizio dei diritti possono essere presentate ed evase positivamente quando risulta comprovato che la risposta ad esse da parte del fornitore è necessaria per evitare "un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397", pur avendo ad oggetto il traffico telefonico in entrata, inteso come "qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione". L'Autorità ha tuttavia chiarito come gravi sul richiedente l'onere di comprovare la necessità dell'accesso, documentando con idonei elementi al fornitore che il mancato accesso determinerebbe un pregiudizio effettivo e concreto allo svolgimento delle investigazioni. Nel caso di specie, il Garante ha ravvisato un collegamento stretto fra dati di traffico richiesti ed ipotesi di reato formulate dall'Autorità giudiziaria, ritenendo altresì sussistente la necessità dei dati richiesti, inclusi quelli in entrata, per lo svolgimento delle investigazioni difensive volte a tutelare il diritto di difesa del reclamante coinvolto in un procedimento giudiziario a suo carico. È stato altresì sottolineato che la perdurante e ingiustificata condotta omissiva della società telefonica non può riflettersi negativamente sull'interessato, impedendogli di esercitare pienamente il suo diritto di difesa. Pertanto è stato ordinato alla compagnia telefonica di soddisfare l'istanza di accesso formulata dal reclamante, ingiungendo alla stessa di adottare – nell'ambito della revisione delle procedure che la medesima stava attuando in base a quanto già prescritto con il citato provvedimento del 15 gennaio 2020, n. 7 (cfr. par. 11.1.1) – misure organizzative e tecniche idonee a dar riscontro tempestivo ad analoghe richieste di accesso ai tabulati.

Una problematica simile si è riscontrata riguardo ad un reclamo (in via di definizione) presentato nei confronti del medesimo operatore telefonico dal difensore di un libero professionista sottoposto anch'esso a procedimento penale, imponendo una riflessione più generale sulla portata applicativa e pratico-operativa dell'art. 132 del Codice in caso di persistente inerzia o diniego da parte degli operatori telefonici che si trovino costretti ad accedere alle banche dati del traffico telefonico/telematico, decorsi i termini rispettivamente previsti dalla legge (24 mesi per il traffico telefonico; 12 mesi per quello telematico: v. art. 132, comma 1, del Codice).

Va ricordato che, mediante il già ricordato provvedimento del 9 luglio 2020, n. 143 (doc. web n. 9435753), sono state rilevate violazioni anche in relazione ai profili, qui considerati, relativi alla conservazione e all'accesso a dati di traffico da parte di soggetti non autorizzati per i quali sono state impartite apposite misure correttive e sanzionatorie.

12.7. *Propaganda elettorale e comunicazione politica*

A seguito del provvedimento in materia di propaganda elettorale e comunica-

zione politica, aggiornato alle novità introdotte dal Regolamento (provv. 18 aprile 2019, n. 96, doc. web n. 9105201), l'Autorità ha avviato, con riferimento alle consultazioni elettorali svoltesi nel mese di maggio 2019, un'attività di monitoraggio circa il corretto trattamento di dati personali da parte dei candidati politici ed amministrativi partecipanti a tale tornata elettorale.

Le istruttorie sono state avviate sulla scorta di segnalazioni e reclami pervenuti nonché d'ufficio sulla base di notizie di stampa che paventavano possibili trattamenti illeciti di dati personali a fini di propaganda politica.

I casi sono stati trattati e decisi congiuntamente al fine di esaminare la materia, per sua natura delicata e per definizione sottoposta al principio della *par condicio*, in maniera unitaria e coerente rispetto alle indicazioni fornite dal Garante nel sopracitato provvedimento in materia di propaganda elettorale e comunicazione politica. In esito alle plurime istruttorie preliminari ed ai procedimenti successivamente avviati ex art. 166, comma 5, del Codice, sei casi sono stati sottoposti alla valutazione del Collegio.

Quale considerazione di ordine generale sull'attività di monitoraggio compiuta, a parte un unico caso connotato da elementi di novità sotto il profilo della propaganda politica, e quindi privo di consolidati punti di riferimento, le restanti violazioni accertate sono state ritenute riconducibili ad iniziative isolate e apparentemente frutto più di ingenuità che di precisa strategia elettorale.

In tutti i casi portati all'attenzione del Collegio è stato rilevato l'invio di messaggi (sms o posta elettronica) di propaganda elettorale in assenza di un'adeguata base giuridica e di idonee informazioni all'interessato. In due casi (provv.ti 1° ottobre 2020, n. 169, doc. web n. 9501766 e, parzialmente, n. 170, doc. web n. 9501845) il procedimento è stato archiviato. Negli altri (provv.ti 1° ottobre 2020, n. 165, doc. web n. 9500388; n. 166, doc. web n. 9500438; n. 167, doc. web n. 9500508; n. 168, doc. web n. 9500554; n. 170, cit.) il procedimento è stato definito formulando nei confronti dei rispettivi titolari la misura dell'ammonimento ai sensi dell'art. 58, par. 2, lett. *b*), del RGPD.

12.8. *L'attività collegata all'emergenza epidemiologica da Covid-19*

Come si è visto, i riflessi della pandemia hanno formato oggetto di approfondimento da parte dell'Ufficio da più punti di vista e con vari contributi: certo in relazione alla segnalata attività concernente l'*app* Immuni – e, più in generale, alle *app* di *contact tracing*, anche con riguardo ai contributi forniti per la predisposizione delle linee guida 4/2020 del Comitato (cfr. parr. 5.1 e 21.1) – e con riguardo alla tematica della didattica a distanza, oggetto del menzionato provvedimento del 26 marzo 2020, n. 64 (cfr. parr. 4.3.1, 13.2 e 24), ma anche in relazione alla tematica delle *fake news*.

Fake news

La situazione di crisi generata dalla pandemia, infatti, ha fatto registrare la propagazione virale, pericolosa per la salute pubblica, di *fake news* in materia di Covid-19, veicolate attraverso i *social network* e le *chat* di messaggistica. In particolare, il Governo (Mise) ha richiesto al Garante elementi informativi per fornire riscontro all'interrogazione a risposta scritta n. 4-03135, presentata dall'on. De Bonis con particolare riguardo ad un sistema di *fact checking* proposto da Whatsapp e Facebook. Inoltre, nell'ambito di più ampie consultazioni interistituzionali sul tema e a partire proprio dal progetto di co-regolazione su Facebook, è stato avviato un tavolo tecnico congiunto con Agcom avente l'intento di coordinare, in maniera permanente, le rispettive competenze in materia di diffusione di false informazioni *online* (cfr. par. 3.2).

La materia, più in generale, ha formato oggetto dell'audizione informale del Presidente del Garante presso le Commissioni riunite trasporti e cultura della Camera dei deputati nell'ambito dell'esame di alcune proposte di legge recanti l'istituzione di una Commissione parlamentare di inchiesta sulla diffusione intenzionale, seriale e massiva di informazioni false (audizione del 3 marzo 2020, doc. web n. 9283850: cfr. par. 3.1.1).

Sms istituzionali

Con riguardo alle esigenze informative connesse all'emergenza pandemica, l'Ufficio ha partecipato alla stesura del testo della previsione concernente l'invio di un sms istituzionale informativo sul Covid-19 a quanti facciano ingresso in Italia.

La possibilità da parte dell'Ambasciata cinese di inviare messaggi informativi via sms alla popolazione di origine cinese residente in Italia mediante un operatore telefonico italiano ha formato oggetto di un'istruttoria, come pure, nell'ambito delle iniziative prese in considerazione nella fase di emergenza sanitaria, il progetto presentato da una compagnia telefonica per consentire la geolocalizzazione dei terminali degli utenti con finalità predittive e di contrasto epidemiologico (con particolare riferimento all'individuazione dell'eventuale base giuridica dei trattamenti ed alle misure organizzative e tecniche da adottare).

12.9. *Le procedure IMI relative a trattamenti di dati in internet e in materia di comunicazioni elettroniche*

Le procedure di cooperazione europea relative a trattamenti transfrontalieri di dati personali assumono particolare rilevanza nell'ambito delle reti telematiche – spazi, per definizione, non delimitati da confini geografici – sia con riferimento a trattamenti che afferiscono ai classici servizi della società dell'informazione (*e-commerce, online advertising*, servizi offerti da *hosting* e *content provider*), sia con riferimento alle problematiche sempre più frequenti e delicate che concernono i *social network*.

Come pure evidenziato in relazione al trattamento dei dati nel settore economico (v. *infra* par. 14.6; v. anche par. 21.1 e parte IV, tab. 10-12), l'attività svolta nel 2020 ha evidenziato un progressivo, costante aumento tendente al graduale assestamento ed affinamento del meccanismo di cooperazione.

Le procedure ex art. 56 del RGPD, riferite alla fase preliminare di individuazione dell'autorità capofila (*Lead Supervisory Authority* - LSA) e delle autorità interessate (*Concerned Supervisory Authority* - CSA) sono diminuite, anche in virtù del fatto che i reclami concernenti un medesimo titolare e medesime presunte violazioni confluiscono direttamente nei registri dei casi già esistenti in cui vengono accorparti (*bundled*) per titolare e per violazioni omogenee. Sono al contempo progressivamente aumentate le procedure di vera e propria cooperazione. In particolare, nel corso del secondo semestre 2020 è stato rilevato un netto incremento del ricorso alla consultazione informale nell'ambito delle procedure di cooperazione (art. 60 del RGPD) e della mutua assistenza volontaria (art. 61 del RGPD).

Tale approccio alla cooperazione europea rappresenta un indubbio cambio di passo, anche in prospettiva futura, nel perseguimento di una modalità di lavoro basata sulla ricerca del consenso condiviso, principio cristallizzato, da ultimo, nelle linee guida 9/2020 sul concetto di obiezione pertinente e motivata, approvate in via definitiva dal Comitato in data 9 marzo 2021.

In particolare, il ricorso alle procedure di consultazione informale ai sensi dell'art. 60 del RGPD è stato finalizzato a condividere risultanze investigative ovvero anticipare alle autorità interessate questioni giuridiche di particolare rilevanza o comples-

sità in relazione alla successiva fase decisoria. Come detto, l'adozione di tali procedure contribuisce ad agevolare la informale ma sostanziale convergenza delle posizioni delle singole autorità di controllo nell'ambito del meccanismo di cooperazione e prevenire, ove possibile, il ricorso all'intervento del Comitato mediante gli strumenti e le procedure previste dal meccanismo di coerenza.

Sulla stessa linea si pone l'evoluzione della prassi nel ricorso alle procedure di mutua assistenza volontaria ex art. 61 del RGPD. Infatti, se in passato tali procedure erano impiegate soprattutto per l'esame e per la condivisione dei quesiti più semplici concernenti profili interpretativi o applicativi del RGPD, nel 2020 è stato riscontrato un loro crescente utilizzo in termini di fungibilità rispetto alle menzionate consultazioni informali (condivisione di documenti e informazioni relativi a grandi titolari) oppure per la trasmissione all'autorità capofila competente di reclami contro titolari per i quali la stessa è già chiaramente individuata, evitando l'attivazione delle più onerose procedure preliminari ex art. 56 RGPD.

Nonostante l'oggettivo riscontro di una volontà comune tesa a comporre con autentico spirito collaborativo i casi transnazionali, non sono mancate le occasioni in cui sono stati formulati commenti o formalizzate obiezioni "pertinenti e motivate" nei confronti di progetti di decisione di altre autorità di controllo ritenuti non condivisibili. Nell'ambito di tale attività sono emerse alcune interessanti questioni giuridiche con riguardo alla corretta interpretazione della disciplina del RGPD e alle differenze rilevabili fra le legislazioni interne dei singoli Stati membri, in merito al rispettivo ordinamento amministrativo, nonché alla ripartizione di competenze tra autorità indipendenti all'interno dei singoli Stati membri.

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

13.1. *La protezione dei dati personali nell'ambito del rapporto di lavoro*

L'Autorità ha dato corso alle numerose istanze pervenute relative ai trattamenti di dati personali effettuati in ambito lavorativo (perlopiù tramite reclami, ma pure si registrano segnalazioni nonché la trasmissione, per i profili di competenza, di verbali di accertamento di presunte violazioni da parte di diversi organi accertatori) ed è proseguita l'attività di implementazione di quanto previsto dal RGPD e dalla disciplina di adeguamento del Codice (d.lgs. 10 agosto 2018, n. 101). Sono stati altresì forniti chiarimenti e, in alcuni casi, assistenza ai soggetti coinvolti dall'applicazione delle disposizioni in materia di protezione dei dati (titolari, interessati, associazioni di categoria rappresentative di interessati) sulle novità del RGPD, anche attraverso la risposta a quesiti di particolare rilevanza o che presentavano aspetti di novità rispetto a quanto già precisato in precedenti provvedimenti adottati dal Garante.

In tale quadro sono stati approvati provvedimenti che hanno stabilito le condizioni di liceità dei trattamenti effettuati in ambito lavorativo mediante dispositivi tecnologici sia del tipo ormai tradizionalmente utilizzato nel rapporto di lavoro (come i sistemi di videosorveglianza e di posta elettronica aziendale), ma anche attraverso sistemi tecnologici caratterizzati da configurazioni sempre più complesse e che pongono, pertanto, problemi nuovi circa le specifiche modalità di conformazione dei trattamenti effettuati ai principi di protezione dei dati.

Il Garante ha ribadito che i trattamenti in ambito lavorativo devono avvenire nel rispetto dei diritti e delle libertà fondamentali nonché, in particolare, della dignità delle lavoratrici e dei lavoratori (v. art. 1 del Codice). È stato altresì sottolineato in più provvedimenti che pure in ambito lavorativo l'esercizio dei diritti riconosciuti all'interessato (v. artt. 12-22 del RGPD) deve essere quanto più possibile agevolato dal titolare, conformemente a quanto stabilito in proposito dalla disciplina di derivazione eurounitaria.

Dati biometrici

Con particolare riferimento ai trattamenti di dati biometrici, la cui disciplina è equiparata dal RGPD a quella più rigorosa prevista per le categorie particolari di dati (v. art. 9, par. 1, del RGPD nonché, con specifico riferimento all'ambito dei rapporti di lavoro, art. 9, par. 2, lett. *b*), del RGPD e considerando da 51 a 53), l'Autorità ha proseguito i lavori per la predisposizione del provvedimento che individua le misure di garanzia previste dall'art. 2-*septies* del Codice relativamente al loro trattamento nel contesto lavorativo. Allo stato, tale trattamento è ammesso solo sulla base dell'art. 2-*septies*, comma 7, del Codice (articolo aggiunto dal d.lgs. n. 101/2018) con riguardo all'"accesso fisico e logico ai dati da parte di soggetti autorizzati" per specifiche finalità di sicurezza. 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.

Si segnala, infine, che è stato sottoscritto il 22 aprile 2021 un protocollo di intesa tra il Garante e l'Ispettorato nazionale del lavoro avente ad oggetto, nell'ambito delle rispettive competenze e salve le prerogative di indipendenza dell'Autorità, attività di collaborazione e consultazione su tematiche specifiche, anche nella prospettiva della assunzione di orientamenti condivisi su singole questioni.

13.2. *I trattamenti effettuati per finalità di prevenzione dal contagio da Covid-19 nel contesto lavorativo*

Indicazioni e chiarimenti sono stati forniti con riguardo ai trattamenti di dati personali nel contesto lavorativo nel quadro dell'emergenza epidemiologica da Covid-19 dichiarata dal Consiglio dei Ministri in data 31 gennaio 2020. Considerato che nel corso dell'emergenza si sono susseguiti, in tempi assai ravvicinati, in ragione dell'aggravarsi dello scenario nel contesto nazionale, interventi normativi e conseguenti atti di indirizzo emanati dalle istituzioni competenti, il Garante è intervenuto fin dalle prime fasi dell'emergenza per chiarire dubbi interpretativi, frutto anche della sovrapposizione di numerosi interventi regolatori, e prevenire il verificarsi di trattamenti di dati personali non conformi alla disciplina di protezione dei dati. In particolare, l'Autorità ha invitato i datori di lavoro a non intraprendere iniziative autonome consistenti nella raccolta di dati personali, anche relativi alla salute di utenti e lavoratori, ove non normativamente previste o disposte dagli organi competenti (cfr. comunicato 2 marzo 2020, doc. web n. 9282117).

Un'attenzione particolare è stata prestata alle problematiche legate alla sicurezza dei luoghi di lavoro pubblici e privati e ai connessi trattamenti di dati relativi al personale, nonché a utenti, clienti e fornitori. In particolare, è stato chiarito che nel contesto dell'emergenza le amministrazioni e le imprese, nello svolgimento dei compiti datoriali in materia di sicurezza nei luoghi di lavoro (artt. 6, 9, par. 2, lett. *b*), e 88 del RGPD), sono tenute a rispettare il Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro, sottoscritto inizialmente il 14 marzo 2020 fra il Governo e le parti sociali – adottato in base a quanto previsto dall'art. 1, n. 7, lett. *d*), d.P.C.M. 11 marzo 2020 (il cui contenuto è stato successivamente richiamato dall'art. 29-*bis*, d.l. n. 23/2020, convertito con l. 5 giugno 2020, n. 40) – ed aggiornato il 24 aprile 2020 (ed inserito quale all. 6, d.P.C.M. 26 aprile 2020). Tale impianto regolatorio è stato confermato dall'art. 2, d.P.C.M. 13 ottobre 2020, il cui allegato 12 nuovamente recepisce il menzionato Protocollo, da ultimo aggiornato il 6 aprile 2021. Dal punto di vista contenutistico, detto Protocollo ha previsto specifiche misure da adottare per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro, indicando, in particolare, le condizioni e le specifiche modalità in presenza delle quali è possibile effettuare trattamenti di dati relativi alla salute nel rispetto dei principi di proporzionalità e di limitazione della raccolta dei dati nonché circoscrivendo i trattamenti effettuati al periodo di emergenza sanitaria.

Protocollo condiviso

Quest'ultima e, in particolare, la necessità di salvaguardare la salute dei lavoratori attraverso l'individuazione di strumenti idonei a minimizzare il rischio di contagio in occasione dello svolgimento dell'attività lavorativa, ha inciso profondamente sulle modalità di svolgimento della prestazione di lavoro. In particolare, gli strumenti di prevenzione del contagio (sia quelli di tipo tecnologico che quelli consistenti in misure organizzative) comportano una inedita possibilità di intrusione del datore di lavoro nella sfera privata del lavoratore (attraverso l'apprensione di notizie non direttamente collegate allo svolgimento della prestazione lavorativa, quali quelle riferite a spostamenti e contatti, nonché di informazioni relative allo stato di salute). Pertanto, sulla base dei numerosi riscontri forniti a quesiti, segnalazioni e reclami, sono state elaborate e pubblicate (il 4 maggio 2020, aggiornandole il 14 maggio e il 6 luglio 2020) alcune FAQ (doc. web n. 9337010) rivolte ad amministrazioni, imprese e cittadini, contenenti prime indicazioni sulle problematiche connesse all'emergenza, in particolare in materia di "Trattamento dei dati nel contesto lavorativo pubblico e privato nell'ambito dell'emergenza sanitaria".

FAQ

13

Si è così precisato che la rilevazione della temperatura corporea del personale per l'accesso ai locali e alle sedi aziendali rientra tra le misure per il contrasto alla diffusione del virus che trovano applicazione anche nei confronti di utenti, visitatori e clienti nonché dei fornitori, ove per questi ultimi non sia stata predisposta una modalità di accesso separata; non è poi ammessa la registrazione del dato relativo alla temperatura corporea rilevata, bensì, nel rispetto del principio di "minimizzazione", la registrazione della sola circostanza del superamento della soglia stabilita dalla legge, in particolare quando sia necessario documentare le ragioni che hanno impedito l'accesso al luogo di lavoro.

È stato rammentato che tra le misure di prevenzione e contenimento del contagio che i datori di lavoro devono adottare in base al quadro normativo vigente, vi è la preclusione dell'accesso alla sede di lavoro a chi, negli ultimi 14 giorni, abbia avuto contatti con soggetti risultati positivi al Covid-19 o provenga da zone a rischio secondo le indicazioni dell'OMS. A tal fine, anche alla luce delle successive disposizioni emanate in materia (v. il citato Protocollo condiviso), è possibile richiedere una dichiarazione che attesti tali circostanze anche a terzi (es. visitatori e utenti): i dati così raccolti dovranno essere solo quelli necessari, adeguati e pertinenti rispetto alla prevenzione del contagio da Covid-19 e non dovranno essere chieste informazioni aggiuntive in merito alla persona risultata positiva, alle specifiche località visitate o altri dettagli relativi alla sfera privata.

Il Garante ha altresì ribadito che il datore di lavoro non può rendere nota l'identità del dipendente risultato affetto da Covid-19 agli altri lavoratori. Inoltre, considerate le notizie di stampa in merito al ricorso, anche da parte di grandi società, ad applicativi preordinati al contenimento del rischio di contagio da Covid-19 (volti ad innalzare i livelli di sicurezza nella delicata fase di progressivo riavvio delle attività produttive sospese o della prosecuzione di quelle che non si sono fermate) e alle segnalazioni pervenute, il 6 luglio 2020 il Garante ha pubblicato sul proprio sito istituzionale ulteriori FAQ. In tale occasione è stato indicato che la funzionalità di *contact tracing*, prevista da alcuni applicativi al dichiarato fine di poter ricostruire, in caso di contagio, i contatti significativi avuti nell'arco temporale individuato dalle autorità sanitarie per ricostruire la catena dei contagi ed allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi, è disciplinato unicamente dall'art. 6, d.l. 30 aprile 2020, n. 28.

L'Autorità ha precisato che il datore di lavoro può ricorrere all'utilizzo degli applicativi disponibili sul mercato se gli stessi non comportano il trattamento di dati personali riferiti a soggetti identificati o identificabili. Ciò nel caso in cui il dispositivo utilizzato non sia associato o associabile, anche indirettamente (es., attraverso un codice o altra informazione), all'interessato né preveda la registrazione dei dati trattati (es., le applicazioni che effettuano il conteggio degli accessi a un determinato luogo, attivando un "semaforo rosso" al superamento del limite prestabilito; oppure alle funzioni di taluni dispositivi indossabili che emettono un segnale sonoro o una vibrazione in caso di superamento della soglia di distanziamento prestabilita, senza così tracciare chi indossa il dispositivo né registrare alcuna informazione). Si pensi, altresì, ad applicativi collegati ai tornelli di ingresso che, attraverso un rilevatore di immagini, consentono l'accesso solo a persone che indossano una mascherina (anche qui, senza registrare le immagini o altre informazioni). Il Garante ha però precisato che in questi casi spetta comunque al titolare verificare il grado di affidabilità dei sistemi scelti, predisponendo misure da adottare in caso di malfunzionamento dei dispositivi.

Sempre con riferimento a tali applicativi aziendali, l'Autorità ha altresì avviato alcune istruttorie per verificare l'effettiva attivazione degli stessi e la loro conformità

alla disciplina di protezione dei dati personali. All'esito di tale attività di controllo è emerso che alcune società, dopo una prima fase di valutazione circa l'opportunità di adottare applicativi dotati di funzionalità di *contact tracing* nell'ambito del rapporto di lavoro, hanno deciso di soprassedere e che altre società hanno adottato applicativi privi della funzionalità di tracciamento; su aspetti circoscritti sono state comunque fornite indicazioni, ai sensi dell'art. 57, par. 1, lett. *d*), del RGPD, circa le modalità per conformarsi pienamente alle disposizioni vigenti in materia di protezione dei dati personali.

Lavoro agile e didattica a distanza

Nell'ambito dell'emergenza si è assistito a un progressivo ricorso a modelli di svolgimento a distanza dell'attività lavorativa (didattica a distanza, lavoro agile). In particolare, il lavoro agile è stato configurato dalle disposizioni dell'emergenza quale "modalità ordinaria di svolgimento della prestazione lavorativa nelle pubbliche amministrazioni" (cfr. art. 87, d.l. 17 marzo 2020, n. 18 e art. 1, lett. *d*), d.P.C.M. 22 marzo 2020), essendosi stabilito di limitare la presenza del personale negli uffici, con esclusivo riguardo alle attività indifferibili che richiedono necessariamente la presenza sul luogo di lavoro, anche quale misura di contrasto della pandemia. Da ultimo, tenuto conto dell'evoluzione della situazione epidemiologica, è stato previsto che nelle p.a. debba essere assicurato "lo svolgimento del lavoro agile nella percentuale più elevata possibile" (art. 6, d.P.C.M. 2 marzo 2021).

In tale quadro, il Garante ha fornito indicazioni volte ad assicurare il rispetto delle disposizioni che prevedono che le attività di ricevimento o di erogazione diretta dei servizi al pubblico siano garantite con modalità telematica o comunque con modalità tali da escludere o limitare la presenza fisica negli uffici (ad es. appuntamento telefonico o assistenza virtuale) e, in pari tempo, il rispetto dei principi di protezione dei dati (art. 5 del RGPD), chiarendo, ad esempio, che la finalità di fornire agli utenti recapiti utili a cui rivolgersi per assistenza o per essere ricevuti presso gli uffici può essere utilmente perseguita pubblicando i soli recapiti delle unità organizzative competenti (numero di telefono e indirizzo Pec) e non quelli dei singoli funzionari preposti agli uffici; ciò anche in conformità agli obblighi di pubblicazione concernenti l'organizzazione delle p.a. (v. FAQ n. 3).

Per le medesime ragioni legate all'emergenza, stante la sospensione dell'attività didattica e delle riunioni degli organi collegiali in presenza, e tenuto conto dell'attivazione di modalità di didattica a distanza e del ricorso al lavoro agile con riguardo ai servizi amministrativi, sono stati forniti chiarimenti, anche alla luce delle indicazioni del Ministro per la pubblica amministrazione e del Ministro dell'istruzione, con riguardo agli aspetti di protezione dei dati riferiti ai docenti e al personale amministrativo (v. FAQ relative al trattamento dei dati nel contesto scolastico, spec. FAQ n. 4).

Piattaforme

Sin dalle prime settimane di emergenza epidemiologica, il Garante ha ritenuto necessario fornire indicazioni a scuole e atenei per orientare scelte consapevoli riguardo alle piattaforme da impiegare, sulla base delle garanzie offerte dai fornitori, in considerazione degli specifici rischi derivanti dal trattamento di dati personali di docenti e altro personale scolastico, alunni e famiglie (provv. 26 marzo 2020, n. 64, doc. web n. 9300784). In particolare, è stato ribadito l'obbligo di rispettare presupposti e condizioni per il legittimo impiego di strumenti tecnologici nel contesto lavorativo in relazione al trattamento di dati personali dei docenti, funzionali allo svolgimento della didattica a distanza da parte di scuole e università (artt. 5 e 88, par. 2, del RGPD; art. 114 del Codice; art. 4, l. 20 maggio 1970, n. 300), utilizzando i soli dati strettamente necessari, senza effettuare indagini sulla sfera privata (art. 113 del Codice) o interferire con la libertà di insegnamento (per tali profili v. più diffusamente par. 4.3.1).

Tale tematica è stata successivamente approfondita con il documento, predispo-

sto in collaborazione con il Ministero dell'istruzione, recante "Linee guida in materia di didattica digitale integrata e tutela della *privacy*: indicazioni generali" (in www.istruzione.it/rientriamoascuola/domandeerisposte.html): con esso è stato raccomandato alle istituzioni scolastiche di verificare, con il supporto del Rpd, che, in applicazione dei principi generali del trattamento dei dati e nel rispetto delle disposizioni che trovano applicazione ai rapporti di lavoro (art. 5 e 88 del RGPD), le piattaforme e gli strumenti tecnologici per l'erogazione della didattica digitale integrata (cd. DDI) consentano il trattamento dei soli dati personali necessari al perseguimento di tale finalità, configurando gli stessi nel rispetto della libertà di insegnamento e in modo da prevenire che vengano raccolte, anche involontariamente, informazioni relative alla vita privata. Più in dettaglio, è stato precisato che, in ragione del fatto che le piattaforme e gli strumenti tecnologici impiegati per la didattica possono comportare il trattamento di informazioni associate in via diretta o indiretta ai dipendenti, con possibilità di controllarne a distanza l'attività, dovrà essere verificata la sussistenza dei presupposti di liceità stabiliti dell'art. 4, l. 20 maggio 1970, n. 300 cui fa rinvio l'art. 114 del Codice, valutando in via preliminare se, tenuto conto delle concrete caratteristiche del trattamento, trovi applicazione il comma 1 o il comma 2 dello stesso articolo. Nel rispetto del principio di responsabilizzazione, l'istituzione scolastica dovrà adottare le misure tecniche e organizzative affinché il trattamento sia conforme alla richiamata normativa di settore, fornendo a tal fine le necessarie indicazioni al fornitore del servizio (cfr. artt. 24 e 25 del RGPD).

13.3. *I trattamenti di dati personali effettuati mediante sistemi di videosorveglianza*

Il Garante ha continuato ad occuparsi del trattamento dei dati effettuato attraverso sistemi di videosorveglianza installati presso luoghi di lavoro, rammentando ai titolari del trattamento l'obbligo di rispettare l'art. 114 del Codice (che rinvia all'art. 4, l. n. 300/1970), l'obbligo di fornire un'adeguata informativa agli interessati prima che entrino nel campo di ripresa delle telecamere nonché la necessità di effettuare il trattamento solo in presenza di una specifica condizione di liceità del trattamento.

Videosorveglianza in assenza di informativa

Sempre con riferimento ad un trattamento di dati personali effettuato attraverso un sistema di videosorveglianza, a seguito di una segnalazione, il Garante, dopo avere delegato al Nucleo speciale tutela *privacy* e frodi tecnologiche l'accertamento ispettivo presso la sede legale del titolare del trattamento, ha adottato un'ordinanza-ingiunzione nei confronti di una struttura ricettiva, avendo accertato che la stessa, a partire dal 2009 (e fino alla data dell'accertamento ispettivo), aveva utilizzato un impianto di videosorveglianza all'interno e all'esterno della struttura omettendo di apporre, in prossimità del raggio di azione delle telecamere, cartelli informativi idonei ad avvisare clienti, dipendenti e fornitori della esistenza e delle caratteristiche essenziali dell'attività di videoripresa, in contrasto con quanto stabilito dall'art. 13 del RGPD (provv. 26 novembre 2020, n. 256, doc. web n. 9533587).

Videosorveglianza non conforme all'autorizzazione

A seguito della presentazione di tre reclami aventi per oggetto i medesimi fatti, è stata irrogata una sanzione pecuniaria nei confronti di una società con la quale i reclamanti avevano stipulato un contratto di *catering* e *banqueting*. L'Autorità, a seguito dell'accertamento ispettivo presso la sede legale della società delegato al Nucleo speciale tutela *privacy* e frodi tecnologiche, ha accertato che il titolare del trattamento aveva fatto installare e utilizzato un impianto di videosorveglianza con caratteristiche non conformi a quanto prescritto nell'autorizzazione rilasciata dall'Ispettorato del lavoro ai sensi dell'art. 4, l. n. 300/1970, né, più in generale, alla disciplina di protezione dei dati personali. In particolare è emerso che: la società aveva fatto in-

stallare due telecamere in più rispetto a quelle autorizzate dall'Ispettorato; non si era conformata all'obbligo di informativa nei confronti di dipendenti e clienti; infine, il sistema di videosorveglianza era stato configurato in modo da consentire l'accesso da remoto alle immagini da parte del titolare del trattamento nonostante nella relazione tecnica presentata per ottenere l'autorizzazione fosse esclusa tale funzionalità (provv. 29 ottobre 2020, n. 213, doc. web n. 9518849).

Videosorveglianza in assenza di autorizzazione

Ha altresì formato oggetto di vaglio l'installazione, avvenuta ad opera di un'azienda sanitaria, di un sistema di videosorveglianza dotato di telecamere dislocate in aree nelle quali normalmente transitano o sostano anche i dipendenti (corridoi, ingressi, sale di attesa, pronto soccorso), con conseguente possibilità di controllarne indirettamente l'attività. Nel corso dell'istruttoria è emerso che l'installazione dei citati sistemi – avvenuta da oltre dieci anni in diverse strutture di competenza dell'azienda sanitaria e funzionale a esigenze di sicurezza e di tutela del patrimonio aziendale – fosse stata effettuata in assenza del necessario previo accordo con le organizzazioni sindacali o dell'autorizzazione da parte del competente Ispettorato del lavoro.

In base alla disciplina in materia di protezione dei dati personali, l'amministrazione, che opera in qualità di datore di lavoro, può trattare i dati personali dei dipendenti se il trattamento è necessario per la gestione del rapporto di lavoro e per adempiere a specifici obblighi o compiti previsti dalla normativa nazionale o dell'Unione (artt. 6, par. 1, lett. *c*); 9, par. 2, lett. *b*) e 4; 88 del RGPD) rispettando altresì le norme nazionali, preesistenti o di futura emanazione, che "includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati in particolare per quanto riguarda la trasparenza del trattamento […] e i sistemi di monitoraggio sul posto di lavoro" (cons. 155, artt. 6, par. 2 e 88, par. 2, del RGPD). Sul punto, il Codice, confermando l'impianto anteriore alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, fa espresso rinvio alle disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro, con particolare riferimento ai possibili controlli a distanza da parte del datore di lavoro (artt. 113 e 114 del RGPD).

In merito, nel solco di precedenti decisioni, l'Autorità ha ulteriormente chiarito che le esigenze di sicurezza e di tutela del patrimonio, pure invocate nel caso di specie dall'azienda, non sono per sé sole sufficienti a legittimare la presenza di tali dispositivi in luoghi ove si svolge anche l'attività lavorativa, comportando un trattamento di dati personali che può essere giustificato solo nel rispetto delle garanzie previste dalla legge nazionale applicabile (v. CEDU sent. 28 novembre 2017, n. 70838/13; v., da ultimo, Cepd, linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del 29 gennaio 2020). Pertanto, il rispetto dell'art. 4, comma 1, l. n. 300/1970, richiamato dall'art. 114 del Codice, costituisce condizione di liceità del trattamento dei dati personali (v. anche provv. 19 settembre 2019, n. 167, doc. web n. 9147290, spec. punto 4.2). Alla luce di tali considerazioni, il conseguente trattamento di dati personali posto in essere dall'azienda è stato ritenuto illecito in quanto sprovvisto di idoneo presupposto di liceità (in violazione degli artt. 5, comma 1, lett. *a*); 6, comma 1, lett. *c*); 88 del RGPD e 114 del Codice, in riferimento all'art. 4, l. n. 300/1970). Avendo l'azienda provveduto nel corso del procedimento ad avviare e concludere la procedura concertativa prescritta dalla legge, l'Autorità non ha disposto misure correttive, pur applicando una sanzione amministrativa pecuniaria (provv. 5 marzo 2020, n. 53, doc. web n. 9433080).

13.4. *I trattamenti di dati personali effettuati mediante posta elettronica e altri dispositivi tecnologici nel rapporto di lavoro*

L'Autorità è tornata a pronunciarsi sulle condizioni di liceità dei trattamenti dei dati personali dei lavoratori effettuati mediante dispositivi tecnologici utilizzati per rendere la prestazione lavorativa. In proposito, il Garante ha ribadito che la protezione della vita privata si estende anche all'ambito lavorativo, come più volte stabilito dalla Corte europea dei diritti dell'uomo che ritiene applicabile l'art. 8 della Convenzione europea dei diritti dell'uomo senza distinguere tra sfera privata e sfera professionale (v. Niemietz c. Allemagne, 16.12.1992, ric. n. 13710/88, par. 29; Copland c. UK, 3 aprile 2007, ric. n. 62617/00, par. 41; Bărbulescu v. Romania [GC], 5 settembre 2017, ric. n. 61496/08, parr. 70-73; Antović and Mirković v. Montenegro, 28 novembre 2017, ric. n. 70838/13, parr. 41-42).

Le decisioni rese sul punto tengono conto della necessità di applicare il vigente quadro normativo caratterizzato da reciproci rinvii operati dal legislatore – anche di recente, in sede di adeguamento dell'ordinamento nazionale alle norme del RGPD – tra la disciplina in materia di protezione dei dati personali (artt. 113, 114 e 171 del Codice; art. 88 del RGPD) e le norme di settore sui controlli a distanza (l. n. 300/1970).

Sistemi di *Work Force Management*

All'esito di un procedimento avviato a seguito della presentazione di un reclamo da parte di alcuni dipendenti di una società tramite una organizzazione sindacale, l'Autorità ha accertato che i trattamenti di dati personali dei lavoratori che operano come tecnici *on field*, effettuati mediante un sistema di *Work Force Management* (WFM), sono avvenuti in violazione di alcune disposizioni del RGPD sotto una molteplicità di profili. È in primo luogo emerso che i dati raccolti con il sistema, completo di funzionalità di geolocalizzazione, erano conservati nei sistemi aziendali – con possibilità di estrarre *report* individuali – per cinque anni, mentre l'informativa resa ai dipendenti indicava il diverso termine di sei mesi; in proposito l'Autorità ha ribadito che non incide sulla unitarietà della conservazione da parte del titolare la circostanza che quest'ultimo memorizzi i dati su banche dati distinte per periodi diversi di conservazione. L'informativa è altresì risultata priva dell'indicazione relativa all'utilizzo di un algoritmo in vista del raggiungimento di una pluralità di scopi non esplicitati con chiarezza agli interessati. Ciò ha comportato la violazione dell'obbligo di fornire una compiuta informativa ai dipendenti e, più in generale, del principio generale di correttezza (v. artt. 5, par. 1, lett. *a*), 13 e 22 del RGPD). L'Autorità ha altresì chiarito che non è conforme al RGPD individuare un unico termine di conservazione di dati raccolti in vista del raggiungimento di finalità diverse, considerato che il titolare deve procedere alla individuazione di tempi di conservazione delle diverse tipologie di dati personali trattati in relazione a ciascuno degli scopi in concreto perseguiti, evitando il riferimento "a blocchi" di fasce temporali omogenee. Inoltre, in occasione della valutazione di congruità dei tempi di conservazione, il titolare deve fare anzitutto riferimento alla finalità principale per la quale il sistema è adottato. Ciò, con riferimento al caso concreto, in quanto, conformemente alla disciplina di settore in materia di controlli a distanza, in particolare dall'art. 4, comma 3, l. n. 300/1970, e ai principi di protezione dei dati personali, il trattamento di dati dei dipendenti raccolti mediante sistemi tecnologici può essere lecitamente effettuato nei limiti dei dati raccolti e dell'arco temporale commisurato alla luce della specifica finalità di tipo organizzativo o produttivo o legata alla sicurezza del lavoro o alla tutela del patrimonio aziendale (scopi legislativamente previsti dall'art. 4, comma 1, l. n. 300/1970). Pertanto il titolare del trattamento è tenuto, in primo luogo, ad individuare la tipologia di dati personali riferiti ai dipendenti (identificati

o identificabili) la cui conservazione è necessaria per il conseguimento delle sopra richiamate finalità perseguite con il sistema e, quindi, a stabilire tempi congrui di conservazione in relazione a ciascuna delle stesse.

L'Autorità, tra le misure a garanzia degli interessati, ha stabilito che in applicazione dei principi di trasparenza e di correttezza, il sistema deve essere configurato in modo tale da rendere sempre visibile sullo schermo del dispositivo detenuto dal lavoratore un'icona che indichi se la funzionalità di localizzazione è attiva (v. art. 5, par. 1, lett. *a*), del RGPD).

Con riferimento, infine, alla prevista implementazione del sistema, il Garante ha chiarito che ogni ulteriore perfezionamento deve essere oggetto di valutazione d'impatto *privacy* nonché, per effetto del principio di liceità del trattamento, in linea con la disciplina lavoristica applicabile. Con specifico riguardo alla raccolta di dati relativi alla geolocalizzazione, è stato ribadito che non è conforme alle richiamate discipline sottoporre i dipendenti al monitoraggio continuo della posizione geografica.

Il Garante ha quindi disposto la limitazione definitiva del trattamento in relazione alla conservazione dei dati, impartito alcune prescrizioni ed altresì comminato una sanzione amministrativa pecuniaria (provv. 9 gennaio 2020, n. 8, doc. web n. 9263597).

Accesso alla casella di posta elettronica aziendale

L'Autorità si è pronunciata sul caso di una società che, cessato il rapporto di lavoro con un dipendente, avvalendosi dell'amministratore di sistema, aveva effettuato una ricerca sulle *e-mail* contenute nell'*account* aziendale (di tipo individualizzato) assegnato al medesimo e conservate sul *server* aziendale per oltre un anno. Alcune *e-mail* erano state così utilizzate per avviare un procedimento in sede giurisdizionale, mentre le altre risultavano ancora conservate dalla società in vista di futuri, possibili contenziosi. In proposito il Garante ha accertato, in primo luogo, che la società non aveva informato l'interessato, prima dell'inizio dei trattamenti, che tutte le *e-mail* in transito sull'*account* aziendale sarebbero state conservate sul *server* anche al fine di poter disporre controlli sul loro contenuto. Tale trattamento è stato dichiarato illecito in relazione agli artt. 12 e 13 del RGPD, in base ai quali il titolare è tenuto a fornire preventivamente all'interessato tutte le informazioni relative alle caratteristiche essenziali del trattamento; peraltro, come detto, nell'ambito del rapporto di lavoro l'obbligo di informare il dipendente è altresì espressione del principio generale di correttezza dei trattamenti (v. art. 5, par. 1, lett. *a*), del RGPD).

L'Autorità ha anche accertato che la sistematica conservazione sul *server* aziendale delle *e-mail* in entrata e in uscita (sia dei dati esterni che del loro contenuto) per un ampio arco temporale, il successivo accesso della società ai dati raccolti nel corso dell'attività lavorativa – attraverso un'indagine interna effettuata *a posteriori* volta a verificare possibili "acquisizioni fraudolente, utilizzazione indebita o rivelazione di segreti" –, nonché l'accesso, nel caso concreto, ad informazioni relative alla vita privata del lavoratore non rilevanti ai fini della valutazione dell'attitudine professionale dello stesso hanno comportato la violazione degli artt. 113 e 114 del Codice (che richiamano gli artt. 4 e 8, l. n. 300/1970 e l'art. 10, d.lgs. 10 settembre 2003, n. 276, quali condizioni di liceità del trattamento), disposizioni rientranti tra le norme del diritto nazionale "più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro", richiamate dall'art. 88 del RGPD.

Il Garante si è anche pronunciato sul regolamento interno relativo all'uso della posta elettronica aziendale adottato dalla società nel corso del procedimento, stabilendo che la sistematica conservazione, ivi prevista, per 12 mesi di tutte le *e-mail* presenti sull'*account* aziendale, in costanza del rapporto di lavoro, in vista di futuri

possibili contenziosi, non è conforme ai principi di minimizzazione dei dati (art. 5, par. 1, lett. *c*), del RGPD) e di limitazione della conservazione (art. 5, par. 1, lett. *e*), del RGPD). Medesima valutazione è stata riservata alla prospettata ulteriore conservazione per sei mesi del contenuto della casella di posta elettronica dopo la cessazione del rapporto di lavoro in relazione al compimento di possibili illeciti. In tale occasione l'Autorità ha ribadito che il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti, posto che tale trattamento risulterebbe elusivo delle disposizioni sui criteri di liceità del trattamento (v. artt. 6, par. 1, lett. *b*), *c*) e *f*) e 9, par. 2, lett. *b*), del RGPD; v., in proposito, provv. 1° febbraio 2018, n. 53, doc. web n. 8159221).

Con riferimento, poi, alla rappresentata finalità di poter far fronte ad eventuali contestazioni da parte di clienti, fornitori e p.a., il Garante ha ribadito che la legittima necessità di assicurare la conservazione di documentazione necessaria per l'ordinario svolgimento e la continuità dell'attività aziendale è assicurata, in primo luogo, dalla predisposizione di sistemi di gestione documentale con i quali – attraverso l'adozione di appropriate misure organizzative e tecnologiche – individuare i documenti che nel corso dello svolgimento dell'attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile; caratteristiche che i sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare.

Infine, il prospettato accesso sia ai dati esterni che al contenuto dei messaggi di posta elettronica costituisce, come già ritenuto in relazione ai fatti oggetto di reclamo, un trattamento di dati personali effettuato in violazione dell'art. 4, l. n. 300/1970, richiamato dall'art. 114 del Codice come condizione di liceità del trattamento (esercitando un controllo sull'attività del lavoratore), nonché in violazione dell'art. 8 della medesima l. n. 300/1970 e dell'art. 10, d.lgs. 10 settembre 2003, n. 276, richiamati dall'art. 113 del Codice (contenenti il divieto di effettuare indagini o comunque trattare dati che non siano strettamente attinenti alla valutazione dell'attitudine professionale del dipendente). Come già rilevato, rientrando la citata disciplina lavoristica tra le disposizioni del diritto nazionale richiamate dall'art. 88 del RGPD (come misura appropriata e specifica ai sensi del par. 2 del medesimo art. 88), essa non consente controlli massivi, prolungati e indiscriminati dell'attività del dipendente.

Il Garante pertanto, dichiarata l'illiceità dei trattamenti, ha disposto il divieto dell'ulteriore trattamento dei dati relativi ad *account* aziendali riferiti al reclamante e agli altri dipendenti, adottando altresì una prescrizione relativa al nuovo regolamento aziendale e una sanzione amministrativa pecuniaria (provv. 29 ottobre 2020, n. 214, doc. web n. 9518890).

Accesso alla cronologia della navigazione in internet

In altra vicenda oggetto di reclamo è emerso che il datore di lavoro aveva effettuato l'accesso al pc fornito in uso ad una dipendente estraendo la cronologia degli accessi ad internet, resa disponibile dal *browser*, per utilizzare le informazioni così raccolte nell'ambito di una contestazione disciplinare. Tale operazione è stata resa possibile dalla condivisione della *password* di accesso tra la lavoratrice e il legale rappresentante della società. Il Garante ha in primo luogo accertato che tale condivisione contrasta con l'obbligo di adottare misure di sicurezza volte ad assicurare "un livello minimo di protezione dei dati personali" (v. art. 33 del Codice, testo vigente all'epoca dei fatti). Infatti, nell'ambito dei sistemi di autenticazione informatica, le credenziali di autenticazione assegnate agli incaricati consistono, quantomeno, in un codice di identificazione associato ad una parola chiave conosciuta esclusivamente

dall'interessato (v. quanto già stabilito nel Disciplinare tecnico in materia di misure minime di sicurezza, regole 1-11, all. B) al Codice, testo precedente alle modifiche poste con d.lgs. n. 101/2018). Tale principio trova conferma nell'art. 32 del RGPD, in base al quale il titolare del trattamento, al fine di garantire la riservatezza e l'integrità dei sistemi informatici, deve adottare "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio". Inoltre, in base all'art. 5, par. 1, lett. *f*), del RGPD, il titolare deve garantire "un'adeguata sicurezza dei dati personali" applicando i principi di "integrità e riservatezza" ai trattamenti effettuati.

Nel caso esaminato è stato altresì accertato che l'informativa fornita dal datore di lavoro alla dipendente – espressione del principio generale di correttezza dei trattamenti (v. art. 11, comma 1, lett. *a*), del Codice, testo vigente all'epoca dell'accesso al pc della reclamante; principio ribadito nell'art. 5, par. 1, lett. *a*), del RGPD) – non conteneva alcuna indicazione sull'uso consentito della posta elettronica, degli altri strumenti di lavoro e dell'accesso ad internet; né era ivi presente alcuna indicazione relativa alla tipologia di controlli che il datore di lavoro si riservava di attivare in relazione all'utilizzo degli strumenti da parte dei lavoratori. Ciò è risultato in violazione dell'art. 13 del Codice, nel testo vigente all'epoca dei fatti (principio ora rinvenibile nell'art. 13 del RGPD).

All'esito dell'istruttoria è altresì emerso che il titolare del trattamento aveva riscontrato solo in parte le istanze di accesso presentate dalla lavoratrice, rigettando l'accesso ai dati contenuti nel pc (ad eccezione di quelli selezionati e riversati in una chiavetta USB) e ad alcune pagine dell'agenda utilizzata dalla reclamante, rimosse prima della sua consegna; anche la richiesta volta a verificare l'esistenza di ulteriori documenti personali all'interno della stanza a suo tempo assegnata per lo svolgimento dell'attività lavorativa era rimasta disattesa. Tale riscontro parziale è avvenuto in assenza di alcun riferimento da parte del titolare ad una delle ipotesi di limitazione dei diritti previste dall'art. 23 del RGPD (successivamente disciplinate dall'art. 2-*undecies* del Codice).

Pertanto il Garante, accertata l'illiceità dei trattamenti effettuati dal titolare in relazione ai profili sopra indicati, nonché in relazione a quanto disposto dall'art. 4, l. n. 300/1970, come modificato dal d.lgs. n. 151/2015, ha disposto la limitazione dell'ulteriore trattamento dei dati raccolti, impartito alcune prescrizioni e comminato una sanzione amministrativa pecuniaria (provv. 26 marzo 2020, n. 65, doc. web n. 9446730).

Gestione di *account* di posta elettronica aziendale durante il periodo di malattia

L'Autorità ha ritenuto non conforme al RGPD la disattivazione dell'*account* di posta elettronica aziendale operata dal datore di lavoro durante il periodo di malattia del lavoratore interessato. All'esito dell'istruttoria avviata a seguito di un reclamo è infatti emerso che tale operazione non costituiva applicazione di (asserite) procedure di sicurezza standard. Ciò anche alla luce del fatto che l'informativa fornita non conteneva alcun riferimento alla possibilità per l'azienda di effettuare tale specifica modalità di trattamento per il raggiungimento di finalità legittime rese note preventivamente, come previsto in via generale dall'art. 13 del RGPD e, nello specifico contesto del rapporto di lavoro, in applicazione del principio generale di correttezza (ex art. 5, par. 1, lett. *a*), del RGPD). Il Garante ha quindi prescritto al titolare di dare corso all'istanza di accesso ai dati contenuti nell'*account* di posta elettronica a suo tempo presentata dal reclamante ed ha comminato una sanzione amministrativa pecuniaria (provv. 9 luglio 2020, n. 145, doc. web n. 9474649).

Anche in un altro caso esaminato dall'Autorità è stata lamentata la modifica da parte del datore di lavoro della *password* di accesso all'*account* di posta elettronica di tipo individualizzato assegnato al lavoratore in pendenza dello stato di malattia. All'esito del procedimento è stato accertato che il titolare non aveva fornito alcuna

informativa circa la ritenuta necessità di una autorizzazione per accedere alla posta elettronica in costanza di malattia, né circa la facoltà del datore di lavoro di provvedere – anche per mezzo del web *agent* – al cambio di *password* di accesso all'*account* di posta elettronica individuale ogni quattro mesi e, più in generale, in ordine alle regole generali sul funzionamento e al corretto utilizzo dell'*account* aziendale. Considerato che il titolare, nel corso del procedimento, ha dichiarato di aver provveduto a comunicare al dipendente la *password* di accesso nel momento del ritorno in azienda e di avere disattivato l'*account* di posta elettronica aziendale intestato al reclamante successivamente all'interruzione del rapporto di lavoro con quest'ultimo, nel frattempo intervenuto, il Garante ha ritenuto che, non essendo il trattamento più in essere, non vi fossero gli estremi per adottare provvedimenti inibitori né prescrittivi. Tuttavia, avendo accertato la violazione dell'art. 13 del RGPD, l'Autorità ha ammonito il titolare del trattamento sulla necessità di conformare la gestione degli *account* di posta elettronica aziendale durante il rapporto di lavoro alle disposizioni ed ai principi in materia di protezione dei dati personali (provv. 19 maggio 2020, n. 91, doc. web n. 9441579).

13.5. *I trattamenti di dati personali relativi alla persistente attivazione dell'*account *di posta elettronica aziendale dopo la cessazione del rapporto di lavoro*

Una parte significativa dei reclami e delle altre tipologie di istanze rivolte all'Autorità in materia di rapporti di lavoro continua a riguardare il persistente utilizzo da parte del datore di lavoro di *account* di posta elettronica aziendale di tipo individualizzato (contenente il nome e/o il cognome della lavoratrice o del lavoratore) anche dopo che il rapporto di lavoro, in forza del quale l'*account* è stato assegnato, si è interrotto.

Reindirizzamento dell'*account* aziendale

Nel caso oggetto di decisione, l'Autorità ha accertato che l'*account* di posta elettronica aziendale di tipo individualizzato assegnato da una società ad un lavoratore era rimasto attivo per circa dieci mesi dopo la cessazione del rapporto di lavoro, all'insaputa dell'interessato, ed i messaggi in arrivo erano stati reindirizzati sull'*account* dell'ex superiore gerarchico del reclamante. Ciò ha consentito al titolare del trattamento (datore di lavoro) di accedere alla corrispondenza elettronica pervenuta sulla casella di posta, proveniente da soggetti interni ed esterni all'ambito lavorativo. La società ha in questo modo appreso alcune informazioni personali relative all'interessato riguardanti non solo i dati cd. esterni delle comunicazioni e gli eventuali *file* allegati, ma anche il contenuto delle stesse che, come accertato dall'Autorità, riguardavano non soltanto l'attività professionale, ma anche aspetti della sfera personale del reclamante in relazione ai quali quest'ultimo e i terzi coinvolti (i cui diritti devono essere parimenti tutelati) vantavano legittime aspettative di riservatezza.

L'Autorità ha pertanto accertato la violazione di una pluralità di disposizioni del RGPD, in primo luogo degli articoli 12 e 15 per non aver dato corso all'istanza di accesso del reclamante ai dati contenuti nella casella di posta elettronica se non dopo la presentazione del reclamo. Posto che il trattamento in concreto effettuato è risultato difforme da quanto prospettato nel documento informativo fornito dalla società ai dipendenti, è stata accertata la violazione dell'obbligo di informativa (art. 13 del RGPD) che, come detto, nell'ambito del rapporto di lavoro è altresì espressione del principio generale di correttezza (art. 5, par. 1, lett. *a*), del RGPD). In relazione alla persistente attività dell'*account* di posta elettronica aziendale per un periodo significativo di tempo dopo la cessazione del rapporto di lavoro e il conseguente accesso a contenuti sia professionali che privati riferiti all'interessato, il

Garante ha ribadito che, come già stabilito con le linee guida per posta elettronica e internet adottate il 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58), il datore di lavoro deve adottare misure tecnologiche e organizzative volte a contemperare il legittimo interesse del titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività con l'aspettativa di riservatezza della corrispondenza dell'ex dipendente e di terzi. Dopo la cessazione del rapporto di lavoro, pertanto, la società avrebbe dovuto rimuovere l'*account* previa disattivazione dello stesso con la contestuale adozione di sistemi automatici volti ad informarne i terzi e a fornire a questi ultimi indirizzi alternativi riferiti alla propria attività professionale (ciò in applicazione dei principi stabiliti dall'art. 5, par. 1, lett. *a*), *c*) e *e*), del RGPD). Nel corso del procedimento la società ha provveduto ad adottare una *policy* interna conforme ai suesposti principi in applicazione del processo di responsabilizzazione previsto dal Regolamento, considerato che il contemperamento degli interessi effettuato dal titolare del trattamento nell'ambito dell'attività di cd. *accountability* non può non tenere conto di quanto stabilito dall'Autorità con propri provvedimenti. All'esito della procedura di accertamento delle violazioni, il Garante ha altresì comminato una sanzione amministrativa pecuniaria (provv. 2 luglio 2020, n. 115, doc. web n. 9445180).

13.6. *Diritto alla protezione dei dati personali e tutela della dignità dei lavoratori*

È stata riaffermata l'importanza e la necessità di tutelare la dignità dei lavoratori – da intendersi come "valore costituzionale che permea di sé il diritto positivo" – attraverso il diritto alla protezione dei dati personali.

Pubblicazione in bacheca della lettera di licenziamento

In particolare, a seguito di un reclamo nel quale è stata lamentata l'affissione della lettera di licenziamento senza giusta causa della reclamante nella bacheca aziendale posta presso il punto vendita del supermercato dove la stessa prestava la propria attività lavorativa, visibile a tutti i dipendenti, il Garante ha irrogato una sanzione amministrativa pecuniaria nei confronti del titolare del trattamento ritenendo illecito il trattamento, avvenuto in assenza di un'idonea base giuridica (art. 6, par. 1, lett. *b*) e *c*), del RGPD). L'Autorità ha in proposito precisato che in materia di procedimento relativo alla risoluzione del rapporto di lavoro per giustificato motivo oggettivo è previsto l'obbligo di comunicazione nei confronti del lavoratore, non di terzi. La pubblicazione della lettera di licenziamento rende conoscibile a terzi le specifiche ragioni del recesso e le informazioni contenute nella stessa che, seppur non annoverabili, di regola, nell'ambito delle categorie particolari di dati (ex art. 9 del RGPD), sono da considerare meritevoli di particolare tutela, anche in ragione delle conseguenze sul piano economico e sociale che derivano dal recesso stesso. Il trattamento è stato effettuato anche in violazione del principio di proporzionalità, in base al quale il datore di lavoro avrebbe potuto informare i dipendenti che la reclamante non faceva più parte della compagine aziendale con altre modalità, nel rispetto della riservatezza e della dignità, anche professionale, dell'interessata (v. art. 5, par. 1, lett. *a*) e *c*), del RGPD) (provv. 2 luglio 2020, n. 124, doc. web n. 9445567).

Dignità dei lavoratori in un *call center*

L'Autorità ha ribadito la centralità della protezione dei dati per la tutela della dignità di lavoratori e lavoratrici irrogando, a seguito di una segnalazione presentata da un'associazione sindacale, una sanzione pecuniaria ad una società di servizi di *call center*, impartendole specifiche prescrizioni. In particolare, all'esito dell'istruttoria è risultato che la società aveva imposto ai propri dipendenti, attraverso disposizioni interne, di "esporre sul tavolo di lavoro oggetti prettamente personali quali medicinali, presidi medici, assorbenti, salviette umidificate, che il lavoratore utilizza nel corso

della prestazione lavorativa anche al di fuori delle ipotesi in cui è possibile recarsi previamente presso l'armadietto assegnato per prelevare tali oggetti di uso personale […]. Ciò senza la possibilità di posizionare tali oggetti all'interno di astucci o comunque contenitori di piccole dimensioni al fine di sottrarli alla visibilità altrui (di colleghi e superiori gerarchici) con conseguente possibilità per costoro di apprendere o desumere stati o situazioni personali o informazioni relative allo stato di salute estranei al contenuto della prestazione lavorativa e lesive della dignità e riservatezza del dipendente". In proposito è emerso che le particolari disposizioni impartite ai lavoratori (oggetto di segnalazione) non sono risultate conformi ai principi di liceità (v. art. 6, par. 1, lett. *b*) e *c*), art. 9, par. 2, lett. *b*), del RGPD) e minimizzazione dei dati (v. art. 5, par. 1, lett. *a*) e *c*), del RGPD), considerato che la legittima finalità di prevenire possibili accessi illeciti ai dati trattati per conto dei committenti nell'ambito della fornitura del servizio di *call center* può e deve essere perseguita astenendosi dal trattare dati personali dei lavoratori, anche di natura particolare, la cui sottoposizione alla altrui conoscibilità comporta l'eliminazione di ogni spazio di riservatezza e di intimità sul luogo di lavoro, consentendo a terzi di apprendere sia lo stato di salute sia la sussistenza di condizioni normalmente tenute riservate dagli interessati nella vita di relazione, con conseguente violazione della dignità della persona, intesa come valore costituzionale che permea di sé il diritto positivo (v. Corte cost., 17 luglio 2020, n. 293; si veda anche Corte cost., 19 dicembre 1991, n. 467; art. 1 CDFUE; art. 1 del Codice; v. altresì art. 88, par. 2, del RGPD). Tenuto conto di ciò, l'Autorità ha ingiunto alla società di conformare ai principi di liceità e minimizzazione previsti dal RGPD i trattamenti effettuati sulla base del regolamento aziendale in fase di elaborazione al momento della pronuncia, impedendo (mediante l'adozione di opportuni accorgimenti) l'acquisizione di informazioni correlate all'uso di oggetti strettamente personali (provv. 26 novembre 2020, n. 235, doc. web n. 9509515).

13.7. *Esercizio dei diritti e rapporto di lavoro*

Nell'esaminare alcuni reclami, è stato rammentato ai titolari del trattamento l'obbligo di agevolare l'esercizio dei diritti riconosciuti agli interessati ai sensi dell'art. 12 del RGPD, fornendo un chiaro ed adeguato riscontro agli stessi nel rispetto dei termini individuati dall'ordinamento. È stato precisato che, anche nel caso di inottemperanza alle istanze di esercizio dei diritti, grava sul titolare del trattamento l'obbligo di manifestare il diniego con la chiara indicazione dei motivi sottostanti, indicando altresì la possibilità di presentare reclamo al Garante o, in alternativa, ricorso giurisdizionale.

In sede di decisione di un reclamo avente ad oggetto l'esercizio del diritto di accesso ai dati relativi al reclamante, un dipendente coinvolto in un'indagine interna effettuata dall'Organismo di vigilanza della banca (datore di lavoro), l'Autorità ha sottolineato che in capo al titolare del trattamento grava l'obbligo di fornire un tempestivo ed effettivo riscontro all'interessato. È stato altresì precisato che, in base all'art. 12, par. 4, del RGPD, il titolare del trattamento deve informare l'interessato anche qualora ritenga di non dare seguito alla richiesta, indicandone i motivi, informando l'interessato della facoltà di proporre reclamo al Garante o ricorso giurisdizionale. L'Autorità ha ritenuto quindi non conforme agli artt. 5, par. 1, lett. *a*), 12, parr. 3 e 4, nonché 15 del RGPD la condotta della banca che, considerando l'istanza di accesso ripetitiva (in quanto già presentata), non aveva dato un riscontro, neanche informale, all'interessato. In proposito l'Autorità, richiamata la giurisprudenza di legittimità, ha ribadito che il diritto di accesso non può essere limitato alla conoscenza di dati nuovi ed ulteriori rispetto a quelli già conosciuti, ma deve consentire

all'interessato una verifica effettiva del trattamento che viene effettuato su tutti i dati a sé riferiti (provv. 23 aprile 2020, n. 76, doc. web n. 9426302).

Esercizio dei diritti in fase preassuntiva

L'obbligo del titolare del trattamento di fornire un tempestivo riscontro alle istanze di esercizio dei diritti previsto dall'art. 12, parr. 3 e 4, del RGPD è stato ribadito in un provvedimento adottato a seguito di un reclamo avente ad oggetto i diritti di accesso e di cancellazione concernente i dati forniti nell'ambito di una procedura di selezione per un posto di lavoro. Il titolare del trattamento, stabilito in un Paese terzo e nei confronti del quale la disciplina di protezione dei dati trovava applicazione ai sensi dell'art. 3, par. 2, del RGPD, è stato così ammonito per avere fornito un riscontro tardivo: l'Autorità ha pertanto ritenuto che tale condotta abbia violato l'art. 12, par. 3 e 4 nonché gli artt. 15 e 17 del RGPD, ammonendo la società sulla necessità di fornire riscontro tempestivamente alle istanze relative all'esercizio dei diritti presentate dagli interessati (provv. 24 giugno 2020, n. 111, doc. web n. 9445163).

Diritto di accesso e richiesta di informazioni da parte dell'Autorità

Nel decidere un reclamo con il quale è stata lamentata l'impossibilità di accedere ai dati riferiti al reclamante concernenti il rapporto di lavoro (contenuti in fogli di registrazione e tabulati estratti dal cronotachigrafo e "scaricati" dalla carta del conducente relativa ai viaggi effettuati) è stata comminata una sanzione pecuniaria per l'omesso riscontro all'interessato come pure in relazione alla richiesta di informazioni formulata dall'Autorità ai sensi dell'art. 157 del Codice. Sono stati ritenuti violati, per tali ragioni, gli artt. 12 e 15 del RGPD nonché 157 del Codice (provv. 2 luglio 2020, n. 125, doc. web n. 9445710).

Diritto di accesso e alla cancellazione di dati nei confronti di un consulente tecnico di parte

La necessità di consentire un esercizio effettivo dei diritti riconosciuti in capo agli interessati è stata ribadita dal Garante anche al di fuori del rapporto di lavoro: in particolare ciò è stato affermato in sede di decisione di un reclamo – collegato ad un diverso procedimento relativo al trattamento di dati in ambito lavorativo – avente ad oggetto l'esercizio del diritto di accesso e alla cancellazione di dati riferiti alla reclamante raccolti, esaminando il pc di un soggetto terzo, da una società designata consulente tecnico di parte nell'ambito di un procedimento giudiziario rispetto al quale la reclamante era estranea.

In tale occasione il Garante, nel precisare che le regole deontologiche relative a trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria (che hanno sostituito il preesistente codice di deontologia) trovano applicazione anche nei confronti di chiunque effettui tali trattamenti – in particolare nei confronti di liberi professionisti o soggetti che in conformità alla legge prestino, su mandato, attività di assistenza o consulenza per le medesime attività –, ha rammentato che le linee guida in materia di trattamento di dati personali da parte di consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero (adottate dall'Autorità il 26 giugno 2008 e pubblicate in G.U. 31 luglio 2008, n. 178) contengono anche specifiche indicazioni per i trattamenti di dati effettuati da soggetti nominati consulenti tecnici dalle parti private con riferimento a procedimenti giudiziari.

Nel caso di specie l'Autorità ha rinvenuto nella condotta tenuta dalla società che non ha fornito un tempestivo ed effettivo riscontro all'interessata relativamente alle istanze di esercizio dei diritti di accesso e alla cancellazione dei dati una violazione dell'art. 12, parr. 3 e 4, del RGPD con riferimento agli artt. 15 e 17 del RGPD; per tale ragione, ha ammonito la stessa sulla necessità di fornire riscontro tempestivamente alle istanze relative all'esercizio dei diritti, anche nel caso in cui ritenga di non ottemperare alle richieste (provv. 29 ottobre 2020, n. 203, doc. web n. 9487946).

13.8. *I trattamenti di dati personali dei candidati nell'ambito di procedure concorsuali*

A seguito di una segnalazione con la quale si lamentava che i dati personali dei candidati di un concorso pubblico indetto da un'azienda ospedaliera – anche relativi alla salute (contenute in titoli di preferenza e certificazioni mediche allegate all'atto di presentazione della domanda di partecipazione) – fossero liberamente accessibili *online* mediante il semplice collegamento alla piattaforma utilizzata nell'ambito della procedura concorsuale, l'Autorità ha avviato una complessa istruttoria sia nei confronti dell'azienda, sia della società fornitrice della piattaforma informatica. In particolare, è stato verificato che, attraverso il semplice collegamento alla piattaforma per l'acquisizione e gestione delle domande, era possibile visualizzare un elenco di codici, assegnati ai candidati al momento dell'iscrizione al concorso. Essi consentivano l'accesso a un'area del portale nella quale erano contenuti i documenti allegati alle domande di partecipazione al concorso e altri dati personali riferiti ai candidati. Peraltro, tali documenti erano liberamente modificabili, con potenziale pregiudizio per gli interessati, atteso che un'eventuale discrepanza fra quelli presentati dai candidati e quelli esaminati dall'azienda avrebbe potuto determinare conseguenze gravi, quali l'esclusione dal concorso o il mancato riconoscimento di eventuali titoli di preferenza.

Il Garante ha rilevato che il trattamento dei dati personali dei candidati è stato effettuato in assenza di un'idonea base giuridica nonché senza che fossero state fornite agli interessati tutte le informazioni di cui all'art. 13 del RGPD. È stato poi accertato che l'impresa, titolare del trattamento sul quale ricade quindi una "responsabilità generale" sulle operazioni poste in essere (v. artt. 5, par. 2 e 24 del RGPD), non aveva disciplinato il rapporto con la società fornitrice ai sensi dell'art. 28 del RGPD, avendo omesso di impartire le necessarie istruzioni e di svolgere la necessaria attività di vigilanza. Considerato che l'incidente di sicurezza nell'ambito della procedura concorsuale si è verificato in conseguenza della mancata adozione di misure tecniche e organizzative adeguate ad assicurare la riservatezza e l'integrità dei dati personali trattati mediante l'ausilio della piattaforma gestita dalla società fornitrice, il Garante ha rilevato violazioni imputabili, seppur con diverso grado di responsabilità, non solo al titolare del trattamento ma anche alla società.

In occasione delle verifiche effettuate sulle circostanze da valutare ai sensi dell'art. 83, par. 2, del RGPD ai fini della quantificazione della sanzione applicabile alla vicenda in esame è stato altresì possibile accertare che, in violazione di quanto stabilito all'art. 28 del RGPD, i dati forniti in sede di presentazione della domanda dai singoli candidati fossero ancora accessibili sulla piattaforma gestita dal fornitore, nonostante la sopravvenuta cessazione del rapporto contrattuale con l'azienda.

Per tali ragioni sono state comminate sanzioni amministrative pecuniarie nei confronti sia dell'azienda che del fornitore, disponendo altresì, per quanto concerne quest'ultimo, la limitazione dei trattamenti in corso e vietando ogni ulteriore operazione di trattamento con riguardo ai dati personali dei candidati ad eccezione di quanto necessario per l'accertamento, l'esercizio o la difesa dei diritti in sede giudiziaria (provv.ti 17 settembre 2020, n. 160 e n. 161, doc. web nn. 9461168 e 9461321).

13.9. *I trattamenti di dati personali nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti (cd.* whistleblowing*)*

L'Autorità ha affrontato il tema dei trattamenti dei dati personali nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti da parte dei

dipendenti e di soggetti terzi, come previsto dalla disciplina del cd. *whistleblowing*.

In particolare, a seguito della notifica al Garante ai sensi dell'art. 33 del RGPD da parte di un ateneo dell'avvenuta diffusione sui motori di ricerca di dati personali comuni riferiti a due segnalanti (nominativi ed indirizzi *e-mail*) per il tramite della piattaforma utilizzata dal medesimo ateneo per l'acquisizione e la gestione delle segnalazioni, l'Autorità ha proceduto a ulteriori verifiche dalle quali è emerso che tali dati identificativi, presenti in alcune delle pagine web dell'applicativo, erano indicizzati e liberamente ritracciabili da chiunque in rete con l'ausilio di comuni motori di ricerca. Gli accertamenti effettuati hanno messo in evidenza che i trattamenti posti in essere dall'ateneo in attuazione della disciplina di settore in materia di tutela dell'identità del dipendente che segnala illeciti (art. 54-*bis*, d.lgs. 30 marzo 2001, n. 165, modificato dalla l. 30 novembre 2017, n. 179), sebbene necessari per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento (artt. 6, par. 1, lett. *c*), 9, par. 2, lett. *b*), del RGPD, in relazione all'art. 54-*bis*, cit.) e per l'esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (artt. 6, par. 1, lett. *e*) e 9, par. 2, lett. *g*), del RGPD), fossero avvenuti in violazione della disciplina in materia di protezione dei dati. Ciò con particolare riguardo all'inidoneità delle misure tecniche e organizzative volte ad assicurare l'integrità e la riservatezza dei dati in riferimento sia al controllo degli accessi sia al trasporto e alla conservazione dei dati (artt. 5, par. 1, lett. *f*) e 32 del RGPD). Contrariamente a quanto rappresentato dall'ateneo, infatti, la reperibilità sul web di tali dati personali è stata ritenuta indicativa del fatto che le pagine web in questione fossero esposte su rete pubblica in assenza di misure tecniche che avrebbero dovuto consentire di limitare l'accesso ai soli soggetti autorizzati dotati di credenziali di autenticazione e di uno specifico profilo di autorizzazione. A tal riguardo, è stato considerato che il titolare del trattamento è tenuto comunque ad adottare apposite procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (art. 32, par. 1, lett. *d*), del RGPD).

Pertanto, nel caso di specie, in cui l'ateneo si era limitato a recepire le scelte progettuali del fornitore dell'applicativo *whistleblowing*, la riduzione dell'efficacia delle misure tecniche per il controllo degli accessi è stata ritenuta riconducibile alla sfera di responsabilità del titolare del trattamento.

L'Autorità ha altresì precisato che, anche tenuto conto della natura, dell'oggetto e della finalità del trattamento, nonché dell'elevato rischio per i diritti e le libertà dei segnalanti, il mancato utilizzo di strumenti di crittografia per il trasporto dei dati fosse in contrasto con l'art. 32 del RGPD (v. anche le linee guida in materia di tutela del dipendente pubblico che segnala illeciti adottate da Anac con delibera 28 aprile 2015, n. 6). Peraltro, la necessità di adottare misure tecniche e organizzative adeguate in relazione alle procedure informatiche per l'acquisizione e gestione delle segnalazioni di presunti illeciti mediante protocolli sicuri di trasporto dei dati era stata evidenziata dal Garante anche in occasione del parere reso sullo schema di linee guida dell'Anac in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-*bis*, d.lgs. n. 165/2001 (cfr. provv. 4 dicembre 2019, n. 215, doc. web n. 9215763).

Ad analoghe conclusioni è pervenuta l'Autorità anche in relazione alla mancata adozione di misure per la cifratura dei dati personali (dati identificativi del segnalante, informazioni relative alla segnalazione nonché eventuale documentazione allegata) conservati nel *database* utilizzato dal medesimo applicativo.

Per tali ragioni, rilevata l'illiceità del trattamento e considerata la particolare gravità della violazione rispetto a trattamenti la cui disciplina di settore prevede, a tu-

tela dell'interessato, un elevato grado di riservatezza, e tenuto conto della rilevante inadeguatezza degli accorgimenti adottati sotto il profilo tecnico e organizzativo in relazione alle stringenti esigenze di sicurezza e particolare riservatezza proprie della gestione dei dati nell'ambito delle procedure di *whistleblowing*, l'Autorità ha comminato una sanzione amministrativa pecuniaria all'ateneo (provv. 23 gennaio 2020, n. 17, doc. web n. 9269618).

13.10. *I trattamenti di dati personali di dipendenti pubblici e di utenti mediante il sistema di prenotazione e gestione dei servizi*

Con riguardo al tema dell'utilizzo di *app* nel settore pubblico, il Garante ha adottato un provvedimento sanzionatorio nei confronti di un comune per illecito trattamento di dati personali di utenti e, per quanto qui più precisamente interessa, dipendenti effettuato attraverso il sistema per la gestione delle prenotazioni dei servizi erogati al pubblico e delle code allo sportello (cfr. in merito anche par. 4.5.4). Tale decisione fa seguito a un precedente provvedimento con il quale era stato ingiunto al medesimo comune di conformare il trattamento alle disposizioni del RGPD e del Codice e di adottare adeguate azioni correttive volte ad eliminare le criticità tecniche e organizzative del sistema (provv. 7 marzo 2019, n. 81, doc. web n. 9121890).

I trattamenti hanno interessato un'ingente mole di dati personali, anche particolarmente delicati, in quanto relativi a prenotazioni di vari servizi e di prestazioni sanitarie. Il sistema consentiva, infatti, di acquisire e memorizzare sui *server* del comune, per un ampio arco temporale, numerosi dati relativi alle prenotazioni riferiti sia agli utenti (tipo di prestazione, canale utilizzato, data e ora della prenotazione), sia al personale impiegato nella gestione degli appuntamenti; a quest'ultimo proposito, infatti, il sistema registrava e generava *report* giornalieri contenenti anche informazioni di dettaglio sull'attività lavorativa (data, tipo di servizio, nominativo dell'addetto allo sportello, tempo di chiamata e tempo di attesa). Tutte le operazioni erano effettuate senza che né gli utenti né i dipendenti avessero ricevuto, come previsto dal RGPD, un'informativa completa sui trattamenti effettuati tramite l'applicativo. Il Garante ha ritenuto inadeguate anche le misure tecniche e organizzative implementate dall'ente, il quale non aveva disciplinato il rapporto con la società fornitrice del sistema di prenotazione. Inoltre è stata ritenuta non conforme al quadro giuridico in materia di protezione dei dati la funzione che consente di produrre *report* sull'attività degli addetti allo sportello, introdotta senza le necessarie garanzie previste dallo Statuto dei lavoratori sui controlli a distanza.

Ai fini della quantificazione della sanzione amministrativa pecuniaria, l'Autorità ha valutato, tra l'altro, le scelte organizzative dell'ente, anche sotto il profilo della corretta individuazione della figura del Responsabile della protezione dei dati, soggetta ad avvicendamenti nel corso dell'istruttoria, circostanza che ha reso meno efficace la cooperazione con il Garante (provv. 17 dicembre 2020, n. 280, doc. web n. 9524175). Con separato provvedimento è stata comminata una sanzione amministrativa anche alla società fornitrice del sistema per i trattamenti effettuati in qualità di autonomo titolare, in particolare con riguardo alla prenotazione di servizi sanitari da parte degli utenti e alla manutenzione del sistema per conto dei clienti (provv. 17 dicembre 2020, n. 281, doc. web n. 9525315).

Dall'istruttoria è emerso che la maggior parte degli addebiti nei confronti dell'ente derivavano anche dalle specifiche caratteristiche del sistema il quale, nella versione standard (originariamente distribuita dalla società), non consentiva di configurare caso per caso la tipologia dei dati trattati e i tempi massimi di conservazione, e

quindi di rispettare i principi applicabili al trattamento dei dati (art. 5 del RGPD). Pertanto, tenuto conto del diffuso utilizzo del sistema da parte di numerosi soggetti pubblici e privati (enti istituzionali, strutture sanitarie ed imprese), nei confronti della medesima società fornitrice e dei fruitori dello stesso, è stato adottato un provvedimento di avvertimento ai sensi dell'art. 58, par. 2, lett. *a*), del RGPD, volto a prevenirne l'impiego con le modalità censurate dal Garante, ingiungendo alla società di avviare i necessari aggiornamenti per conformarsi alla disciplina in materia di protezione dati. A seguito del provvedimento di avvertimento, che nell'ambito dei poteri correttivi attribuiti dal RGPD all'autorità di controllo consente un'azione che fa leva sul principio di responsabilizzazione (art. 5, par. 2, del RGPD) prescindendo dall'accertamento di una specifica violazione (e quindi dall'adozione delle conseguenze anche di natura sanzionatoria), i titolari del trattamento sono chiamati a verificare la conformità dei trattamenti in corso ai principi di protezione dei dati (art. 5 del RGPD) e ad adottare le opportune misure tecniche e organizzative, impartendo le necessarie istruzioni al fornitore del servizio (cfr. artt. 5, par. 2 nonché 24, 25, 28 e 32 del RGPD) (provv. 17 dicembre 2020, n. 282, doc. web n. 9525337).

13.11. *Diffusione* online *di dati personali dei lavoratori*

Permangono numerosi i reclami nei confronti di amministrazioni, anche locali, e di altri enti in merito alla pubblicazione sui siti web istituzionali, talvolta anche nella sezione "Amministrazione trasparente", di atti e documenti che contengono dati personali di dipendenti.

I soggetti pubblici, anche in qualità di datori di lavoro, possono trattare tali informazioni se ciò è necessario "all'esecuzione di un contratto di cui l'interessato è parte" (ovvero il contratto di lavoro), "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" (ovvero gli specifici obblighi o compiti previsti dalla legge per finalità di gestione del rapporto di lavoro) oppure "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (artt. 6, par. 1, lett. *b*), *c*) ed *e*), e 9, par. 2, lett. *b*) e *g*), del RGPD, nonché art. 2-*sexies* del Codice). In ogni caso, i dati relativi alla salute (art. 4, par. 1, n. 15 e cons. 35 del RGPD), in ragione della loro particolare delicatezza, non possono essere diffusi (art. 2-*septies*, comma 8, e art. 166, comma 2, del Codice e art. 9, parr. 1, 2, 4, del RGPD).

Per quanto concerne il trattamento dei dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza, la normativa in materia di protezione dei dati prevede che esso possa avvenire soltanto sotto il controllo dell'autorità pubblica o in caso di trattamento autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati (art. 10 del RGPD) ovvero qualora il trattamento sia autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-*octies* del Codice).

In tale quadro, sono stati definiti alcuni reclami, di seguito illustrati, concernenti l'illecita diffusione di dati personali di lavoratori, specialmente sui siti web istituzionali degli enti, nell'ambito delle pubblicazioni effettuate per asserite finalità di trasparenza dell'azione amministrativa.

Pubblicazione di una sentenza

A fronte di un reclamo avente ad oggetto la pubblicazione sul sito web istituzionale di un comune di un provvedimento e del testo integrale di una sentenza relativa a un caso di *mobbing* (contenente anche dati personali relativi alla salute di un lavoratore), il Garante ha avviato un procedimento all'esito del quale è stato ribadito che non soddisfa i requisiti del consenso alla diffusione dei propri dati personali (com-

prendenti informazioni relative a vicende professionali e giudiziarie con il datore di lavoro) il generale contegno tenuto nel caso di specie dall'interessato. Né è stato ritenuto pertinente il richiamo all'art. 52 del Codice il quale trova applicazione nel diverso caso della riproduzione delle sentenze o di provvedimenti dell'Autorità giudiziaria esclusivamente a fini di informatica giuridica (titolo I, capo III del Codice); la pubblicazione della sentenza, detenuta dal comune in quanto parte del relativo procedimento giudiziario, non è stata infatti effettuata per dette finalità, bensì al fine (peraltro dichiarato) di "riscattare […] il danno all'immagine" subito dall'amministrazione (suscettibile però di essere tutelato nelle forme previste dall'ordinamento), nonché per generiche finalità di trasparenza, che non hanno trovato però riscontro nella normativa vigente (provv. 13 febbraio 2020, n. 35, doc. web n. 9285411).

Pubblicazione di dati relativi a condanne penali e reati

L'Autorità ha accolto due distinti reclami presentati dal medesimo interessato nei confronti di due enti locali che avevano pubblicato sui rispettivi siti web, nella sezione "Amministrazione trasparente" e nell'albo *online*, atti amministrativi riferibili al reclamante, identificabile mediante i riferimenti al numero di matricola o alle iniziali del cognome e del nome, diffondendo così anche dati personali relativi a condanne penali e alla commissione di reati.

Contrariamente a quanto sostenuto dai due titolari del trattamento, il Garante, evidenziando che per identificazione non si intende solo la possibilità di risalire in via immediata all'identità di una persona, ma anche la potenziale identificabilità mediante riferimenti ad elementi ulteriori (sul punto, Gruppo Art. 29, parere 5/2014 sulle tecniche di anonimizzazione del 10 aprile 2014, WP216), ha rilevato che la menzione delle iniziali del cognome e del nome della reclamante all'interno della determinazione era idonea a consentirne l'identificazione, quantomeno da parte dei dipendenti del comune e dei familiari o conoscenti della reclamante, anche in considerazione delle dimensioni delle amministrazioni coinvolte e dei rimandi incrociati tra i vari documenti oggetto di pubblicazione. A tal riguardo, già nelle linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati (provv. 15 maggio 2014, n. 243, doc. web n. 3134436), il Garante aveva chiarito che la prassi seguita da alcune amministrazioni di sostituire il nome e cognome dell'interessato con le sole iniziali è di per sé insufficiente ad anonimizzare i dati e che il rischio di identificare l'interessato è tanto più probabile quando (fra l'altro) accanto alle iniziali del nome e cognome permangono ulteriori informazioni di contesto che rendono comunque identificabile l'interessato, essendo necessario oscurare del tutto il nominativo e le altre informazioni riferite all'interessato che ne possono consentire l'identificazione anche *a posteriori*.

Le due amministrazioni hanno inoltre sostenuto che la pubblicazione fosse obbligatoria ai sensi della normativa sulla trasparenza e sulla pubblicità legale degli atti. A tal riguardo, richiamando le citate linee guida, il Garante ha ribadito che, laddove l'amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento sul proprio sito web istituzionale, essa deve selezionare i dati personali da rendere pubblici, verificando caso per caso se ricorrono i presupposti per l'oscuramento di determinate informazioni in conformità al principio di minimizzazione dei dati quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità (art. 5, par. 1, lett. *c*), del RGPD). Pertanto, anche in presenza degli obblighi di pubblicazione ai sensi del d.lgs. n. 33/2013, i soggetti chiamati a darvi attuazione non possono comunque rendere "intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione" (art. 7-*bis*, comma 4, d.lgs.

n. 33/2013). Le medesime considerazioni valgono altresì in merito agli obblighi derivanti dall'art. 124, d.lgs. n. 267/2000, invocato per giustificare la pubblicazione di taluni degli atti amministrativi nella sezione "Albo pretorio" del sito web istituzionale, atteso che anche a tali pubblicazioni si applicano i limiti sopra menzionati con riguardo al rispetto del principio di minimizzazione dei dati e alle cautele da adottare nel caso in cui gli atti da pubblicare contengano dati appartenenti a categorie particolari o giudiziari. La pubblicazione della determinazione, con il previo oscuramento dei dati relativi all'interessato, non avrebbe peraltro compromesso il principio di adeguata motivazione di cui all'art. 3, l. n. 241/1990, poiché la versione integrale della determinazione sarebbe in ogni caso restata agli atti dell'amministrazione, accessibile, da parte di soggetti qualificati, nei modi e nei limiti previsti dalla legge.

Infine, contrariamente a quanto sostenuto da uno dei titolari del trattamento, il Garante ha affermato che le informazioni relative a vicende connesse alla commissione di reati o a procedimenti penali che interessano una persona fisica sono soggetti al regime di cui all'art. 10 del RGPD, senza che rilevi la circostanza che tali informazioni non contengano riferimenti agli specifici reati commessi e allo stato in cui si trovino i procedimenti penali in questione.

Con riguardo all'illecito trattamento posto in essere da uno dei titolari, il Garante, ai fini della commisurazione della sanzione (art. 83, par. 2, del RGPD), ha tenuto conto, tra l'altro, della circostanza che il titolare, prima di procedere alla pubblicazione, aveva provveduto a coinvolgere il proprio responsabile della protezione dei dati personali e a conformarsi in buona fede al parere dello stesso (provv.ti 2 luglio 2020, nn. 118 e n. 119, rispettivamente doc. web nn. 9440025 e 9440042).

Organigramma e pubblicazione di dati relativi alla salute

In merito alla pubblicazione nella sezione "Amministrazione trasparente" del sito web istituzionale di un organigramma nel quale a taluni nominativi dei dipendenti di un ente pubblico strumentale veniva associato il riferimento alla legge 5 febbraio 1992, n. 104 (legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate) e alla legge 12 marzo 1999, n. 68 (norme per il diritto al lavoro dei disabili), il Garante ha dichiarato l'illiceità del trattamento e applicato una sanzione amministrativa per violazione del generale divieto di diffusione di dati sulla salute (art. 2-*septies*, comma 8, del Codice). Contrariamente a quanto sostenuto dall'azienda, proprio in ragione della definizione di dato personale contenuta nel RGPD (art. 4, par. 1, n. 1, del RGPD), anche il mero riferimento alle menzionate normative che, notoriamente, disciplinano benefici e garanzie per l'assistenza, l'integrazione sociale e lavorativa di persone disabili o di loro familiari, consente di ricavare informazioni sullo stato di salute di una persona (provv. 28 maggio 2020, n. 92, doc. web n. 9434609).

13.12. *I trattamenti di dati personali per finalità di gestione del rapporto di lavoro*

L'attività di controllo dell'Autorità si è estesa anche ai trattamenti effettuati nell'ambito di procedimenti disciplinari, delle procedure di protocollazione degli atti e della pianificazione dei turni di servizio dei dipendenti.

Procedimento disciplinare

In un caso un comune aveva notificato a un dipendente alcuni provvedimenti e documenti relativi a un procedimento disciplinare all'indirizzo di posta elettronica certificata utilizzato dal reclamante nell'ambito della propria attività professionale. A tal riguardo, il Garante ha chiarito che le disposizioni di legge che disciplinano le forme e i termini del procedimento disciplinare (cfr. art. 55-*bis*, comma 5, d.lgs. 30 marzo 2001, n. 165), allorquando consentono la comunicazione della contestazione dell'addebito al dipendente tramite posta elettronica certificata (nonché, per le co-

municazioni successive alla contestazione, anche mediante l'utilizzo della posta elettronica), fanno riferimento agli indirizzi di posta elettronica messi a disposizione del lavoratore da parte del datore di lavoro ai fini della prestazione lavorativa, essendo ammesso l'invio di comunicazioni a un diverso indirizzo solo qualora quest'ultimo sia stato previamente comunicato dal dipendente al datore di lavoro. Ciò vale anche quando, come nel caso esaminato, l'indirizzo di posta elettronica certificata del dipendente sia reperibile su un albo professionale *online*, atteso che i dati personali pubblicati in pubblici registri, elenchi, atti o documenti conoscibili da chiunque possono essere trattati con i limiti e le modalità che le leggi di settore applicabili stabiliscono rispetto ad essi (cfr. art. 24, comma 1, lett. *c*), del Codice, nel testo antecedente alle modifiche apportate dal d.lgs. n. 101/2018), nel rispetto del principio di limitazione della finalità (art. 5, par. 1, lett. *b*), del RGPD), in base al quale i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati secondo modalità non incompatibili con tali finalità (provv. 12 marzo 2020, n. 56, doc. web n. 9429218).

Sempre con riguardo alle modalità di notifica di atti relativi a procedimenti disciplinari, il Garante ha trattato un reclamo presentato da un dipendente di una città metropolitana nel quale si lamentava che una nota contenente una segnalazione, da cui avrebbe avuto origine un procedimento disciplinare nei propri confronti, sarebbe stata protocollata senza i necessari attributi di riservatezza, essendo stata resa disponibile a una pluralità di soggetti all'interno dell'amministrazione, alcuni dei quali avevano successivamente condiviso tale nota tramite messaggi di posta elettronica e *social network*. Il Garante, nel ricordare che 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 a procedimenti disciplinari, ha precisato che, analogamente, deve essere adottata tale procedura con riguardo agli atti prodromici all'attivazione dei medesimi procedimenti, in ragione delle informazioni delicate che possono essere contenute in tali atti. Nel caso di specie, è stato accertato che, per effetto della mancata protocollazione in forma riservata dell'atto che conteneva informazioni particolarmente delicate riferite al reclamante – ossia dettagli relativi a comportamenti aventi rilevanza disciplinare –, si sono determinate le condizioni che hanno reso possibile la consultazione del documento a soggetti che, pur operando nell'ambito dell'organizzazione del titolare, non erano, in base alle mansioni svolte, autorizzati a trattare i dati personali in questione (provv. 29 ottobre 2020, n. 204, doc. web n. 9513059).

Affissione in bacheca di turni di servizio e causali assenza

In un altro caso, un'organizzazione sindacale aveva presentato un reclamo per conto di un dipendente di un'azienda concessionaria del servizio di trasporto pubblico locale, lamentando che essa, per prassi interna, affiggeva quotidianamente su una bacheca il documento relativo ai turni di servizio degli autisti contenente anche le causali delle assenze, con specifico riferimento alle condizioni di salute dei lavoratori o di loro familiari e conviventi. Il Garante, sul presupposto che i dati personali dei dipendenti trattati dal datore di lavoro per finalità di gestione del rapporto di lavoro non possono essere messi a conoscenza di soggetti diversi dalle parti del rapporto contrattuale, né possono essere trattati da coloro che, in ragione delle mansioni svolte, non siano autorizzati ad accedere a tali dati, ha ritenuto che – tenuto conto che i dati erano stati resi conoscibili a un novero determinato o, comunque, determinabile di soggetti – tali procedure fossero in contrasto con la disciplina in materia di protezione dei dati, comportando una comunicazione (art. 2-*ter* comma 4, lett. *a*), del Codice) illecita di dati personali, anche relativi allo stato di salute, a terzi non autorizzati (cfr. art. 4, par. 1, n. 10), del RGPD), in assenza quindi di un'idonea base giuridica.

In generale, le informazioni strettamente connesse allo svolgimento dell'attività lavorativa, quali le ragioni delle assenze (ferie, permessi individuali, assenza dal servizio nei casi previsti dalla legge o dai contratti collettivi di lavoro), possono essere trattate dal datore di lavoro in base a specifiche disposizioni normative che prevedono anche l'obbligo per il dipendente di presentare apposita certificazione allo stesso e, a seconda dei casi, anche agli enti previdenziali. Tali obblighi sono funzionali non solo a giustificare i trattamenti normativi ed economici spettanti al lavoratore, ma anche a consentire al datore di lavoro, nelle forme di legge, di effettuare le necessarie verifiche e assumere le conseguenti determinazioni ovvero al fine di permettere ai dipendenti di godere dei benefici di legge, come nel caso delle agevolazioni previste per l'assistenza a familiari disabili, ai permessi retribuiti e ai congedi per gravi motivi familiari (v., sul punto, il par. 6 delle linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati, provv. 23 novembre 2006, n. 53, doc. web n. 1364939 e, non diversamente, il par. 8 delle linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, provv. 14 giugno 2007, n. 23, doc. web n. 1417809).

Tali trattamenti devono tuttavia avvenire mediante personale autorizzato e istruito in merito all'accesso ai dati (artt. 4, par. 10, 29, 32, par. 4, del RGPD), al ricorrere dei presupposti di liceità sopra indicati, in relazione alle funzioni svolte e alle istruzioni impartite, nella misura in cui i dati siano pertinenti per dare esecuzione al rapporto di lavoro nel quadro delle previsioni normative applicabili (cfr. artt. 5, par. 1, lett. *c*) e 88 del RGPD). Entro tale cornice, gli altri addetti al servizio di trasporto non potevano considerarsi legittimati a trattare informazioni di dettaglio sulle assenze dei colleghi, in quanto, in base alle mansioni assegnate, non sono autorizzati ad accedere ai dati funzionali alla gestione delle assenze del personale e alla pianificazione dei turni di lavoro. Nell'erogazione del servizio di trasporto pubblico, l'azienda locale avrebbe potuto, nel rispetto della disciplina di protezione dei dati e in modo parimenti efficace, affiggere in aree disponibili agli addetti al servizio, il solo documento riepilogativo dei turni giornalieri (provv. 18 giugno 2020, n. 105, doc. web n. 9444865).

In un'altra occasione il Garante ha censurato l'invio ad alcune testate giornalistiche, da parte della commissione straordinaria di un comune, di una nota nella quale si menzionavano vicende relative al rapporto di lavoro e richieste avanzate dal reclamante in via stragiudiziale, circostanza che ha dato luogo alla successiva indebita diffusione su dette testate dei dati personali (provv. 2 luglio 2020, n. 116, doc. web n. 9440000).

13.13. *Prerogative sindacali: legittimità dell'accesso a dati personali dei dipendenti da parte delle organizzazioni sindacali*

Il Garante è tornato a pronunciarsi sulla possibilità per i sindacati di conoscere i nominativi dei lavoratori che ricevono una retribuzione accessoria e i relativi importi nonché, in particolare, sulla legittimità delle richieste avanzate in tal senso dalle organizzazioni sindacali alla dirigenza scolastica.

La questione era stata già affrontata nel 2014 alla luce di una diversa disposizione presente nel Ccnl di settore. Considerato il nuovo quadro giuridico introdotto dal RGPD e l'intervenuta modifica del Ccnl, l'Ufficio, anche nell'ottica di prevenire trattamenti di dati non conformi da parte delle scuole, ha fornito specifici chiarimenti all'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (Aran), all'Avvocatura generale dello Stato e al Miur, con una nota la cui valenza ha una portata più generale rispetto allo specifico contesto scolastico.

13

Nel ricordare che la messa a disposizione delle organizzazioni sindacali di dati personali di dipendenti in qualunque forma comporta una comunicazione di dati personali (art. 2-*ter*, comma 4, lett. *a*), del Codice), è stato precisato che, anche in tale contesto, ciò è ammesso in presenza di una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-*ter*, commi 1 e 3 del Codice). Nei limiti e negli ambiti ad essi demandati da norme di legge o di regolamento, i contratti collettivi possono contenere specificazioni e disposizioni di dettaglio (cfr. cons. 41 e art. 88 del RGPD; v. raccomandazione 1° aprile 2015, CM/Rec(2015)5, del Comitato dei ministri agli Stati membri sul trattamento di dati personali nel contesto occupazionale, par. 7). La contrattazione collettiva disciplina, infatti, taluni aspetti del rapporto di lavoro espressamente individuati dalla legge (ad es., la corresponsione del trattamento accessorio) nonché le relazioni sindacali nei limiti previsti dalle norme di legge (art. 40, d.lgs. n. 165/2001). In ogni caso, in assenza di una disposizione normativa che soddisfi i requisiti previsti dalla disciplina di protezione dei dati, potranno essere forniti alle organizzazioni sindacali solo dati numerici o aggregati. Peraltro, le prerogative sindacali previste dalle disposizioni dei contratti collettivi applicabili per i singoli comparti dell'amministrazione (ad es., diritti di informazione preventiva o successiva) possono di regola essere soddisfatte rendendo note solamente informazioni aggregate, senza far ricorso a dati personali. Per tali ragioni, salve le forme di conoscibilità degli atti amministrativi, nei limiti e con le modalità stabilite dalla disciplina di settore (artt. 22 ss., l. n. 241/1990 e art. 5, d.lgs. n. 33/2013), tenuto conto del quadro normativo vigente applicabile al cd. comparto scuola, è stato ritenuto che non sia consentito agli istituti scolastici comunicare alle organizzazioni sindacali i nominativi dei docenti o di altro personale e le somme liquidate a ciascuno per lo svolgimento di attività finanziate con il cd. fondo d'istituto.

14 Le attività economiche

14.1. *Il trattamento dei dati personali in ambito assicurativo*

Continua a registrarsi un significativo afflusso di istanze connesse al settore assicurativo, ancorché in prevalenza relative a tematiche già esaminate e definite in passato dall'Autorità e illustrate anche in occasione di precedenti Relazioni annuali.

Beneficiari di polizze vita

L'Ufficio, in particolare, è tornato a occuparsi della questione relativa alla conoscibilità, da parte degli eredi del *de cuius*, dei nominativi dei beneficiari di polizze vita stipulate da quest'ultimo. Muovendo, infatti, da un recente orientamento giurisprudenziale che attribuisce ai premi versati natura di donazioni indirette, come tali riconducibili alla massa ereditaria, molti istanti, temendo una lesione dei propri diritti successori, hanno chiesto alle società con cui erano state stipulate dette polizze di poter accedere ai dati personali dei relativi beneficiari, onde verificare la propria eventuale legittimazione ad esperire verso costoro azione di riduzione o collazione. Ricevendo, tuttavia, riscontri solo parziali o documentazione oscurata *in parte qua*, gli istanti si sono rivolti al Garante al fine di ottenere quanto richiesto.

L'Ufficio, premessa la propria incompetenza a pronunciarsi sull'inquadramento giuridico che gli istanti avrebbero voluto fosse riconosciuto alle polizze in esame, ha ribadito che il diritto di cui all'art. 15 del RGPD permette all'interessato di accedere ai dati e alle informazioni che lo riguardano, ma non consente a quest'ultimo di ottenere anche i dati personali relativi a terzi. Lo stesso art. 2-*terdecies* del Codice, nel riconoscere ai soggetti ivi richiamati – compresi gli eredi, in linea di continuità con il previgente art. 9, comma 3, del medesimo Codice – la possibilità di esercitare i diritti previsti dagli artt. 15-22 del RGPD, ne ha circoscritto l'applicabilità ai soli dati personali del *de cuius*, escludendo la possibilità di accesso ai dati personali riferiti ad altri soggetti (le cui esigenze di tutela, al contrario, trovano conferma nello stesso art. 15, par. 4, del RGPD).

Documentazione assicurativa

Altra questione portata all'attenzione dell'Autorità, anch'essa già oggetto di disamina in passato, si riferisce alla differenza tra il diritto di accesso ai dati personali previsto dall'art. 15 del RGPD e il diverso diritto di accesso agli atti e ai documenti previsto dall'art. 146, d.lgs. n. 209/2005 (recante il codice delle assicurazioni private). Numerose istanze pervenute, infatti, chiedevano al Garante di intervenire presso alcune società di assicurazioni al fine di far acquisire ai richiedenti copia di documentazione assicurativa potenzialmente utilizzabile in sede giudiziaria. Nel richiamare l'orientamento già espresso in precedenti pronunce, l'Ufficio ha ribadito che l'esercizio del diritto di accesso ai dati personali permette agli interessati di conoscere i dati e le informazioni a sé riferite, ma non di ottenere anche l'accesso agli (o la copia degli) atti e documenti che li contengono, specie se l'accesso documentale è già previsto e disciplinato da normative di settore eventualmente applicabili. Pertanto, pur restando nella facoltà dei richiedenti richiedere l'accesso ai dati personali a sé riferiti, è stata ribadita l'incompetenza dell'Autorità a pronunciarsi sulle richieste volte a ottenere, come nei casi esaminati, l'accesso o la copia di atti o documenti detenuti dai titolari.

Perizie medico-legali

Meno significativo – ma non per questo meno importante – è stato poi il flusso di istanze relative all'accesso ai dati personali contenuti nelle perizie medico-legali, con

particolare riguardo alle informazioni valutative (giudizi) ivi contenute. Anche in questo caso l'Ufficio, pur confermando – sulla scia di un consolidato orientamento del Garante – che le informazioni contenute nelle perizie medico-legali costituiscono dati personali suscettibili di accesso ai sensi della disciplina in materia di protezione dei dati personali, ha tuttavia ribadito che il diritto di cui all'art. 15 del RGPD incontra precise limitazioni (cfr. artt. 23 del RGPD e 2-*undecies* del Codice), sovente ricorrenti anche in ambito assicurativo, che ne circoscrivono talora l'esercizio. In particolare, muovendo dal contesto di riferimento descritto dagli istanti – quasi sempre di natura aspramente contenziosa o pre-contenziosa – si è ritenuta applicabile, in numerosi casi, la limitazione di cui alla lett. *e*) del suddetto art. 2-*undecies* del Codice, secondo cui il diritto di accesso non può essere esercitato con richiesta al titolare qualora dal suo esercizio possa derivare un pregiudizio effettivo e concreto allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria. Nelle sue valutazioni, l'Ufficio ha tenuto conto delle precedenti pronunce adottate dall'Autorità in casi analoghi, nelle quali erano state escluse dal novero delle informazioni accessibili dagli interessati quelle concernenti le valutazioni e/o le considerazioni espresse in sede peritale e aventi carattere potenzialmente difensivo, di strategia contrattuale o procedimentale, ovvero comunque incidenti sulle ragioni del titolare (v., *ex multis*, provv.ti 22 gennaio 2001, doc. web n. 39961; 31 marzo 2003, doc. web n. 1068357; 7 maggio 2003, doc. web n. 1079747; 2 luglio 2003, doc. web n. 1079919; 22 settembre 2003, doc. web n. 1081790; 19 aprile 2004, doc. web n. 1092649). 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, l'alterità tra il diritto di accesso ai dati personali e il diritto di accesso agli atti e ai documenti che li contengono.

Alcune istanze hanno riguardato, spesso genericamente, la circolazione dei dati personali all'interno della cd. catena assicurativa; al riguardo, l'Ufficio, nel richiamare il provvedimento generale del 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 della (talora inevitabile) intensità dei flussi comunicativi che si registrano in questo ambito, sovente tale 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.

Frodi assicurative

Particolare interesse, da ultimo, ha destato il progetto proposto dall'Associazione che raggruppa le compagnie assicurative (Ania) per prevenire e contrastare le frodi assicurative in rami diversi da quello della responsabilità civile autoveicoli (cd. settore no auto). Tale progetto, nella descrizione fattane all'Autorità, prevederebbe la costituzione di una banca dati, accessibile tramite portale web, alimentata con i dati forniti dalle singole società di assicurazioni in relazione ai sinistri verificatisi negli ultimi 5 anni nei segmenti di rischio diversi da quello della r.c.a. (malattia; infortunio; incendio; altri beni; responsabilità civile generale; ecc.); i dati raccolti verrebbero elaborati per estrarre un indice sintetico di rischiosità (*score*) da assegnare a ciascun sinistro denunciato, offrendo così alle compagnie di assicurazione, per ogni singola chiave di interrogazione, utili indicazioni in merito a possibili comportamenti fraudolenti.

Il livello e la "profondità" di accesso alle informazioni da parte delle singole com-

pagnie verrebbero graduati sulla base di un meccanismo "semaforico", funzionale a garantire una conoscibilità più dettagliata dei dati relativi ai sinistri solo in caso di rischio elevato. L'accesso alla banca dati – previsto tanto in fase assuntiva che liquidativa – verrebbe garantito anche alle Autorità giudiziarie e di vigilanza per gli accertamenti e le verifiche di rispettiva competenza.

A seguito di un primo esame, l'Autorità ha ritenuto opportuno, in considerazione delle rilevanti dimensioni della banca dati, della sua potenziale pervasività sui diritti e sulle libertà degli interessati e delle criticità già emerse in occasione di precedenti incontri informali presso l'Ufficio, proseguire nell'attività istruttoria e di analisi, coinvolgendo anche altri interlocutori istituzionali (in specie, l'Ivass e il Consiglio nazionale dei consumatori e degli utenti). L'Autorità ha invitato Ania a effettuare la necessaria valutazione d'impatto (art. 35 del RGPD), all'esito della quale si è riservata più mirate iniziative anche sulla base dei risultati forniti e della consultazione preventiva eventualmente attivata ai sensi dell'art. 36 del RGPD.

L'esame del progetto, su cui sono state avviate istruttorie anche da parte di altre autorità (in particolare, l'Agcm), proseguirà nel 2021.

14.2. *Settore bancario-finanziario e sistemi di informazioni creditizie*

Come ogni anno, notevole è stato l'afflusso di segnalazioni, reclami, quesiti e richieste di parere relativi ai trattamenti di dati personali effettuati da banche, società finanziarie, sistemi di informazione creditizia gestiti da soggetti privati, Centrale dei rischi pubblica gestita dalla Banca d'Italia e Centrale di allarme interbancaria. Le istanze pervenute hanno riguardato, come per il passato, anzitutto profili e questioni su cui il Garante si è ripetutamente espresso nel corso degli anni anche a mezzo di provvedimenti collegiali, tra cui le linee guida adottate il 25 ottobre 2007 (provv. 25 ottobre 2007, n. 53, doc. web n. 1457247), i cui principi sono già stati ritenuti compatibili con il vigente quadro regolatorio (v. già Relazione 2018, p. 138).

In particolare, numerose richieste hanno riguardato il trattamento dei dati personali effettuato in occasione delle operazioni di identificazione e adeguata verifica della clientela prescritte dalla normativa vigente in materia di antiriciclaggio e antiterrorismo che è stata più volte oggetto di disamina da parte del Garante per i profili di propria competenza (da ultimo con il parere del 24 luglio 2019, n. 150, sul d.lgs. n. 125/2019, adottato in attuazione della cd. quinta direttiva: doc. web n. 9126288). L'Ufficio è tornato a ribadire che tutte le categorie di soggetti obbligate ai sensi della vigente normativa di settore devono sia identificare l'interessato ed effettuare la cd. adeguata verifica prima di stipulare qualsiasi rapporto contrattuale o effettuare operazioni occasionali, sia eseguire una serie di interventi, tra cui il monitoraggio e il controllo continuativo del rapporto pendente. L'identificazione del cliente prevede la consegna di copia di un valido documento d'identità dell'interessato, mentre l'adeguata verifica richiede l'acquisizione di dettagliate informazioni e di specifica documentazione (anche sull'attività lavorativa svolta e sulla situazione economica e patrimoniale), variabile a seconda delle modalità in concreto adottate (verifica semplificata, ordinaria o rafforzata). Nelle fattispecie esaminate, per i connessi profili di protezione dei dati personali, si è ritenuto che tanto i principi contenuti nei provvedimenti adottati dal Garante nel corso del tempo, quanto la vigente disciplina in materia di protezione dei dati personali non fossero stati violati.

Sempre numerosi sono stati i reclami e le segnalazioni in materia di esercizio dei diritti degli interessati, con specifico riguardo al diritto di accesso ai dati personali. In linea con il consolidato orientamento dell'Autorità in materia, è stato precisato che

l'accesso ai dati personali è altro rispetto all'accesso ai documenti bancari disciplinato dall'art. 119, d.lgs. 1° settembre 1993, n. 385 (Testo unico delle leggi in materia bancaria e creditizia); le istanze di accesso ai dati, pertanto, non devono tendere all'acquisizione di copia di documenti bancari, non possono riguardare dati di terzi e devono conformarsi alla disciplina in materia di protezione dei dati (in specie, agli articoli 12 e ss. del RGPD).

Sic

Rilevante è stato il numero di istanze pervenute in materia di dati personali trattati nell'ambito dei sistemi di informazioni creditizie gestiti da soggetti privati (cd. Sic). Alcune di queste avevano ad oggetto il mancato rilascio del preavviso di inserimento nei Sic, altre i tempi di conservazione, altre, ancora, i presupposti per effettuare la segnalazione. L'Ufficio ha provveduto ad applicare i principi di legge e a richiamare le disposizioni del nuovo codice di condotta – strumento di autoregolamentazione ad adesione volontaria in grado di concorrere, nell'ambito qui considerato, alla corretta applicazione del RGPD (art. 40) –, invitando i partecipanti e i gestori dei Sic, laddove necessario, ad aderire spontaneamente alle richieste formulate dagli interessati. In numerosi casi le richieste (soprattutto di cancellazione dei dati dai Sic) sono state ritenute infondate, non essendo state riscontrate violazioni della normativa in materia di protezione dei dati personali.

Proprio l'applicazione delle disposizioni del nuovo codice di condotta sopra richiamato (che sostituiscono quelle contenute nel precedente codice deontologico) è stata tenuta in considerazione dal Garante rispetto ad alcune richieste di cancellazione delle segnalazioni positive inserite nei Sic in ragione della revoca del consenso al trattamento dei dati personali. In tali casi, infatti, il Garante ha rappresentato che il nuovo codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti, prevede che "il trattamento dei dati personali degli interessati da parte dei gestori e dei partecipanti al Sic secondo i termini e le condizioni stabilite nel codice di condotta risulta lecito ai sensi dell'art. 6, par. 1, lett. *f*), del RGPD, in quanto è necessario per il perseguimento di legittimi interessi dei partecipanti all'utilizzo del Sic per le finalità di cui al presente codice di condotta. Pertanto, non è necessario acquisire il consenso dell'interessato". Naturalmente, il cd. principio del legittimo interesse (quale base giuridica del citato trattamento per le finalità individuate nel codice di condotta e connesse alla corretta valutazione del merito e del rischio creditizio, alla valutazione dell'affidabilità e della puntualità dei pagamenti dell'interessato, alla prevenzione del rischio di frode, ivi inclusa la prevenzione del rischio del furto di identità) deve essere richiamato nell'informativa sul trattamento dei dati personali resa dai partecipanti, anche per conto dei Sic, al momento della raccolta dei dati degli interessati (cfr. all. 3 al codice di condotta) ovvero dai gestori medesimi (art. 6, par. 2 e ss. del codice di condotta), i quali sono tenuti a pubblicarle sui rispettivi siti istituzionali.

Nel corso dell'anno si sono intensificate anche le richieste di intervento rivolte al Garante in casi potenzialmente riconducibili al fenomeno del cd. furto d'identità. Tenuto conto della diffusione di tecniche sempre più sofisticate (soprattutto informatiche e derivanti dal cd. *phishing*) volte ad appropriarsi di informazioni personali riservate al fine ultimo di compiere operazioni fraudolente, si è ricordato agli interessati che l'Autorità ha da tempo reso disponibile sul proprio sito una scheda informativa con la quale si sensibilizza l'utenza affinché adotti accorgimenti e cautele per evitare di incorrere in queste tipologie di comportamenti illeciti (v. doc. web n. 5779914). Preso atto del disconoscimento delle operazioni bancarie o finanziarie effettuato dagli interessati e delle denunce sporte dai medesimi nelle competenti sedi giudiziarie per l'accertamento delle fattispecie di reato rinvenibili nei fatti segnalati, l'Ufficio si è riservato – anche in considerazione di quanto stabilito dall'art. 140-*bis*

del Codice circa l'alternatività tra tutela amministrativa e tutela giurisdizionale – di assumere proprie determinazioni all'esito e sulla base delle risultanze degli accertamenti già attivati in sede giudiziaria sui casi segnalati.

Sono poi pervenuti all'attenzione dell'Ufficio casi, nuovi, in cui imprese individuali e professionisti hanno segnalato la possibile violazione della normativa emergenziale adottata durante l'anno per arginare i danni economici prodotti dalla pandemia ancora in corso. In particolare, talune istanze hanno riguardato la lamentata violazione dell'obbligo di sospensione delle segnalazioni a sofferenza presso la Centrale dei rischi della Banca d'Italia e presso i cd. Sic disposta dall'art. 37-*bis* (Sospensione temporanea delle segnalazioni a sofferenza alla Centrale dei rischi e ai sistemi di informazioni creditizie) del decreto-legge 8 aprile 2020, n. 23, Misure a sostegno della liquidità per le imprese danneggiate da Covid-19 (cd. d.l. Liquidità), convertito, con modificazioni, nella legge 5 giugno 2020, n. 40 (con disposizione successivamente modificata dall'art. 65, comma 4, del decreto-legge 14 agosto 2020, n. 104, Misure urgenti per il sostegno e il rilancio dell'economia (cd. d.l. Agosto), convertito – anch'esso con modificazioni – nella legge 13 ottobre 2020, n. 12). La richiamata disposizione ha stabilito che fino "al 31 gennaio 2021, le segnalazioni a sofferenza effettuate dagli intermediari alla centrale dei rischi della Banca d'Italia […], riguardanti le imprese beneficiarie delle misure di sostegno finanziario di cui all'articolo 56, comma 2, del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, sono sospese a decorrere dalla data dalla quale tali misure sono state concesse. 2. Le disposizioni del comma 1 si applicano anche ai sistemi di informazioni creditizie dei quali fanno parte altri archivi sul credito gestiti da soggetti privati e ai quali gli intermediari partecipano su base volontaria". Nei casi esaminati, tuttavia, non sono emerse violazioni in quanto la particolare sospensione delle segnalazioni in esame, disposta *ex lege*, opera nella sola ipotesi in cui le misure previste dall'art. 56 siano state accordate, circostanza che, nei casi in questione, è risultata insussistente (nota 10 novembre 2020).

In un caso particolare l'istante ha manifestato dubbi sulla legittimità della procedura adottata da un istituto di credito per il rilascio dei finanziamenti coperti dalla garanzia pubblica previsti dal cd. d.l. Liquidità. Nella fattispecie considerata, dopo il rifiuto del finanziamento richiesto, l'interessato ha ritenuto che la valutazione del merito creditizio effettuata dalla banca dovesse essere esclusa per l'accesso a tali tipologie di finanziamento. Si è pertanto ricostruito il quadro normativo di riferimento, evidenziando che le modifiche apportate in sede di conversione in legge all'art. 13 del d.l. Liquidità – relativo all'operatività del Fondo di garanzia per le Pmi e gli ulteriori soggetti ai quali è stata estesa l'applicazione delle fattispecie di finanziamento introdotte per fare fronte ai danni creati da Covid-19 (con particolare riguardo alla lett. *g*) – prevedono espressamente, tra le condizioni in base alle quali è possibile accedere al beneficio della garanzia, che il soggetto finanziatore, sulla scorta dell'analisi in concreto della situazione finanziaria del debitore, possa ragionevolmente presumere il rimborso integrale dell'esposizione alla scadenza. La verifica della complessiva posizione creditizia del richiedente, indispensabile per valutare la presenza in capo allo stesso di esposizioni "deteriorate", pertanto, è testualmente prevista dalla norma in questione. Allo stesso modo, l'art. 37-*bis* – che sospende le segnalazioni a sofferenza effettuate dagli intermediari alla Centrale dei rischi della Banca d'Italia riguardanti le imprese beneficiarie delle misure di moratoria previste all'art. 56, comma 2, del d.l. Cura Italia – si limita a disporre la sospensione, senza pronunciarsi in ordine alla valutazione del merito creditizio degli interessati. Infine, il punto 8 dell'all. 4 *bis* – recante il modulo da presentare al soggetto richiedente del fondo di garanzia (banca, intermediario finanziario, confidi) ai sensi del d.l. Liquidità, come conver-

tito nella legge n. 40/2020 – contiene, tra le autodichiarazioni da rendere a cura del soggetto che intenda accedere ai finanziamenti, quella "di essere a conoscenza che il soggetto richiedente […], potrà inviare al Gestore documentazione riguardante i dati andamentali dell'impresa provenienti dalla Centrale rischi di Banca d'Italia o da altra società privata di gestione di sistemi di informazione creditizia". Il modello stesso, quindi, fa espresso riferimento alla possibile valutazione del merito creditizio dell'interessato. Ritenuto che in concreto non fosse ascrivibile in capo all'istituto di credito coinvolto nella vicenda segnalata alcuna violazione della normativa di settore, si è ritenuto di dover rammentare il motivo per cui gli intermediari svolgono ordinariamente verifiche circa le condizioni economico-finanziarie dei (potenziali) clienti ovvero, in generale, la salvaguardia del sistema bancario e la tutela del singolo richiedente un prestito nonché, nel caso dei finanziamenti introdotti dalla recente normativa emergenziale (d.l. Liquidità e successive modifiche e integrazioni) e coperti dalla garanzia pubblica, l'esigenza di evitare il rischio di impiegare risorse pubbliche "a pioggia". Si è poi evidenziato che l'obbligo di effettuare la valutazione del merito creditizio delle imprese e dei professionisti si ricava dal principio generale di "sana e prudente gestione" previsto dall'art. 5, d.lgs. 1° settembre 1993, n. 385 (Testo unico delle leggi in materia bancaria e creditizia), declinato da una puntuale normativa secondaria (v. in particolare, le disposizioni di vigilanza della Banca d'Italia che, nell'erogazione del credito alla clientela, impongono alle banche, tra l'altro, di adottare regolamenti interni per la standardizzazione delle procedure di valutazione del merito creditizio).

Settore bancario-finanziario e "tracciamento" delle operazioni

Permane l'attenzione sul tema dell'adozione, da parte degli istituti di credito, delle misure previste dal provvedimento del 12 maggio 2011, n. 192 (doc. web n. 1813953), in materia di circolazione delle informazioni e di tracciamento delle operazioni bancarie; continuano infatti a pervenire reclami con i quali gli interessati lamentano l'illecita comunicazione di dati bancari a terzi non autorizzati e se, nella maggior parte dei casi, il cd. tracciamento degli accessi ha consentito di verificare la legittimità degli accessi medesimi (e quindi del trattamento effettuato), in qualche caso, gli stessi istituti di credito coinvolti nel reclamo, già prima dell'avvio del procedimento dinanzi al Garante, avevano provveduto a sanzionare il dipendente responsabile di accessi indebiti, non giustificati da esigenze operative sui rapporti bancari intestati al cliente.

In questo contesto, l'analisi di alcune tra le fattispecie pervenute all'attenzione dell'Autorità ha consentito di rilevare l'esigenza di prevedere l'adozione di ulteriori tipologie di *alert* per la rilevazione di comportamenti anomali o a rischio, che siano allineati alle recenti tecnologie e che consentano di operare sempre di più in chiave preventiva rispetto ad eventuali comportamenti illeciti posti in essere da dipendenti "infedeli".

14.3. *Codici di condotta in ambito privato*

Nonostante le difficoltà connesse all'emergenza sanitaria, sono proseguite le iniziative (rispetto alle quali il Garante ha esercitato una funzione al tempo stesso di stimolo e di controllo) miranti a redigere alcuni codici di condotta secondo le prescrizioni degli artt. 40 e 41 del RGPD.

Nella prima parte dell'anno è stato possibile completare l'*iter* del provvedimento nazionale contenente i requisiti per l'accreditamento degli organismi di monitoraggio: organo, quest'ultimo, previsto come corollario obbligatorio di ogni nuovo codice e strumento indispensabile per assicurarne il corretto funzionamento, specie in

relazione all'ammissibilità dei titolari del trattamento, alle verifiche sull'osservanza del codice e, soprattutto, alla gestione dei reclami relativi alle possibili violazioni del codice stesso.

Dopo le osservazioni formulate dal Cepd, con provvedimento del 10 giugno 2020, n. 98 (doc. web n. 9432569) si sono individuati i requisiti richiesti per gli organismi di monitoraggio (OdM): fra essi, particolarmente significativi (come constatato "sul campo" fin da questi primi mesi di applicazione delle nuove disposizioni) si sono rivelati quelli concernenti l'autonomia organizzativa e finanziaria, nonché quelli richiesti ai componenti degli OdM, riguardanti la competenza tecnica e l'assenza di conflitto di interessi. Nell'applicazione pratica, tali requisiti sono apparsi come potenzialmente confliggenti; proprio per questo il Garante ne ha promosso, fin dal primo caso concretamente esaminato, un'interpretazione non formalistica e volta a salvaguardare la presenza di entrambi questi requisiti come caratterizzanti l'Organismo nel suo complesso.

Informazioni commerciali

In particolare, il Garante si è confrontato con i problemi applicativi appena evidenziati in relazione all'OdM del codice di condotta in materia di informazioni commerciali. Si tratta di un codice, nato per revisione del preesistente codice di deontologia e buona condotta per il trattamento di dati personali effettuato a fini di informazioni commerciali, già approvato con riserva con il provv. 12 giugno 2019, n. 127 (doc. web n. 9119868). L'*iter* di accreditamento di tale OdM si è concluso con l'adozione del provv. 11 febbraio 2021, n. 59 (doc. web n. 9565426); definita la sua composizione, si sta ora completando l'esame del testo definitivo.

Sic

Percorso in qualche misura parallelo è quello attualmente in corso relativamente al codice di condotta riferito all'attività dei cd. sistemi di informazioni creditizie (Sic), anch'esso approvato con riserva il 12 settembre 2019, n. 163 (doc. web n. 9141941).

Altri codici di condotta

Si sono anche seguiti, in collaborazione con le categorie interessate, alcuni progetti di codici di condotta in ambiti non precedentemente presidiati da appositi codici di deontologia. Ciò sul presupposto che lo strumento del codice di condotta possa aiutare i soggetti operanti in un ambito omogeneo a declinare in modo univoco i principi di protezione dei dati, fornendo indicazioni e regole condivise per gestire le operazioni di trattamento tipiche di un determinato ambito economico, sociale, associativo, ecc.

In questi casi, la linea di indirizzo seguita dall'Autorità è stata quella di verificare, anzitutto d'intesa con i promotori, se effettivamente vi fosse spazio (non coperto da altre disposizioni normative) per la redazione di un codice di condotta e, quindi, per disciplinare unitariamente alcune tipologie di trattamenti. Allo stato, seguendo questa impostazione, è in avanzata fase di redazione un codice per il settore delle agenzie per il lavoro.

14.4. *Videosorveglianza in ambito privato*

Negli ultimi anni le problematiche concernenti il trattamento di dati personali attraverso l'utilizzo di impianti di videosorveglianza nell'ambito privato sono sensibilmente aumentate in termini numerici. In particolare, le numerose controversie derivanti dall'utilizzo di sistemi di videosorveglianza per fini personali hanno prevalentemente interessato l'adozione di un raggio di ripresa degli apparecchi eccedente il legittimo ambito della singola proprietà privata che si intende tutelare.

L'azione dell'Autorità, in questi casi, è stata improntata ad un'attività di tipo essenzialmente educativo/conciliatorio con l'intento di illustrare al titolare del trat-

tamento il corretto utilizzo degli apparecchi di ripresa secondo parametri coerenti con il provvedimento generale del 2010 (in larga parte compatibile con il nuovo quadro regolatorio), le più recenti linee guida europee e le sentenze sull'argomento della CGUE (tra cui determinante è la sentenza dell'11 dicembre 2014, causa C-212/13). Proprio al fine di fornire elementi di maggiore chiarezza, l'Ufficio ha recentemente contribuito alla formulazione di FAQ rese pubbliche tramite il sito internet del Garante che hanno costituito un valido ausilio agli utenti in relazione ai casi più ricorrenti.

Medesimo approccio (pur con un numero di casi meno rilevante) ha riguardato sia l'ambito dei trattamenti svolti attraverso l'utilizzo di sistemi di videosorveglianza condominiale (che ha trovato nell'art. 1122-*ter* c.c. anche una base normativa chiara per quanto concerne le maggioranze assembleari necessarie per deliberare in materia), sia quelli effettuati da parte di esercizi pubblici o di altre imprese essenzialmente a fini di tutela del patrimonio aziendale.

Per effetto del continuo sviluppo tecnologico e, in particolare, della miniaturizzazione dei dispositivi, merita segnalare la crescente diffusione degli apparecchi di ripresa sugli automezzi e sui droni, la diffusione di impianti video controllati a distanza e la richiesta di utilizzare tecnologie di riconoscimento facciale. In alcuni casi, l'Autorità si è richiamata ai principi già espressi con i numerosi provvedimenti (che continuano a costituire un significativo punto di riferimento) che avevano definito le richieste di verifica preliminare (cd. *prior checking*), istituto previsto dal previgente art. 17 del Codice.

14.5. *Trattamenti di dati personali in ambiti e settori particolari*

14.5.1. Concessionari di pubblici servizi

L'attività di esame e valutazione delle segnalazioni, dei reclami e dei quesiti nel settore dei concessionari di pubblici servizi è stata particolarmente intensa. In gran parte ha riguardato, come in passato, il settore energetico (in particolare i fornitori operanti nel mercato libero), con una sostanziale incidenza, però, dal punto di vista numerico, dei reclami inerenti ad altri concessionari (società di gestione dei servizi idrici, del trasporto pubblico, dei servizi ambientali, dei servizi postali, dei concessionari autostradali, ecc.).

I profili oggetto di contestazione hanno riguardato, in particolare, i presupposti di legittimità del trattamento (con specifico riferimento alla definizione degli ambiti dei trattamenti necessari per l'adempimento delle finalità contrattuali), i solleciti per finalità di recupero credito (tema sul quale l'Autorità si è già pronunciata: v. da ultimo *vademecum* pubblicato al doc. web n. 4893274), le segnalazioni di *data breach* (specialmente in ordine all'invio telematico di fatture e bollette), il funzionamento dei portali clienti *online* (soprattutto relativamente alle modalità di registrazione agli stessi) e le verifiche di affidabilità dei potenziali contraenti.

Le istanze pervenute hanno costituito l'occasione per ribadire alcuni principi già espressi in provvedimenti di carattere generale, confermandone la compatibilità con il nuovo quadro normativo, nonché per puntualizzare la portata di alcune norme del RGPD con riferimento allo specifico settore di riferimento. In alcune occasioni, per esempio, è stata ribadita la legittimità dei trattamenti posti in essere, in ambito energetico, al fine di determinare l'affidabilità dei potenziali clienti; ciò ove i trattamenti siano effettuati per il tramite di servizi forniti da società specializzate nello svolgimento di attività di informazione commerciale o dai gestori di sistemi informativi di rilevazione di rischi creditizi e alle condizioni di cui al RGPD (v. art.

134 del TULPS; d.m. 1° dicembre 2010, n. 269 e d.m. 25 febbraio 2015, n. 56; art. 6-*bis*, legge 14 settembre 2011, n. 148; art. 30-*ter*, d.lgs. n. 141/2010; v. anche l. n. 124/2017; cfr. anche provv. 12 giugno 2019, n. 127, codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali, doc. web n. 9119868; provv. 12 giugno 2019, codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti, doc. web n. 9141941). In tali contesti, l'Autorità ha raccomandato ai titolari di valutare l'opportunità di intervenire, in base al principio di *accountability,* sui propri processi interni al fine di dare migliore e più compiuta attuazione al principio di trasparenza. In merito, da un lato i fornitori di energia sono stati invitati ad adottare, nell'ambito delle informazioni fornite ai sensi dell'art. 13 del RGPD, formulazioni più chiare, onde rendere più agevole per l'interessato la comprensione in linea generale dei trattamenti svolti. Dall'altro, è stata richiamata l'esigenza di rimodulare in parte il contenuto dei riscontri resi ai sensi dell'art. 12, par. 3, del RGPD, al fine di indicare chiaramente il soggetto o i soggetti cui sono affidati i servizi di verifica dell'affidabilità del cliente nonché le motivazioni alla base delle valutazione ivi fornite; ciò anche al fine di consentire all'interessato medesimo di potersi direttamente rivolgere, in caso di informazioni inesatte o non aggiornate, ai titolari del trattamento (società di informazione commerciale o gestori di sistemi informativi di rilevazione del rischio creditizio) per esercitare i diritti di cui agli artt. 15-22 del RGPD (in particolare, il diritto di accesso e quello di rettifica dei propri dati).

Con riferimento ad altre istanze, soprattutto in relazione alla titolarità del trattamento per la gestione dei servizi idrici, è stato più volte chiarito che la materia relativa ai cd. servizi tutelati (tra cui rientra anche la gestione dei servizi idrici) è espressamente disciplinata dalla normativa (cfr., per lo specifico settore idrico, il d.lgs. n. 152/2006) la quale, tra l'altro, ha espressamente previsto, in diverse ipotesi – al fine di garantire il rispetto del principio di unicità della gestione all'interno dell'ambito territoriale ottimale –, il subentro del gestore del servizio idrico integrato agli ulteriori soggetti operanti all'interno del medesimo ambito territoriale; tale subentro, i cui effetti sono espressamente disciplinati dalla legge, produce efficacia non solo sul piano contrattuale, ma anche su quello della titolarità del trattamento, non necessitando di una nuova specifica adesione degli interessati al rapporto di fornitura (art. 6, par. 1, lett. *b*), del RGPD), né del rilascio di preventiva informativa da parte del titolare subentrante (v. art. 14, par. 5, del RGPD).

Sono stati definiti alcuni episodi di trasmissione di documentazione (spesso singole fatture) a destinatari diversi dal diretto interessato in ragione di errore umano o di momentanei disallineamenti dei sistemi informatici adoperati: in tali occasioni è stato raccomandato ai titolari coinvolti di intervenire sul piano tecnico e organizzativo, anche mediante specifica formazione del personale incaricato, al fine di prevenire il ripetersi di fatti analoghi in futuro, prendendo comunque atto, nei casi istruiti, della corretta gestione, da parte dei medesimi titolari, delle procedure di notifica all'Autorità ex art. 33 del RGPD (ove applicabile) e di annotazione dell'evento nell'apposito registro interno.

Contratti non richiesti

Il Garante ha infine proseguito la propria attività di vigilanza e di controllo con riferimento ai trattamenti di dati personali effettuati da parte dei venditori di energia elettrica e gas nel mercato libero nell'ambito dei cd. contratti non richiesti, anche mediante il ricorso a richieste ex art. 58, par. 1, lett. *b*), del RGPD. In tale settore, è stata rilevata, rispetto all'anno precedente, una notevole flessione dei reclami pervenuti, in concomitanza con la sempre maggiore attenzione dei titolari in ordine all'implementazione di misure tecniche e organizzative volte a prevenire tali fattispecie. È emerso, in particolare, un generalizzato impegno da parte degli operatori

di settore nell'adozione, ai sensi del principio di *accountability*, di misure analoghe a quelle prescritte dal Garante nei confronti di una società operante nel medesimo settore con il provv. 11 dicembre 2019, n. 231 (doc. web n. 9244358), con buoni risultati in termini non solo di riduzione dei reclami presentati all'Autorità, ma anche di minore gravità delle fattispecie dedotte in contestazione. Nella maggior parte delle ipotesi esaminate, infatti, le misure preventive adottate dai fornitori hanno consentito agli interessati di intercettare l'evento in una fase anteriore allo *switching*, con conseguenziale inibizione del passaggio al nuovo fornitore, riducendo i pochi casi di illiceità del trattamento ad ipotesi isolate, attribuibili ai comportamenti scorretti e truffaldini di singoli agenti.

14.6. *Procedure IMI relative a trattamenti di dati personali in ambito economico*

Come già sottolineato (v. Relazione 2019, p. 157), dal 25 maggio 2018 le autorità di protezione dei dati accedono alla piattaforma IMI (*Internal Market System Information*), uno strumento veloce, sicuro, flessibile e trasparente utilizzato per la gestione dei meccanismi di cooperazione e coerenza previsti dal Capo VII del RGPD. La partecipazione alle procedure di cooperazione tra le autorità di protezione dei dati in presenza di trattamenti transfrontalieri occupa ormai una parte rilevante dell'attività dell'Autorità, sia in termini di risorse impegnate che di quantità di lavoro svolto (cfr. anche parr. 12.9, 21.1 e parte IV, tab. 10-12).

Per quanto riguarda il settore economico (e rinviando al par. 12.9 per un'indagine ravvicinata dedicata al settore delle comunicazioni elettroniche), si segnala che le procedure IMI riguardano casistiche eterogenee riferite ad una variegata pluralità di titolari del trattamento, considerata la granularità dell'ambito di riferimento, diversamente da altri settori – quali quello delle comunicazioni elettroniche e dei *social media* – in cui operano per lo più i cd. *over the top*.

Si conferma la prevalenza delle procedure IMI ai sensi dell'art. 56 del RGPD volte all'identificazione dell'autorità capofila (*Lead Supervisory Authority*) e delle autorità interessate (*Concerned Supervisory Authority*) che rappresentano circa il 90% delle procedure trattate.

Nel settore in esame, l'Autorità si è dichiarata "interessata" ai sensi dell'art. 4, n. 22 del RGPD, in 127 casi (pari al 43%) assumendo invece la posizione di "autorità capofila" in un numero molto limitato di casi riguardanti imprese con stabilimento unico o principale in Italia; in relazione a queste ultime fattispecie, esse si sono incentrare, in particolare, sul ritardo del titolare nel fornire riscontro all'istanza per l'esercizio dei diritti dell'interessato in violazione dell'art. 12, par. 3, del RGPD; sulla mancata adozione di adeguate misure di sicurezza in violazione dell'art. 32 del RDPD (in fase di registrazione e conservazione di *password*); sulla violazione dei dati personali consistenti nell'invio ad un terzo della corrispondenza intercorsa tra il titolare e l'interessato e nell'errata consegna ad un terzo di un pacco contenente foto personali dell'interessato.

Rimane invariato rispetto al 2019 il numero delle procedure IMI di consultazione informale previste dall'art. 60, par. 1, del RGPD. A questo proposito si rileva come nel settore in questione le autorità di protezione dei dati ricorrano ancora in misura insufficiente a tale specifica procedura di cooperazione che consente lo scambio di informazioni, valutazioni e documenti in ordine alle questioni oggetto della controversia. Ciò, nonostante l'invito più volte ribadito dal Comitato ad avviare una discussione fra le autorità di controllo coinvolte nel procedimento di cooperazione prima della fase decisoria vera e propria che si esplica con il "caricamento" sulla

piattaforma IMI del progetto di decisione da parte dell'autorità capofila. La scelta di quest'ultima di coinvolgere, attraverso tale consultazione preventiva, le autorità interessate anticipando il dibattito in ordine al progetto di decisione vero e proprio è infatti volta ad evitare che le stesse, una volta sottoposto loro il progetto di decisione, sollevino in merito obiezioni pertinenti e motivate, peraltro nei tempi strettissimi previsti dall'art. 60, par. 4, del RGPD. Tale approccio consente, già in una fase prodromica, di raggiungere un consenso in ordine al progetto di decisione fra le autorità che partecipano al procedimento di co-decisione previsto dal meccanismo dello sportello unico, limitando contemporaneamente il ricorso al meccanismo di coerenza previsto dall'art. 65, par. 1, lett. *a*), del RGPD per la composizione delle controversie da parte del Comitato.

Si è invece registrato un lieve aumento rispetto al 2019 delle procedure di cooperazione giunte alla fase decisoria. Rispetto ai progetti di decisione "caricati" sulla piattaforma IMI dalle competenti autorità capofila si è ritenuto, complessivamente, di condividerli, limitandosi a sollevare solo commenti o richieste di chiarimenti ove ritenuto opportuno. Solo in un caso, in relazione ad un progetto di decisione adottato dall'autorità di controllo francese (Cnil) in qualità di autorità capofila nei confronti di una società di *e-commerce*, l'Autorità, in quanto interessata ai sensi dell'art. 4, par. 22, lett. *b*), del RGPD, ha sollevato un'obiezione "pertinente e motivata" ai sensi del successivo art. 60, par. 4. In particolare, attraverso tale obiezione l'Autorità ha sottoposto all'attenzione della Cnil l'opportunità di riconoscere l'esistenza di una violazione del principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. *c*), del RGPD, anche con riguardo al trattamento eccedente dei dati contenuti nelle tessere sanitarie di clienti italiani per finalità antifrode, pur tenendo conto che tale violazione era avvenuta in un arco temporale limitato (circa tre settimane) e che tali dati erano stati in seguito distrutti dalla società. Successivamente, la Cnil ha trasmesso alle autorità interessate, sempre attraverso IMI, il progetto di decisione revisionato ai sensi dell'art. 60, par. 5, con il quale ha preso positivamente in considerazione i rilievi formulati, dando seguito alle obiezioni sollevate dal Garante e da altre autorità di protezione dei dati. Non essendo state formulate ulteriori osservazioni si è raggiunto il consenso in ordine a tale progetto di decisione che è divenuto pertanto vincolante per le autorità coinvolte nel procedimento come previsto dall'art. 60, par. 6, del RGPD.

Si segnala altresì che sono stati "caricati" sulla piattaforma IMI due progetti di decisione proposti dal Garante in qualità di "capofila". Nel primo caso, concernente un reclamo proposto da un cittadino tedesco che lamentava l'illecito trattamento dei dati personali per finalità di *telemarketing* nonché la violazione del diritto di cancellazione dei dati e di opposizione al trattamento previsti dagli artt. 17 e 21 del RGPD, l'Autorità, preso atto del riscontro fornito dalla società resistente nel corso dell'istruttoria, ha archiviato il procedimento non ravvisando una violazione della disciplina in materia di dati personali. Nel secondo, concernente un reclamo proposto (anche in questo caso) da un cittadino tedesco volto a segnalare un asserito illecito trattamento di dati personali in violazione dell'art. 32 del RGPD (il titolare gli avrebbe inviato, nella *e-mail* di conferma della registrazione al proprio sito web, la *password* "in chiaro"), l'Autorità, ritenute adeguate le misure di sicurezza adottate (che risultano comunque essere state rafforzate), ha deliberato la chiusura del procedimento, pur invitando il titolare del trattamento ad una scrupolosa e continua verifica degli standard di sicurezza utilizzati. Entrambi i progetti di decisione non sono stati oggetto di obiezioni pertinenti e motivate ai sensi dell'art. 60, par. 4, del RGPD da parte delle autorità interessate e pertanto è prossima l'adozione del relativo provvedimento ai sensi dell'art. 60, par. 8, del RGPD.

14

In due casi riguardanti trattamenti transfrontalieri con impatto esclusivamente locale (vale a dire esclusivamente nazionale) di cui all'art. 56, par. 2, del RGPD – posti in essere nell'ambito di rapporti di lavoro privato da titolari aventi stabilimento principale in altro Stato membro – l'Autorità ha attivato la specifica procedura IMI nei confronti delle competenti autorità capofila le quali hanno dichiarato di non avere interesse a trattare i casi secondo il meccanismo di *One stop shop* previsto dall'art. 60 del RGPD. L'Autorità, quindi, all'esito delle istruttorie che sono tuttora in corso, adotterà autonome decisioni nell'esercizio dei poteri di cui agli artt. 57 e 58 del RGPD, sempre limitatamente ai trattamenti con impatto esclusivamente locale, avendo cura di trasmetterle alle autorità capofila nell'ambito della mutua assistenza.

Per quanto riguarda l'assistenza reciproca fra le autorità di controllo ex art. 61 del RGPD, si conferma l'utilizzo della relativa procedura IMI allo scopo di ottenere informazioni sulle normative nazionali in tema di protezione dei dati o su questioni relative all'applicazione di particolari disposizioni del RGPD (ad es. sulla figura del Rpd esterno, prevista dall'art. 37; sull'applicabilità delle deroghe al divieto di trattamento di dati particolari previste dall'art. 9, par. 2, lett. *d*), del RGPD).

Brexit

Infine, si sottolinea che, in conseguenza della scadenza del periodo di transizione della Brexit, dal 31 dicembre 2020 l'autorità di controllo inglese (*Information Commissioner Office*-ICO) non è più coinvolta nelle procedure di cooperazione europea gestite attraverso la piattaforma IMI. Ne consegue che in merito ad alcuni casi tuttora pendenti, rispetto ai quali l'autorità di controllo inglese allo stato non è più capofila, il Garante è chiamato ora ad acquisire, anche attraverso contatti con i vari titolari, informazioni circa lo stabilimento principale eventualmente fissato in altro Stato membro in vista dell'individuazione dell'attuale autorità capofila (attraverso la procedura IMI di cui all'art. 56 del RGPD). Qualora invece lo stabilimento principale del titolare rimanga nel Regno Unito, non trovando più applicazione il meccanismo di *One Stop Shop*, il Garante, in quanto autorità competente ai sensi dell'art. 55 del RGPD, si interfaccerà direttamente con il titolare per il tramite del rappresentante designato ai sensi dell'art. 27 del RGPD o, in mancanza, attraverso contatti con lo stabilimento locale nel territorio italiano, ove esistente. Ciò ferma restando l'opportunità di avviare un coordinamento fra le autorità di protezione dei dati europee per stabilire piani di *enforcement* comuni e condivisi nei confronti di *big player* stabiliti nel Regno Unito che offrano servizi in più Paesi UE.

14.7. *Accreditamento e certificazioni*

Anche a fronte della intensa attività di collaborazione già avviata negli anni precedenti con le altre autorità europee per la protezione dei dati sul tema dell'accreditamento degli organismi di certificazione e della certificazione dei trattamenti (cfr. Relazione 2019, p. 158), il Garante ha approvato, previo parere favorevole del Comitato reso ai sensi dell'art. 64, par. 1, lett. *c*), del RGPD, i "Requisiti aggiuntivi di accreditamento degli organismi di certificazione" con il provvedimento del 29 luglio 2020 (in G.U. 12 agosto 2020, n. 201 e doc. web n. 9445086).

Tali requisiti, che integrano quelli individuati dalla norma tecnica EN-ISO/IEC 17065:2012, sono previsti dall'art. 43, parr. 1, lett. *b*), e 3, del RGPD, ai fini dell'accreditamento degli organismi che intendono rilasciare certificazioni sulla base di schemi nazionali o sigilli europei approvati ai sensi dell'art. 42, par. 5, del RGPD. Gli stessi sono stati elaborati in conformità alle linee guida 4/2019 in materia di accreditamento degli organismi di certificazione a norma dell'art. 43 del RGPD, adottate il 4 giugno 2019 dal Comitato e tengono conto del proficuo rapporto col-

laborativo con l'Ente nazionale di accreditamento (Accredia) consolidatosi nel 2019 con la sottoscrizione della relativa Convenzione (cfr. Relazione 2019, p. 159) e proseguito nel corso del 2020.

Accredia verificherà quindi il soddisfacimento da parte degli organismi di certificazione dei criteri di onorabilità, indipendenza e imparzialità, attestando l'assenza di conflitti di interesse con i titolari o responsabili che intendono certificarsi; l'adeguata qualifica, formazione e il costante aggiornamento delle risorse umane; l'adozione di efficienti processi di gestione di eventuali reclami, nonché di procedure per la periodica sorveglianza sui prodotti, processi e servizi certificati.

Con il citato provvedimento l'Autorità ha anche sottolineato l'importanza dello strumento della certificazione quale elemento di responsabilizzazione dei titolari o dei responsabili che possono così dimostrare la conformità al RGPD dei trattamenti svolti, accrescendo in tal modo anche la fiducia degli interessati riguardo alla gestione dei loro dati personali.

Qualificazione soggettiva ai fini *privacy* degli OdV

La nota del 12 maggio 2020 (doc. web n. 9347842) si è incentrata sulla questione della qualificazione soggettiva ai fini *privacy* degli Organismi di Vigilanza (OdV), di cui al d.lgs. 8 giugno 2001, n. 231, recante disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300. Le disposizioni contenute in tale normativa prevedono che l'ente (persona giuridica, società o associazione) non risponde per reati commessi nel suo interesse o a suo vantaggio da soggetti che ricoprono funzioni apicali e da persone sottoposte alla loro direzione o vigilanza, se dimostra di avere "adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire i reati della specie di quello verificatosi" e di avere "affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo" il compito di vigilare sul funzionamento e l'osservanza di detti modelli e di curarne l'aggiornamento (art. 6, comma 1, lett. *a*) e *b*), d.lgs. cit.). Tali organismi, pertanto, hanno il compito di vigilare sull'osservanza dei modelli di organizzazione e di gestione adottati dall'ente allo scopo di prevenire i reati commessi nell'interesse o a vantaggio dello stesso ente.

Pur prendendo atto con il citato parere che l'OdV è dotato di autonomi poteri di iniziativa e controllo, si è ritenuto che lo stesso non possa essere considerato quale autonomo titolare del trattamento (art. 4, par. 1, n. 7, del RGPD) con riferimento all'attività svolta in favore dell'ente; ciò tenuto conto che i compiti allo stesso affidati sono stabiliti dalla legge ma, di fatto, disciplinati dall'organo di vertice dell'ente che predispone il modello di organizzazione e gestione definendo anche gli aspetti relativi al funzionamento dell'OdV, compresa l'attribuzione delle risorse, i mezzi e le misure di sicurezza (art. 6, commi 1 e 2, d.lgs. n. 231/2001).

Analogamente, l'OdV non può essere considerato responsabile del trattamento, inteso come soggetto chiamato ad effettuare un trattamento "per conto del titolare", ovvero una "persona giuridicamente distinta dal Titolare, ma che agisce per conto di quest'ultimo" (art. 28 del RGPD), dal momento che l'OdV non è distinto dall'ente, ma è parte dello stesso.

Si è quindi ritenuto che l'OdV – a prescindere dalla circostanza che abbia una composizione monosoggettiva o plurisoggettiva e sia composto da membri interni o esterni all'ente – debba essere considerato nel suo complesso come "parte dell'ente". Ne deriva che sarà l'ente, in qualità di titolare del trattamento, nell'ambito delle misure tecniche e organizzative da porre in essere in linea con il principio di *accountability* (art. 24 del RGPD), a designare i singoli membri dell'OdV quali soggetti autorizzati (art. 2-*quaterdecies* del Codice) al trattamento dei dati personali, provvedendo anche ad impartire loro le relative istruzioni.

15 Il trattamento dei dati personali nell'ambito del condominio

In relazione ai numerosi reclami, segnalazioni e quesiti relativi a questioni inerenti il trattamento dei dati personali in ambito condominiale, l'attività dell'Autorità è stata orientata, da una parte, a fornire i necessari chiarimenti; dall'altra, a promuovere la consapevolezza da parte dei titolari e dei responsabili del trattamento degli obblighi previsti (anche in tale settore) dalla nuova normativa.

Nel confermare quanto già a suo tempo stabilito dal Garante nel provvedimento del 18 maggio 2006 sul tema (doc. web n. 1297626), è stato quindi ribadito – tenendo anche conto che i condomini devono essere considerati contitolari di un medesimo trattamento – che le informazioni personali riferibili a ciascun partecipante possono essere condivise all'interno della compagine condominiale purché le stesse vengano trattate per il perseguimento delle finalità di gestione ed amministrazione del condominio e nel rispetto, qualora i relativi adempimenti siano posti in essere anche tramite soggetti terzi, di quanto previsto dagli artt. 28 e 29 del RGPD.

Condominio e pandemia

Un altro aspetto che ha particolarmente interessato l'Autorità in ragione dello stato di emergenza epidemiologica ha riguardato la possibilità di raccogliere e condividere, anche nel contesto condominiale, informazioni in ordine alla salute degli interessati come misura di prevenzione dal contagio. In merito, nel richiamare l'attenzione sugli approfondimenti condotti nel corso dell'anno sul tema (v. doc. web n. 9293264), il Garante ha ritenuto necessario puntualizzare che la suddetta finalità di prevenzione può essere perseguita dai soli soggetti che istituzionalmente sono chiamati a svolgere queste funzioni (cfr. comunicato stampa 2 marzo 2020, doc. web n. 9282117). In termini generali, è stata colta l'occasione per rammentare che possono formare oggetto di trattamento nell'ambito delle menzionate finalità di amministrazione del condominio i "dati personali di natura sensibile […], nella misura indispensabile al perseguimento delle medesime finalità" (cfr. punto 2.4) e che il trattamento dei dati relativi allo stato di salute degli interessati deve essere svolto nel rispetto dei principi di liceità e correttezza, finalità, nonché di minimizzazione dei dati (artt. 4, par. 1, n. 15, 5 e 9 del RGPD).

Da ultimo, il Garante, richiamando in diverse occasioni l'attenzione degli interessati sulle previsioni 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 numerose istanze, ha avuto, ancora una volta, modo di ribadire che eventuali responsabilità derivanti da inadempimenti in ordine alle attribuzioni e ai compiti affidati all'amministratore di condominio in base alle norme del codice civile (art. 1117 cod. civ. ss.) concernono specifici profili di carattere civilistico rispetto ai quali non è riconosciuta alcuna competenza all'Autorità (cfr. Relazione 2019, p. 160).

16 Violazione dei dati personali

Dal 1° gennaio al 31 dicembre 2020 sono pervenute all'Autorità 1.387 notifiche di violazione dei dati personali ai sensi dell'art. 33 del RGPD o dell'art. 26, d.lgs. n. 51/2018 che hanno avuto ad oggetto, come titolari del trattamento, soggetti pubblici (nel 29% dei casi) e privati (nel 71% dei casi).

I casi più significativi hanno riguardato enti pubblici come l'Inps, interessato da violazioni dei dati personali nel periodo di avvio dei cd. *bonus* 600 euro e *babysitter*; diversi enti locali; la sanità, con la diffusione di dati relativi al Covid-19; il sistema scolastico e le università; il settore delle telecomunicazioni, energetico e bancario; enti pubblici non economici di rilievo nazionale; operatori privati nel settore bancario e dei servizi.

I fenomeni più frequentemente riscontrati sono consistiti in attacchi informatici di tipo *Distributed Denial of Service*, che hanno compromesso temporaneamente la disponibilità di importanti servizi *online* interferendo con le infrastrutture di rete; nella diffusione di *malware* di tipo *ransomware*, che ha compromesso la disponibilità dei dati all'interno dei sistemi *server*, delle postazioni di lavoro e dei *database* di numerose organizzazioni pubbliche e private, per lo più senza incidere sulla riservatezza delle informazioni; nella realizzazione di accessi non autorizzati ai dati trattati; nella diffusione accidentale di dati personali a causa di erronee configurazioni dei sistemi *software* di gestione della posta elettronica; in accessi abusivi alle aree di videoconferenza, particolarmente significativi in una fase in cui tali strumenti conoscevano una ampia e rapida diffusione legata all'emergenza pandemica e alla necessità di assicurare lo svolgimento di attività lavorative e didattiche a distanza.

L'attività istruttoria svolta a seguito delle notifiche di violazione dei dati personali ha avuto come duplice obiettivo quello di valutare le 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 necessità di effettuare la comunicazione della violazione agli interessati, fornendo loro indicazioni specifiche sulle misure che possono adottare per proteggersi da eventuali conseguenze pregiudizievoli.

Con riferimento ad alcune violazioni dei dati personali per cui i titolari del trattamento avevano ritenuto di non dover informare gli interessati coinvolti, l'Autorità, dopo aver valutato la probabilità che le violazioni presentassero un rischio elevato, ha richiesto ai titolari di provvedervi senza ritardo.

Nei casi in cui è emersa una possibile inadeguatezza delle misure di sicurezza adottate dal titolare, sono stati acquisiti gli elementi necessari a individuare le lacune organizzative e tecniche da cui hanno avuto origine le violazioni notificate. Tale attività di approfondimento, resa più difficoltosa a causa della sospensione delle attività ispettive (cfr. par. 18.2), ha portato all'adozione di alcuni provvedimenti collegiali di tipo prescrittivo e, nei casi più gravi, sanzionatorio.

Da dicembre 2020 il Garante ha messo a disposizione dei titolari del trattamento uno strumento di autovalutazione (*self assessment*) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza, aiutandoli nell'assolvimento degli obblighi di notifica all'au-

torità di controllo e di comunicazione all'interessato (artt. 33 e 34 del RGPD e artt. 26 e 27, d.lgs. n. 51/2018).

Inps

In occasione dell'avvio delle procedure per la richiesta di erogazione di prestazioni a sostegno del reddito legate alla situazione emergenziale da Covid-19 e previste dal decreto-legge 17 marzo 2020, n. 18 (cd. *bonus* Covid), si sono verificate alcune violazioni di dati personali sul portale dell'Inps che hanno comportato la visualizzazione, da parte di terzi, di dati personali riferiti a una ampia platea di beneficiari che hanno tentato di accedere contemporaneamente ai servizi *online*. A questo proposito, l'Istituto ha notificato al Garante due distinte violazioni di dati personali: la prima, riguardante l'accesso ai dati personali di utenti del portale www.inps.it da parte di terzi non autorizzati, determinato da una non corretta configurazione delle funzionalità di *caching* del servizio CDN (*Content Delivery Network*) utilizzato; la seconda, riguardante l'accesso ai dati personali di utenti che hanno richiesto l'erogazione del *bonus* per l'acquisto di servizi di *baby-sitting*, con visualizzazione, modifica, cancellazione o invio all'Inps di domande, contenenti dati personali riferiti a minori, anche con disabilità, da parte di terzi non autorizzati. Contestualmente, l'Autorità ha ricevuto numerosi reclami e segnalazioni da parte di utenti concernenti ulteriori e diversi profili e criticità.

Nelle more dello svolgimento della complessa istruttoria, il Garante ha ritenuto che le descritte violazioni dei dati personali fossero suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 34 del RGPD (in particolare, in considerazione del ruolo centrale rivestito dall'Istituto nel sistema previdenziale e assistenziale nazionale nel panorama delle grandi banche dati pubbliche, dell'impatto che le decisioni adottate, in relazione al trattamento di dati personali, hanno avuto sulla collettività e della natura delle violazioni), e ha ingiunto all'Inps di comunicare i *data breach* rilevati agli interessati coinvolti, rappresentando agli stessi la natura delle violazioni e le conseguenze che ne sarebbero potute derivare, nonché fornendo – unitamente ai dati di contatto del Rpd o di altro centro di competenza – indicazioni specifiche sulle misure che potevano adottare per proteggersi da eventuali conseguenze pregiudizievoli (provv. 14 maggio 2020, n. 86, doc. web n. 9344061).

***Data breach* in sanità e ricerca**

Numerose le notifiche di *data breach* pervenute ai sensi dell'art. 33 del RGPD con riferimento ai trattamenti di dati personali effettuati in ambito sanitario dalle quali sono scaturite numerose istruttorie.

Con provvedimento del 1° ottobre 2020, n. 174 (doc. web n. 9469345), il Garante ha sanzionato un ospedale che aveva notificato una violazione dei dati personali in relazione al sistema dedicato al servizio di consultazione *online* dei referti (nel caso di specie concernente immagini radiologiche associate a dati identificativi e referti clinici di 74 altri utenti). Nel provvedimento il Garante ha evidenziato che, seppure la condotta oggetto dell'istruttoria fosse iniziata prima della data di piena applicazione del Regolamento, al fine della determinazione della norma applicabile sotto il profilo temporale doveva essere richiamato il principio di cui all'art. 1, comma 2, l. n. 689/1981, secondo cui devono essere prese in considerazione le disposizioni vigenti al momento della commessa violazione: nel caso di specie, considerata la natura permanente della condotta contestata, il momento di cessazione della condotta illecita è risultata essere successiva al 25 maggio 2018, data in cui il Regolamento è divenuto pienamente applicabile.

Il Garante ha altresì accertato che, a causa di un errore umano nella configurazione di un sistema informatico, protrattosi per un ampio arco temporale, si era verificata la possibilità che gli utenti del servizio di consultazione *online* dei referti potessero visualizzare i dati relativi alla salute di altri 74 utenti (specificatamente

le immagini radiologiche associate a dati identificativi e referti clinici) e che tale evenienza si era effettivamente verificata con riferimento a 39 utenti. Pur essendo il titolare intervenuto sul sistema informatico, il trattamento è risultato in violazione del principio di integrità e sicurezza dei dati.

In altra vicenda il Garante ha ammonito una azienda sanitaria in relazione all'invio di una segnalazione di malattia infettiva per un caso di scabbia di un minorenne (cd. caso indice) che, contrariamente a quanto previsto dalle disposizioni di settore, consentiva di identificare l'interessato (in quanto effettuata con un'unica comunicazione sia all'istituto scolastico, sia a una associazione, entrambi frequentati dall'interessato). Il Garante ha ritenuto effettuata una comunicazione di dati relativi alla salute di un paziente minore in assenza di un idoneo presupposto giuridico e, quindi, in violazione dei principi di base del trattamento di cui all'art. 5, del RGPD, nonché in violazione dell'art. 9 del Regolamento (provv. 1° ottobre 2020, n. 176, doc. web n. 9486446).

In considerazione del fatto però che l'episodio risultava essere stato isolato e determinato da un evento sicuramente colposo; che l'Autorità aveva preso conoscenza dell'evento a seguito della notifica di violazione dei dati personali effettuata dallo stesso titolare; che non erano pervenuti reclami o segnalazioni al Garante sull'accaduto e che, nei confronti dell'operatore che aveva inviato la segnalazione, l'azienda aveva già valutato, nell'ambito di apposito procedimento, le responsabilità disciplinari, l'Autorità ha qualificato il fatto come violazione minore, ai sensi del cons. 148 del RGPD e delle linee guida WP 253, riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del RGPD.

In un altro caso, il Garante ha adottato un provvedimento di ammonimento nei confronti di una struttura del servizio sanitario locale per aver inviato una comunicazione in merito al rispetto degli obblighi vaccinali ai genitori dei bambini in posizione di non regolarità vaccinale con piena visibilità gli indirizzi *e-mail* dei sedici genitori destinatari della comunicazione (provv. 9 gennaio 2020, n. 1, doc. web n. 9261234). Come già indicato dal Garante, le informazioni relative alla non regolarità vaccinale devono essere qualificate idonee a rivelare lo stato di salute dei minori, poiché tra i soggetti non in regola con l'obbligo vaccinale non è possibile escludere che siano ricompresi minori rientranti nei casi di esonero, omissione o differimento connesse a situazioni di morbilità, pregresse o attuali, temporanee o permanenti (cfr. nota del Presidente Soro 20 ottobre 2017, doc. web n. 7055771). L'invio di una comunicazione mediante un unico messaggio di posta elettronica indirizzato a un numero plurimo di destinatari inseriti nel campo copia conoscenza, ha, in assenza di qualsivoglia presupposto normativo, rivelato reciprocamente, alle famiglie coinvolte, lo stato di inadempimento rispetto agli obblighi vaccinali relativi ai minori. Il Garante ha così ammonito il titolare ritenendo che la finalità della comunicazione potesse essere utilmente raggiunta inserendo gli indirizzi dei destinatari nel campo denominato copia conoscenza nascosta.

Con riferimento ai casi di diffusione *online* di dati sulla salute, il Garante ha ammonito anche una società per aver reso conoscibili a chiunque i dati relativi a prestazioni sanitarie effettuate da un interessato presso una determinata azienda sanitaria, pubblicandole in una pagina web accessibile senza alcuna procedura di autenticazione. Il Garante ha ritenuto che la società abbia effettuato una diffusione di dati relativi alla salute di un paziente in assenza di un idoneo presupposto giuridico e, quindi, in violazione dei principi di base del trattamento di cui all'art. 5, par. 1. lett. *a*) e *f*), del RGPD, nonché in violazione degli artt. 9 e 32 del Regolamento. Anche in questo procedimento, le circostanze del caso concreto (si è trattato di un episodio unico e isolato, determinato da un comportamento colposo della società,

l'indirizzo web seppure pubblico, non risultava facilmente raggiungibile in quanto doveva essere noto l'indirizzo Ip del *server*, i *file* in questione erano in un formato non facilmente fruibile, senza la disponibilità di un opportuno programma di visualizzazione, assenza di reclami o segnalazioni sull'accaduto) hanno consentito al Garante di qualificare la violazione come minore (art. 83, par. 2, cons. 148 del RGPD e linee guida WP 253) e di ammonire la società affinché provvedesse a rispettare le richiamate previsioni del RGPD (provv. 9 luglio 2020, n. 142, doc. web n. 9446166).

Sempre nel corso del 2020, le istruttorie avviate a seguito di comunicazioni di violazioni di dati personali effettuate da aziende e strutture sanitarie in diversi casi hanno avuto ad oggetto l'erronea comunicazione della documentazione clinica a un soggetto diverso dall'interessato (cfr. provv.ti 18 giugno 2020, n. 103, doc. web n. 9451705 e 2 luglio 2020, n. 123, doc. web n. 9440096).

***Data breach* in ambito bancario**

Anche il settore bancario risulta essere uno di quelli maggiormente esposti al fenomeno dei *data breach*. Numerose sono state infatti le violazioni dei dati personali che gli istituti di credito hanno notificato all'Autorità ai sensi dell'art. 33 del RGPD. In alcuni casi, laddove l'Autorità ha ritenuto di non poter disporre l'archiviazione, ai necessari approfondimenti tecnico-informatici ha fatto seguito un'istruttoria ai fini dell'individuazione delle fattispecie di illiceità che sono state poi oggetto della comunicazione, ai sensi dell'art. 166, comma 5, del Codice, di avvio del procedimento per l'adozione dei provvedimenti correttivi di cui all'art. 58, par. 2 e delle sanzioni di cui all'art. 83 del RGPD.

In particolare, l'Ufficio è stato impegnato nell'attività istruttoria relativa ad alcuni significativi *data breach* che hanno interessato importanti gruppi bancari (taluni dei quali ancora in corso approfondimento). Una delle istruttorie è stata definita con provvedimento del 14 gennaio 2021, n. 4 (doc. web n. 9582744) nei confronti di istituti di credito afferenti ad un medesimo gruppo bancario. Si è trattato di una violazione dei dati personali che ha coinvolto (oltre a numerosi enti e società) circa 300 persone fisiche, violazione che si è verificata a seguito dell'invio, tramite posta elettronica certificata, da parte del responsabile del trattamento (una società facente parte del medesimo gruppo bancario), di estratti conto a clienti diversi dagli intestatari dei rapporti bancari cui gli estratti medesimi si riferivano. L'incidente si è verificato a causa di un malfunzionamento del *software* per l'invio di *e-mail* tramite Pec il cui "rilascio nell'ambiente di produzione" è avvenuto sulla base di test che sono stati effettuati solo parzialmente e in assenza di controllo da parte delle strutture aziendali preposte. L'Autorità, sulla base dei riscontri forniti dai titolari e dal responsabile del trattamento nel corso dell'istruttoria, ha ritenuto che, sebbene l'incidente si sia verificato nell'ambito dell'operatività del responsabile del trattamento (i cui dipendenti hanno agito in parziale violazione delle istruzioni ricevute), lo stesso coinvolgesse pienamente i titolari del trattamento. Questi ultimi – cui è attribuita la responsabilità generale del trattamento da essi posto in essere direttamente o che altri abbiano effettuato per loro conto – hanno omesso di verificare, in relazione alla natura, al contesto, alle finalità e ai rischi del trattamento realizzato nell'ambito del processo di gestione delle modifiche ai sistemi informatici l'effettiva conformità dello stesso ai principi di integrità e riservatezza di cui all'art. 5, par. 1, lett. *f*), e agli obblighi in materia di sicurezza del trattamento di cui all'art. 32, parr. 1 e 2, lett. *b*) e *d*), del RGPD.

Merita sottolineare che l'Autorità, nel determinare l'ammontare della sanzione pecuniaria inflitta ai titolari del trattamento, ha tenuto in particolare considerazione, tra gli altri criteri previsti dall'art. 83, par. 2, del RGPD, l'atteggiamento ampiamente collaborativo manifestato dai titolari del trattamento, sia in termini di osservanza degli obblighi di cui agli artt. 33 e 34 del RGPD, sia nel senso dell'efficacia delle

attività profuse (seppure *ex post*) al fine di porre rimedio a quanto accaduto e attenuarne così gli effetti negativi (art. 83, par. 2, lett. *f*), del RGPD) nei confronti degli interessati coinvolti.

In un altro caso, il Garante ha ingiunto a un istituto bancario – che aveva segnalato di aver inviato documentazione bancaria a soggetti diversi dagli effettivi destinatari – di comunicare la violazione dei dati personali agli interessati coinvolti, fornendo almeno le informazioni di cui all'art. 34, par. 2, del RGPD (provv. 10 dicembre 2020, n. 264, doc. web n. 9557555).

L'Autorità ha fornito i propri contributi in relazione a diversi casi transfrontalieri di violazione di dati personali che hanno coinvolto interessati in diversi Paesi dell'Unione europea, fra cui l'Italia. Fra i principali, si ricordano i casi di un primario operatore di trasporto aereo e di una catena alberghiera, per i quali l'autorità di controllo capofila ha adottato la decisione finale nel secondo semestre del 2020, nonché il caso Twitter che ha portato all'avvio della procedura di risoluzione delle controversie e all'adozione della prima decisione del Cepd a norma dell'art. 65 del RGPD (cfr. par. 21.1).

***Data breach* transfrontalieri**

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 rivolta alle novità introdotte a seguito dell'adozione, da parte della CGUE, della pronuncia cd. Schrems II (cfr. causa C-311/18) e dei documenti del Comitato europeo per la protezione dei dati, recanti raccomandazioni sulle misure volte a garantire, nel contesto dei trasferimenti transfrontalieri di dati, il rispetto del RGPD (cfr. par. 21.1).

Al riguardo, di particolare rilievo è stata l'attività di collaborazione tra il Garante e le altre autorità di controllo europee, posta in essere nell'ambito di una *task force* incaricata di coordinare l'esame di 101 reclami presentati nei confronti di diversi titolari del trattamento stabiliti negli Stati membri del See in merito all'utilizzo, tramite i loro siti internet, di servizi prestati da Google e Facebook che comportano il trasferimento dei dati personali degli utenti verso gli Stati Uniti. In tale ambito, e con specifico riferimento ai reclami pervenuti al Garante, è stata avviata una preliminare attività istruttoria, tuttora in corso, volta ad acquisire maggiori elementi in merito alle garanzie adottate dai titolari e dai responsabili coinvolti a seguito della dichiarazione della CGUE in ordine all'invalidità della decisione della Commissione n. (UE) 2016/1250 (cd. Scudo UE-USA - *Privacy Shield*) ai fini del trasferimento all'estero dei dati degli interessati.

È proseguita l'attività di valutazione delle istanze pervenute in ordine all'approvazione di Norme vincolanti di impresa (cd. *Binding corporate rules* - Bcr) ai sensi dell'art. 47 del RGPD, volte a chiedere il coinvolgimento dell'Autorità in qualità di *Bcr Lead*. In particolare, il ruolo del Garante quale capofila della procedura europea di cooperazione è stato formalizzato con riferimento ad un procedimento inerente ad un gruppo multinazionale d'imprese, *leader* nel settore delle infrastrutture digitali, previa verifica della sussistenza dei requisiti di cui al WP 263 (documento del Gruppo Art. 29, dell'11 aprile 2018). In tale veste, è stata effettuata una prima articolata analisi dei documenti pervenuti, anche grazie a frequenti interlocuzioni con il gruppo finalizzate ad apportare al testo delle Bcr proposto le modifiche necessarie a ricomprendere tutti gli elementi indicati dal WP 256 (documento del Gruppo Art. 29, del 6 febbraio 2018) e, più in generale, a conformare lo stesso al RGPD; ciò anche al fine della sua successiva trasmissione, ai sensi dell'art. 57, par. 1, lett. *g*), del RGPD, alle autorità di controllo che saranno individuate quali *co-reviewer* nell'ambito della relativa procedura europea di cooperazione.

Il Garante ha infine continuato a fornire chiarimenti su vari quesiti pervenuti in merito a quanto previsto nel Capo V del RGPD (cfr. Relazione 2019, p. 162) concernenti, tra l'altro, l'utilizzo delle deroghe in specifiche situazioni (v. art. 49 del RGPD), l'applicazione delle clausole tipo di protezione dei dati ex art. 46, par. 1, lett. *c*), del RGPD, le norme vincolanti d'impresa e la loro approvazione ai sensi dell'art. 47 del RGPD.

18 L'attività ispettiva

18.1. *I poteri di indagine e il regolamento del Garante n. 1/2019*

La complessiva cornice normativa all'interno della quale si inscrivono i poteri di indagine del Garante (già puntualmente descritti nella Relazione 2018, p. 170 ss.) a seguito del RGPD e delle significative modifiche al Codice introdotte dal decreto legislativo 10 agosto 2018, n. 101, come pure di quelle introdotte con il regolamento del Garante 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), ha ulteriormente valorizzato le attività ispettive nonché le attività di revisione, previste dall'art. 58, par. 1, lett. *b*), del RGPD. Il rafforzamento dei poteri istruttori delle autorità di protezione dei dati si caratterizza per alcune novità riguardanti le modalità di svolgimento delle attività di controllo realizzate a cura del Dipartimento attività ispettive, se del caso con l'ausilio della Guardia di finanza (v. par. 18.2), prevedendo che, con 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 e agli archivi;
- acquisire copia delle banche dati e degli archivi su supporto informatico.

18.2. *La programmazione dell'attività ispettiva e i principali settori oggetto di controllo*

La pandemia ha penalizzato fortemente lo svolgimento delle attività ispettive *in loco* (in ipotesi anche nella forma delle ispezioni congiunte, ora previste dall'art. 62 del RGPD), sia quelle delegate al Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza, sia quelle da svolgersi a cura dell'Ufficio: ventuno sono state così le ispezioni *in loco* effettuate nei primi mesi dell'anno, prima della sospensione dovuta all'emergenza sanitaria. Tuttavia, per far fronte alle difficoltà logistiche che ne sono derivate, sulla base di uno specifico ordine di servizio dirigenziale del 1° giugno 2020, sono state avviate verifiche da remoto in relazione ai trattamenti di dati personali effettuati tramite siti web.

Le ispezioni 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 dell'Autorità (*Newsletter* 18 febbraio 2020, n. 462, doc. web n. 9266789; *Newsletter* 26 ottobre 2020, n. 469, doc. web n. 9469615) e l'Ufficio, sulla base dei criteri stabiliti dal Garante, ha individuato le categorie dei titolari dei trattamenti da sottoporre a controllo negli ambiti di seguito indicati:

- trattamenti di dati personali effettuati da enti pubblici relativamente alla cd. medicina di iniziativa;
- trattamenti di dati relativi alla salute effettuati da società multinazionali ope-

ranti nel settore farmaceutico e sanitario;
- trattamenti di dati personali effettuati nel quadro dei servizi bancari *online*;
- trattamenti dei dati personali effettuati mediante applicativi per la gestione delle segnalazioni di condotte illecite (cd. *whistleblowing*);
- trattamenti dei dati personali effettuati da intermediari per la fatturazione elettronica;
- trattamenti di dati personali effettuati da enti pubblici in tema di rilascio di certificati anagrafici e di stato civile, attraverso l'accesso all'Anagrafe nazionale della popolazione residente (Anpr);
- trattamenti di dati personali effettuati da società ed enti pubblici per la gestione e la registrazione delle telefonate nell'ambito del servizio di *call center*;
- trattamenti di dati personali effettuati da società per attività di *marketing*;
- trattamenti di dati personali effettuati da società con particolare riferimento all'attività di profilazione degli interessati che aderiscono a programmi di fidelizzazione;
- trattamenti di dati personali effettuati da società rientranti nella filiera della cd. *food delivery*;
- trattamento di dati personali effettuati da società in tema di banche dati cd. reputazionali;
- *data breach*.

Le verifiche, nel corso delle quali specifica attenzione è stata prestata ai profili sostanziali del trattamento (che spiegano significativi effetti sulle persone interessate) nonché al rispetto del generale principio di responsabilizzazione posto in capo al titolare del trattamento dall'art. 5 del RGPD, si sono incentrate sui seguenti aspetti:
- l'adozione di misure di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di categorie particolari 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.

Le attività ispettive, avviate anche sulla base delle precedenti programmazioni, hanno così riguardato le seguenti categorie di titolari del trattamento:
- 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, in particolare, l'eventuale attività di *marketing* nei confronti degli interessati o di comunicazione dei dati personali a soggetti terzi, nonché 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, in particolare, 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 formulate proposte di adozione di provvedimenti inibitori e/o prescrittivi per conformare il trattamento alla legge, a fronte delle quali il Garante ha adottato alcuni provvedimenti particolarmente significativi oggetto di illustrazione in più luoghi della Relazione.

18.3. *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, a seguito di una proficua collaborazione ed interlocuzione tra i due Enti, è stato rinnovato il 30 marzo 2021. Tale aggiornamento si è reso indispensabile 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 dal luglio 2018, ha visto la soppressione del Nucleo speciale *privacy* e l'istituzione del Nucleo speciale tutela *privacy* e frodi tecnologiche.

Tale rinnovata collaborazione, che prevede l'aumento del personale distaccato presso il Garante da quattro a sei unità, consentirà all'Autorità, anche grazie all'apporto della nuova unità speciale che ingloba le competenze in ambito tecnologico, di avvalersi di un efficace sostegno allo svolgimento delle proprie funzioni ispettive, conoscitive ed informative sui fenomeni che riguardano, nei contesti pubblici e privati, il trattamento dei dati personali. Il nuovo Protocollo d'intesa introdurrà, 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 di controllo dell'UE.

Da un punto di vista più strettamente operativo, invece, l'adozione del Protocollo ha finora consentito: un ampliamento delle verifiche ispettive dell'Autorità attraverso ulteriori controlli puntuali presso i vari titolari del trattamento presenti sul territorio nazionale; una semplificazione dei flussi documentali tra l'Ufficio e il Nucleo speciale tutela *privacy* e frodi tecnologiche (grazie all'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, nella fase preliminare di controllo, di ispezioni *in loco*).

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 principi previsti dalla legge; ove nell'ambito dell'ispezione emergano violazioni di rilevanza penale, la Guardia di finanza procede direttamente alla segnalazione della notizia di reato all'Autorità giudiziaria.

Come previsto dal 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 più recenti innovazioni legislative) e dei provvedimenti dell'Autorità.

Si può quindi osservare che, grazie alla sinergia ormai collaudata con il Nucleo speciale, 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, delle necessarie verifiche *in loco* sull'intero territorio nazionale.

19 L'attività sanzionatoria del Garante

L'applicabilità del RGPD – con particolare riferimento al rigoroso regime delle sanzioni amministrative pecuniarie previsto dall'art. 83 del RGPD – e l'approvazione del decreto legislativo n. 101/2018 – che pure individua fattispecie penalmente rilevanti agli artt. 167-171 (rispetto alle quali devono registrarsi otto comunicazioni di notizie di reato effettuate dall'Autorità nel 2020: cfr. parte IV, tab. 1 e 8) – hanno profondamente modificato il quadro sanzionatorio in materia di protezione dei dati personali.

Dal punto di vista operativo, 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 e nel 2020 il Garante ha dovuto provvedere alla gestione straordinaria dell'avvio delle procedure di riscossione coattiva per tutti i procedimenti sanzionatori che non fossero stati 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 quanti 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, comma 2, d.lgs. n. 101/2018, prevedeva 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.

Come anticipato al par. 18.1, si è avviata un'attività di analisi e revisione degli atti di accertamento ispettivo condotti da altri organi accertatori (principalmente, il Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza) al fine di individuare possibili violazioni e adottare quindi i necessari provvedimenti correttivi e sanzionatori.

19.1. *La rilevazione di criticità a seguito di accertamenti ispettivi*

Le modifiche normative e regolamentari sopra richiamate hanno mutato in maniera rilevante le attività relative alla rilevazione di violazioni amministrative del Codice nel corso di accertamenti ispettivi. Prima del 25 maggio 2018, oltre al personale dell'Ufficio addetto all'attività ispettiva, poteva rilevare e contestare una violazione del Codice 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. Oggi l'Autorità è l'unico organo competente ad avviare i procedimenti

amministrativi sanzionatori a fronte dell'accertamento di possibili violazioni e ad irrogare le relative sanzioni. Di conseguenza, le risultanze degli accertamenti ispettivi condotti dal Nucleo speciale o da altri enti esterni sono sottoposte all'esame del Dipartimento attività ispettive che, valutata la configurabilità di possibili violazioni del RGPD e del Codice, propone l'avvio dei relativi procedimenti sanzionatori e/o l'adozione di altre misure correttive ai competenti dipartimenti dell'Autorità. Sono state così rilevate n. 87 possibili violazioni delle disposizioni del RGPD e del Codice nei confronti di n. 22 distinti soggetti, prevalentemente in relazione a trattamenti effettuati per finalità di *marketing* e profilazione, anche in relazione a minori di età. Al riguardo, sono state trasmesse le risultanze per la successiva valutazione e formale contestazione da parte del Dipartimento competente, ai sensi dell'art. 22, comma 1, reg. Garante n. 1/2019. Le suddette violazioni, in ordine di frequenza riscontrata, sono così suddivise:

- n. 16 casi di omessa o inidonea informativa per i dati raccolti presso l'interessato (art. 13 del RGPD);
- n. 15 casi di violazione dei principi generali applicabili al trattamento di dati personali (art. 5 del RGPD);
- n. 11 casi di violazione delle condizioni per la liceità del trattamento (art. 6 del RGPD);
- n. 11 casi di violazione delle condizioni per il consenso dell'interessato (art. 7 del RGPD);
- n. 8 casi di mancata o inidonea valutazione di impatto sulla protezione dei dati (art. 35 del RGPD);
- n. 6 casi di omessa o irregolare tenuta del registro delle attività di trattamento (art. 30 del RGPD);
- n. 4 casi di omessa o inidonea designazione del responsabile del trattamento (art. 28 del RGPD);
- n. 4 casi di trattamento sotto l'autorità del titolare o del responsabile svolto in assenza di istruzioni (art. 29 del RGPD);
- n. 4 casi di omessa o inidonea designazione del Responsabile della protezione dei dati (art. 37 del RGPD);
- n. 3 casi di omessa o inidonea informativa per dati che non siano stati ottenuti presso l'interessato (art. 14 del RGPD);
- n. 2 casi di violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (art. 8 del RGPD);
- n. 1 caso di violazione relativa al trattamento di categorie particolari di dati personali (art. 9 del RGPD);
- n. 1 caso di violazione del principio di responsabilità del titolare del trattamento (art. 24 del RGPD);
- n. 1 caso di mancata adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio (art. 32 del RGPD).

Alcune di tali violazioni hanno riguardato il trattamento di dati personali di soggetti minori di età effettuato ai fini dello svolgimento dell'attività di *marketing*; in particolare, è stata rilevata la non conformità del trattamento all'art. 8, par. 3, del RGPD e all'art. 2-*quinquies*, d.lgs. n. 101/2018, in ragione del fatto che il titolare del trattamento non aveva provveduto all'adozione di meccanismi di verifica dell'età dell'utente minorenne (cfr. linee guida 05/2020 sul consenso adottate il 4 maggio 2020, punto 7.1.3).

19

19.2. *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 consentito la definizione in maniera agevolata di 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 al 25 maggio 2018.

Alla data di entrata in vigore del 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 era quindi ammesso il pagamento in misura ridotta, entro novanta giorni dalla data di entrata in vigore del decreto legislativo n. 101/2018 (pertanto, entro il 18 dicembre 2018), di una somma pari a due quinti del minimo edittale.

In realtà, tale procedura di definizione agevolata non ha registrato un'elevata adesione da parte dei soggetti coinvolti e solo 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 2020, l'Autorità ha effettuato ulteriori n. 308 iscrizioni a ruolo relativamente ai residui procedimenti sanzionatori definiti automaticamente per effetto delle previsioni di cui al citato art. 18 (in ragione del 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 2020 è stato pari a 5.414.800 euro.

Ricapitolando, l'attuazione delle disposizioni relative al mancato esercizio da parte dei trasgressori della facoltà di definizione agevolata dei procedimenti sanzionatori pendenti, prevista dall'art. 18, d.lgs. n. 101/2018, ha condotto, complessivamente, alla chiusura di n. 1.094 procedimenti sanzionatori ed alla conseguente iscrizione a ruolo delle sanzioni dovute per un totale pari a euro 17.345.867.

Oltre a quanto sopra evidenziato, l'Autorità ha provveduto ad avviare la riscossione coattiva delle sanzioni irrogate con alcuni provvedimenti di ordinanza-ingiunzione, prevalentemente a seguito di decisioni favorevoli adottate dall'Autorità giudiziaria presso la quale gli stessi erano stati impugnati (cfr. par. 20.3).

19.3. *Versamenti relativi alle sanzioni amministrative*

Il totale incassato nel 2020 sul capitolo del Tesoro per sanzioni comminate dal Garante è pari a € 38.448.895,38. Di questi, € 2.185.782,06 vengono dalla riscossione coattiva e € 36.263.113,32 da pagamenti spontanei dei contravventori.

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.

19.4. *Il quadro sanzionatorio introdotto dal RGPD*

La complessiva riforma della normativa in materia di protezione dati si caratterizza, come è noto, per un più rigoroso assetto delle sanzioni amministrative pecuniarie che rappresentano un elemento centrale con il quale le autorità di controllo – come pure accaduto al Garante in talune occasioni nel corso del 2020 (cfr., in particolare, par. 11.1) – possono articolare le misure correttive a fronte delle violazioni poste in essere da parte del titolare o del responsabile del trattamento. Se una puntuale ricostruzione del nuovo assetto normativo con riguardo alle sanzioni è rinvenibile nella Relazione 2018 (alla quale si fa pertanto rinvio: cfr. p. 181) merita qui rilevare che l'applicazione coerente nella cornice europea delle norme in materia di sanzioni amministrative pecuniarie rappresenta un elemento cruciale del nuovo regime introdotto dal RGPD.

In tale prospettiva, ai sensi dell'art. 70, par. 1, lett. *e*), del RGPD, il Comitato ha la facoltà di pubblicare linee guida, raccomandazioni e curare la redazione delle migliori prassi al fine di promuovere l'applicazione coerente del RGPD; più precisamente, l'art. 70, par. 1, lett. *k*), del RGPD, specifica che è prevista l'elaborazione di linee guida riguardanti la previsione di sanzioni amministrative pecuniarie. A tal fine, l'Autorità partecipa attivamente alla *Task force fining* istituita ai fini della predisposizione di tali linee guida nell'ambito dei lavori del Comitato per un'armonizzata applicazione dei criteri di valutazione fissati dall'art. 83, par. 2, del RGPD.

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 16 ricorsi notificati nel 2018 e dei 49 nel 2019, nel 2020 sono stati notificati all'Autorità e da questa trattati 56 ricorsi.

Permane comunque la rilevanza dell'obbligo per le cancellerie – purtroppo non sempre puntualmente adempiuto – di trasmettere al Garante copia dei provvedimenti emessi dall'Autorità giudiziaria in relazione 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, è funzionale al monitoraggio dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e consente altresì di assolvere al meglio il compito di "consulenza" a vantaggio di Parlamento e Governo segnalando gli interventi normativi ritenuti necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f*), del Codice).

20.2. *I profili procedurali*

In tema di incompetenza funzionale si sono avute due pronunce. In un primo caso, la Corte di appello di Firenze, con sentenza 23 dicembre 2019, n. 3102, decidendo sull'impugnazione di una sentenza del Tribunale di Prato in relazione all'omesso rispetto dell'obbligo di notificazione del trattamento di dati biometrici, ha dichiarato l'inammissibilità dell'appello, in quanto, ai sensi dell'art. 152, comma 13, d.lgs. n. 196/2003, avverso la sentenza si sarebbe dovuto proporre ricorso per cassazione.

In un altro caso, la Corte di cassazione ha dichiarato inammissibile il ricorso proposto dal Garante a seguito dell'annullamento di una cartella di pagamento emessa a carico di una società per omessa informativa, poiché la diretta ricorribilità per cassazione è prevista per le controversie relative all'applicazione delle disposizioni del Codice e non, come nel caso di specie, per quelle relative alla riscossione della relativa sanzione alla quale si applica la disciplina generale della responsabilità amministrativa prevista (in generale) dalla legge n. 689/1981.

Non si sono riscontrate pronunce che hanno dichiarato un difetto di competenza territoriale né per materia.

20.3. *Le opposizioni ai provvedimenti del Garante*

L'anno 2020 ha registrato un notevole incremento nella proposizione delle opposizioni a provvedimenti dell'Autorità, 171 a fronte dei 109 ricorsi del 2019. Di

queste, 130, di cui 119 cartelle esattoriali emesse ex art. 18 d.lgs. n. 101/2018, si riferiscono a opposizioni a ordinanze-ingiunzioni, in sensibile crescita rispetto alle 50 del 2019. Di seguito si dà conto delle sentenze di maggior rilievo.

Complessivamente l'Autorità, avuto notizia di 56 decisioni giurisdizionali relative a opposizioni a provvedimenti del Garante (delle quali 33 relative a ordinanze-ingiunzioni, di cui 11 cartelle di pagamento), si è sempre costituita tramite l'Avvocatura dello Stato territorialmente competente.

Tra le decisioni che hanno avuto ad oggetto cartelle esattoriali emesse ai sensi dell'art. 18, d.lgs. n. 101/2018, in un caso il Tribunale di Bologna, con sentenza 9 giugno 2020, n. 863, ha respinto il ricorso proposto ex artt. 152, d.lgs. n. 196/2013 e 10, comma 3, d.lgs. n. 150/2011 da un ente ospedaliero avverso la cartella esattoriale, notificata al suddetto istituto ed emessa dall'Agenzia delle entrate, nonché avverso l'atto di contestazione del Garante del 19 marzo 2018, trasformatosi in ordinanza-ingiunzione ai sensi dell'art. 18, d.lgs. n. 101/2018. Nella fattispecie, circa la richiesta di disapplicazione del menzionato art. 18, il giudice ha confermato la linea difensiva proposta dall'Autorità escludendo che il meccanismo ivi previsto possa costituire una violazione del diritto di difesa poiché le esigenze di semplificazione e di deflazione delle impugnazioni avverso le violazioni alla disciplina della protezione dei dati personali rappresentate dalla normativa introdotta sono state affiancate dall'attribuzione al contravventore della facoltà di scelta se pagare una sanzione in misura ridotta pari ai due quinti del minimo e porre fine al procedimento, ovvero esercitare pienamente il suo diritto di difesa presentando al Garante una ulteriore memoria difensiva, che modificasse ovvero anche meramente ripercorresse le argomentazioni già svolte nella precedente memoria prima di presentare eventualmente ricorso all'Autorità giurisdizionale. Secondo il Tribunale, la circostanza che il ricorrente non si sia avvalso delle molteplici facoltà che la legge ha previsto va ascritta a esclusiva responsabilità dello stesso, non potendo l'opponente lamentare la non conoscenza della norma in esame, poiché secondo la costante giurisprudenza successiva alla sentenza della Corte costituzionale n. 364/1988, l'ignoranza della legge è scusabile quando è inevitabile ed in questo caso il testo del d.lgs. n. 101/2018 è stato pubblicato in G.U. 4 settembre 2018, n. 205. Peraltro, con comunicato stampa del 1° ottobre 2018 il Garante aveva altresì fornito indicazioni operative per chiarire ai soggetti pubblici e privati come usufruire della definizione agevolata dei procedimenti sanzionatori pendenti. Alla luce delle sopra esposte considerazioni, il Tribunale ha concluso che l'art. 18, d.lgs. n. 101/2018 non si pone in contrasto con il RGPD.

Per le medesime ragioni, il Tribunale ha ritenuto manifestamente infondata la prospettata eccezione di illegittimità costituzionale dell'art. 18, d.lgs. n. 101/2018 – nella parte in cui prevede che l'atto con il quale sono stati notificati gli estremi della violazione o l'atto di contestazione immediata di cui all'art. 14, l. n. 689/1981 assuma il valore di ordinanza-ingiunzione e nella parte in cui ammette la sola facoltà (e non l'obbligatorietà) della notifica del provvedimento stesso – per violazione degli artt. 3, 23, 24, 25, 97, 111 Cost. e 6 CEDU.

Rispetto a quanto rilevato in precedenza, il Tribunale ha solo aggiunto che "la delega è stata conferita in termini ragionevolmente ampi per consentire un adeguamento al Regolamento 679/2016 dell'Unione europea dell'intero quadro normativo nazionale e in particolare del sistema sanzionatorio con la previsione di sanzioni penali, civili e amministrative efficaci, dissuasive e proporzionate alla gravità delle violazioni. Dunque, non appare censurabile per eccesso di delega l'art. 18, che prevede, con finalità deflattiva, la possibilità per il contravventore di definire le infrazioni pregresse in modo particolarmente vantaggioso economicamente e comunque con

la piena salvaguardia del diritto di difesa, con il solo onere di inviare una nuova memoria difensiva".

Sulla base delle stesse argomentazioni il Tribunale ha ritenuto poi inammissibili le doglianze di merito prospettate dall'istituto con specifico riferimento all'ordinanza-ingiunzione ex art. 18, d.lgs. n. 101/2018; non essendo stata pagata la sanzione in misura ridotta, né presentate le memorie, il verbale di contestazione ha assunto infatti "il valore dell'ordinanza-ingiunzione" di cui all'art. 18, l. n. 689/1981, senza obbligo di ulteriore notificazione.

In linea con la decisione testé sintetizzata, lo stesso Tribunale di Bologna, con sentenza del 9 giugno 2020, n. 862, ha rigettato il ricorso presentato da una società avverso altra cartella di pagamento. Nella fattispecie, il Tribunale si è pronunciato in via preliminare sull'applicabilità alla vicenda in esame dell'art. 18, d.lgs. n. 101/2018 e sull'intervenuta prescrizione del diritto a riscuotere del Garante. Il Tribunale ha poi escluso la fondatezza della doglianza avanzata dalla ricorrente in ordine alla presunta violazione del diritto di difesa, ritenendo che l'art. 18, d.lgs. n. 101/2018 non si pone in contrasto con il RGPD. Per le medesime ragioni illustrate con sentenza n. 683/2020, il Tribunale non ha poi accolto le doglianze della società relative alla lamentata omessa notificazione dell'ordinanza-ingiunzione e alla mancanza del titolo esecutivo.

Argomentazioni similari sono state esposte dal Tribunale di Milano, con sentenza del 10 dicembre 2020, che ha dichiarato inammissibile il ricorso presentato da un comune avverso una cartella di pagamento, non ritenendo, preliminarmente, ravvisabile nel meccanismo previsto dall'art. 18, d.lgs. n. 101/2018, la violazione dei principi di cui agli artt. 18, l. n. 689/1981 e 3, l. n. 21/1990, essendo pienamente garantiti il contraddittorio e l'obbligo di motivazione da parte del Garante. Anche la questione di costituzionalità dell'art. 18, d.lgs. n. 101/2018 non è stata ritenuta configurabile in relazione all'eccesso di delega ai sensi dell'art. 13, l. n. 163/2017.

Infine, tenuto conto della data del deposito del ricorso, il giudice lo ha considerato tardivo e, dunque, inammissibile, poiché il Garante è esentato, ai sensi del citato art. 18, dall'onere di provvedere alla notifica del provvedimento, che assume il valore di ordinanza-ingiunzione decorso il termine di cui al comma 1 della medesima norma (novanta giorni dalla data di entrata in vigore del decreto legislativo).

Sulla stessa linea, il Tribunale di Verona ha respinto un ricorso proposto da un centro diagnostico specialistico ritenendo infondata la contestazione circa l'illegittimità del procedimento amministrativo sanzionatorio conclusosi senza l'adozione di un provvedimento formale, in quanto ha ritenuto applicabile nel caso *de quo* l'art. 18, d.lgs. n. 101/2018, poiché la società ricorrente non ha provveduto al pagamento della sanzione comminata nel verbale di accertamento, né nella misura ridotta né per l'intero, e non ha presentato una nuova memoria difensiva, non potendosi considerare tale quella presentata dalla ricorrente prima dell'entrata in vigore della suddetta norma (15 ottobre 2020, n. 1588).

Di diverso orientamento, la decisione del Tribunale di Verbania che, in un ricorso avverso una cartella esattoriale proposto da una società, ha ritenuto che la trasformazione del verbale di contestazione in ordinanza-ingiunzione prevista dall'art. 18, d.lgs. n. 101/2018, avrebbe potuto essere evitata, oltre che con il pagamento della sanzione in misura ridotta, con la produzione di nuove memorie, intendendosi per tali anche quelle depositate tempestivamente (rispetto alla notifica del verbale di contestazione) nel procedimento sanzionatorio, come avvenuto nel caso di specie. Pertanto, il ricorso è stato accolto e la cartella annullata per inesistenza di un'ordinanza-ingiunzione su cui fondare il ruolo esecutivo (9 settembre 2020, n. 385).

In altra sentenza, il Tribunale di Cremona, nel giudizio proposto da un comune

avverso una cartella esattoriale, ha ritenuto che la mancata determinazione dell'importo dovuto a titolo di sanzione nell'atto di contestazione (nel caso di specie contenente solo il minimo e il massimo previsti per la violazione rilevata) rende necessaria l'adozione da parte del Garante di un provvedimento di ordinanza-ingiunzione per quantificare l'importo stesso al fine di definire il procedimento ai sensi dell'art 16, l. n. 689/1981, come indicato nelle FAQ relative all'interpretazione ed applicazione dello speciale procedimento introdotto dal d.lgs. n. 101/2018 pubblicate nel sito dell'Autorità.

Secondo il giudice, la quantificazione e l'irrogazione rimessi ad un successivo atto mai notificato hanno lasciato il ricorrente privo della possibilità di esercitare compiutamente il diritto di difesa e di tutela giurisdizionale contro gli atti della p.a. garantiti dagli artt. 24 e 113 Cost.; con ciò gravemente inficiando l'intero procedimento sanzionatorio e per l'effetto privando la cartella esattoriale impugnata di un legittimo fondamento giuridico.

In tal senso, la cartella risulta in concreto essere il primo atto idoneo a porre il soggetto in grado di esercitare validamente il proprio diritto di difesa e pertanto, in considerazione delle motivazioni suesposte, il ricorso è stato accolto disponendo la nullità della cartella esattoriale (8 settembre 2020, n. 366).

Altra decisione ha accolto il ricorso proposto da una società avverso la cartella esattoriale emessa per omessa informativa in quanto la condotta prevista nell'art. 161, d.lgs. n. 196/2003 e contestata con avviso di accertamento effettuato nell'anno 2014 non è più sanzionata in via amministrativa, essendo stato tale articolo di legge abrogato dal successivo d.lgs. n. 101/2018 e spiegando la suddetta abrogazione effetti retroattivi. Avverso tale decisione pende giudizio in Cassazione (Trib. Macerata, 18 novembre 2020, n. 15).

Cumulo materiale delle sanzioni

Con sentenza 3 settembre 2020, n. 18288, la Corte di cassazione è intervenuta sulla questione del cumulo delle sanzioni con riferimento al regime sanzionatorio antecedente a quello introdotto con il RGPD. In particolare, la Cassazione, in riforma della sentenza di primo grado e confermando il provvedimento del 5 dicembre 2013, n. 549 (doc. web n. 2954335), ha stabilito che la fattispecie prevista dall'art. 164-*bis*, comma 2, del Codice costituisce non un'ipotesi aggravata rispetto alle violazioni semplici ivi richiamate, ma una figura di illecito del tutto autonoma, atteso che essa prevede la possibilità che vengano infrante dal contravventore, anche con più azioni e in tempi diversi, una pluralità di ipotesi semplici, unitariamente considerate dalla norma con riferimento a "banche di dati di particolare rilevanza o dimensioni", sicché, in caso di concorso di violazioni di altre disposizioni unitamente a quella in esame, ne deriva un'ipotesi di cumulo materiale delle sanzioni amministrative. Tale orientamento era stato già espresso dalla Cassazione nella sentenza n. 17143/2016.

Misure di sicurezza e medici di base

Alcune sentenze hanno avuto ad oggetto ordinanze-ingiunzioni emesse nei confronti dei medici di base per la violazione delle misure di sicurezza indicate nell'art. 33 del Codice, avendo i sanitari interessati consentito al collega medico in sostituzione di accedere al sistema informatico (denominato TS-progetto tessera sanitaria, attraverso l'applicativo FPF), fornendo allo stesso *user id* e *password* di accesso e consentendo così il rilascio di certificati medici telematici con credenziali non proprie.

Nei casi in esame i giudici hanno rilevato che il medico, "assumendo la veste giuridica di titolare ai sensi dell'art. 4, comma 1, lett. *f*), del Codice […] avrebbe dovuto fornire al medico sostituto diverse credenziali di accesso applicativo", dovendosi attenere al disciplinare tecnico contenuto nell'allegato B) del Codice, in base al quale "ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione […] 6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi" (Trib. Roma,

Trasparenza amministrativa

15 gennaio 2019, n. 24202; 7 gennaio 2020, n. 279 e n. 300; 15 gennaio 2020, n. 34346; 22 gennaio 2020, n. 445 e 12 marzo 2020, n. 3798 che hanno confermato, rispettivamente, le ordinanze-ingiunzioni 16 maggio 2018, n. 302; 3 maggio 2018, n. 263; 22 maggio 2018, nn. 332, 333, 336 e 343).

Tre pronunce hanno riguardato la pubblicazione di dati nei siti web di amministrazioni pubbliche.

In un primo caso, il Tribunale di Parma, nel giudizio di rinvio dopo la cassazione della sentenza di primo grado (Cass. 7 agosto 2019, n. 21148, pronunciatasi in relazione a Trib. Parma, 22 dicembre 2017, n. 1651), ha accolto il ricorso di un comune avverso il provvedimento del 25 giugno 2015, n. 382 (doc. web n. 4242968), ravvisando la base normativa della pubblicazione nel sito web dello stesso di dati personali riferiti ai candidati non ammessi ad un concorso, al fine di assicurare la trasparenza ed efficienza della procedura di reclutamento, nell'art. 19, d.lgs. n. 165/2001, ritenendo rispettato il principio di proporzionalità in ragione del contenuto delle informazioni pubblicate (24 giugno 2020, n. 575). Avverso la decisione è stato presentato ricorso alla Corte di cassazione.

In altro caso, la Corte di cassazione, confermando la sentenza del Tribunale di Sciacca del 6 giugno 2016, n. 308, di rigetto del ricorso proposto da un comune che aveva mantenuto visibili sul proprio albo pretorio *online* per oltre un anno, e quindi oltre il termine di legge di quindici giorni, determinazioni dirigenziali contenenti dati personali di una dipendente, ha statuito che, a fronte del fatto che il comune si fosse avvalso dell'opera di un consulente esterno per configurare il sito internet in conformità alla normativa vigente, il titolare del trattamento è la persona giuridica, non il legale rappresentante o l'amministratore, e che il Codice deroga al principio della imputabilità personale della sanzione di cui alla legge n. 689/1981, configurando nello specifico regime sanzionatorio ivi dettato un'autonoma responsabilità della persona giuridica.

Tale responsabilità non può ritenersi oggettiva ma, analogamente a quanto previsto dal d.lgs. n. 231/2000 in tema di responsabilità da reato degli enti, va configurata come "colpa di organizzazione", da intendersi, in senso normativo, come rimprovero derivante dall'inottemperanza da parte dell'ente dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenire la commissione degli illeciti (cfr. sez. un. penali n. 38343/2014). È stato confermato, pertanto, il provvedimento del 26 marzo 2015, n. 193 (doc. web n. 4000337).

In altro caso, il Tribunale di Vallo della Lucania ha confermato l'ordinanza-ingiunzione 19 febbraio 2015, n. 101 (doc. web n. 3986654) con cui il Garante ha sanzionato un comune per aver posto in essere un illecito trattamento di dati personali attraverso la pubblicazione, sul sito web istituzionale, di ordinanze sindacali con le quali venivano disposti trattamenti sanitari obbligatori, con l'indicazione dell'identità degli interessati e dei motivi dei ricoveri. Il Tribunale ha precisato che, nel caso in cui il trattamento dei dati personali venga effettuato da una persona giuridica, la titolarità si innesta in capo alla medesima nel suo complesso e non alla persona fisica cui materialmente sia demandato, quale organo della persona giuridica, lo svolgimento di una determinata attività; titolare del trattamento è, dunque, la persona giuridica.

Informativa e consenso

Una pronuncia ha confermato la sanzione comminata ad una società con il provvedimento del 9 novembre 2017, n. 464 (doc. web n. 7830163) per aver omesso di rendere l'informativa tramite il proprio sito internet, ritenendo che la circostanza addotta dalla ricorrente, secondo cui il titolare del trattamento si fosse avvalso di terzi non investiti dell'incarico di responsabili nello svolgere le attività che implicano raccolta di dati personali, non esime il titolare da responsabilità per l'eventuale inade-

guatezza dell'opera dagli stessi prestata. È stata invece annullata la sanzione irrogata alla medesima società per avere conservato le immagini riprese dal proprio impianto di videosorveglianza per un periodo superiore di dieci giorni a quello consentito, poiché il provvedimento generale 8 aprile 2010 emesso dal Garante in materia di videosorveglianza, avendo portata generale e astratta ed essendo finalizzato a dettare le linee guida applicabili alla materia in esame, non appare presidiato dalla sanzione di cui all'art. 162, comma 2-*ter*, applicata a carico dell'istante (Trib. Napoli, sez. dist. di Ischia, 30 novembre 2020, n. 158).

In materia di consenso, in sede di riassunzione ex art. 392 c.p.c. è stato rigettato il ricorso in opposizione avverso l'ordinanza-ingiunzione 20 giugno 2013, n. 304 (doc. web n. 2629849) per la violazione degli artt. 23 e 24 del Codice da parte di una società che aveva omesso di documentare la richiesta di consenso al trattamento dei dati personali sensibili dei clienti delle sue strutture termali.

Per quanto riguarda il rito, alla luce dell'ordinanza della Corte di cassazione n. 25671/2018, il giudice ha considerato che, ai fini dell'esame del ricorso in opposizione a ordinanza-ingiunzione e dell'eventuale rigetto dello stesso, non è necessaria la produzione in giudizio del verbale di contestazione ad opera dell'amministrazione opposta, pur sempre gravata degli oneri probatori dell'attore sostanziale, essendo compito del giudice valutare la fondatezza della sanzione irrogata alla luce della restante documentazione in atti e, in particolare, del verbale delle operazioni di accertamento in base al quale è stata poi formulata la contestazione. Nella specie, dagli atti non risultava la documentazione relativa all'acquisizione del consenso, essendo insufficiente l'informativa con la quale si comunicava la necessità del conferimento dei dati per poter eseguire correttamente la prestazione e la circostanza che il loro mancato conferimento avrebbe potuto comportare la mancata erogazione del servizio.

Il Tribunale di Roma, nel confermare le ordinanze-ingiunzioni del Garante del 26 luglio 2018, nn. 442 e 443 (docc. web nn. 9052099 e 9054309) emesse nei confronti di una società per l'invio di comunicazioni promozionali alla casella Pec di diversi professionisti in assenza di specifico consenso degli stessi, ha ritenuto ormai preclusa la valutazione dell'illegittimità della contestazione, essendo spirato il termine per impugnare l'atto presupposto, accogliendo quindi le sole doglianze relative ai vizi formali delle impugnate ordinanze di applicazione delle sanzioni amministrative. Nel merito, si è ribadito che l'agevole reperibilità degli indirizzi Pec utilizzati non giustifica il loro trattamento per qualsiasi scopo ma solo per le finalità che ne hanno determinato la pubblicazione; in proposito, si è affermato che la libera consultabilità in via telematica degli indirizzi Pec non implica la legittimità della diversa attività di estrazione degli stessi, consentita alle sole p.a. per le comunicazioni relative agli adempimenti di loro competenza. Tale utilizzo, disciplinato dall'ordinamento, rischia di essere pregiudicato dall'invio di comunicazioni promozionali che esulano dalle finalità per le quali sono resi disponibili gli indirizzi Pec, ponendosi in violazione dei principi di correttezza e liceità delle operazioni di trattamento, come è avvenuto nel caso di specie con l'estrazione massiva di indirizzi Pec per l'invio di comunicazioni con finalità promozionale (18 dicembre 2019, n. 24555).

In una pronuncia, confermando il provvedimento dell'11 aprile 2019, n. 95 (doc. web n. 9116053), avente ad oggetto i trattamenti di dati personali effettuati da una società nell'ambito della sua attività di *marketing/teleselling* svolta tramite *call center* per conto di più committenti, il Tribunale di Vibo Valentia ha evidenziato l'importanza di rendere un'idonea informativa e di ottenere il consenso al trattamento da parte degli interessati che non può ritenersi soddisfatto dalla compilazione manuale dell'operatore sulla scorta delle dichiarazioni verbali rese, ma deve risultare

20

Controllo a distanza dei lavoratori

su supporto materiale che consenta di acclarare che effettivamente esso è stato reso; l'assenza della registrazione, che in teoria avrebbe permesso di accertare quantomeno il consenso verbale, impedisce tale accertamento (5 marzo 2020, n. 172).

In due casi il Tribunale di Sondrio ha accolto, con motivazioni pressoché identiche, i ricorsi con i quali due società hanno impugnato, rispettivamente, le sanzioni loro comminate dal Garante con i provvedimenti 21 giugno 2018, n. 393 e 14 giugno 2018, n. 386 (docc. web nn. 9039215 e 9038679) per omessa notificazione ai sensi dell'art. 37, comma 1, lett. *a*), d.lgs. n. 196/2003 in riferimento ad un sistema di geolocalizzazione installato a bordo dei mezzi. Il Tribunale, con le decisioni di cui si tratta, ha ritenuto che le ricorrenti non fossero titolari del trattamento, in quanto il sistema di geolocalizzazione a bordo dei propri mezzi, che avrebbe imposto l'obbligo di notifica, era in capo ad una terza società, che in realtà lo avrebbe fornito ed istallato, ritenendo assorbite dall'accoglimento nel merito tutte le altre questioni sollevate dall'Autorità (sentenze 2 novembre 2020).

Profilazione

Un caso ha avuto ad oggetto la violazione delle disposizioni degli artt. 13, 20 e 37 del Codice da parte di un istituto previdenziale per aver fatto uso di un *software* che attribuisce in modo automatico un punteggio convenzionale ai certificati medici prodotti dai lavoratori al fine di indirizzare in modo mirato e più efficiente il sistema dei controlli medico-legali. A fronte dell'avvio di una interlocuzione da parte del Garante e delle contestazioni da questi elevate, l'ente ha sospeso l'utilizzo del sistema; pur non essendo stato emesso alcun provvedimento prescrittivo o inibitorio, si è dato corso al procedimento sanzionatorio.

Le condotte sanzionate dal Garante si riferiscono al sistema normativo previgente all'entrata in vigore del d.lgs. n. 101/2018 e si sono sostanziate nell'avere effettuato un trattamento dei dati sensibili senza aver fornito idonea informativa; nell'aver effettuato un trattamento illecito di dati personali, anche idonei a rivelare lo stato di salute in mancanza dei necessari presupposti e nell'aver effettuato attività di profilazione con i dati personali dei lavoratori, anche idonei a rivelare lo stato di salute, senza notificare preventivamente tale trattamento all'Autorità.

Nel confermare il provvedimento ingiuntivo del 29 novembre 2018, n. 492 (doc. web n. 9078812), il Tribunale, in riferimento alla questione della titolarità del trattamento, ha richiamato l'indirizzo manifestato dalle Sezioni Unite della Cassazione (22 settembre 2017, n. 22082).

Riguardo all'eccezione di prescrizione dell'illecito di cui all'art. 37, in linea con la giurisprudenza in tema di sanzioni amministrative, ha ribadito che la permanenza dell'illecito omissivo è configurabile con riferimento a quelle condotte che l'autore avrebbe potuto porre in essere utilmente anche dopo la prima omissione (v. Cass. civ., Sez. II, 31 maggio 2019, n. 15025), situazione che certamente si attaglia al caso di specie.

Circa poi il riferimento all'attività di controllo demandata all'istituto previdenziale, il medesimo Tribunale ha evidenziato come nel caso considerato non rilevasse l'attività di controllo medico-legale, quanto la valutazione della specifica operazione di raccolta di dati, prodromica al controllo ed indubbiamente funzionale ad una sua maggiore efficienza, ma non dovuta per legge né necessitata, sì da doversi escludere la ricorrenza dell'esimente di cui all'art. 24 del Codice.

È stata altresì ritenuta non condivisibile l'argomentazione dell'ente previdenziale secondo cui il trattamento della sola frequenza e durata delle malattie (priva delle relative diagnosi) non determinerebbe un trattamento dei dati riferiti allo stato di salute degli interessati.

Altrettanto ha stabilito in relazione all'asserita assenza di attività idonea a profilare l'utenza oggetto di detto trattamento, rimandando sul punto alla definizione

di profilazione contenuta nel RGPD. Nel caso di specie si è con ogni evidenza di fronte ad una raccolta di dati idonei a definire un profilo dell'interessato, trattati con strumenti elettronici, attraverso una procedura funzionale ma non indispensabile alla realizzazione degli scopi dell'Ente.

Infine, per quanto concerne l'asserito mancato accesso alla definizione agevolata di cui all'art. 18, d.lgs. n. 101/2018, è stato sottolineato che tale agevolazione ha ad oggetto i procedimenti sanzionatori pendenti alla data di applicazione del RGPD (non ricorrente nel caso di specie). Sulla vicenda pende ricorso in Cassazione.

In un'altra pronuncia, che ha confermato l'ordinanza-ingiunzione del 22 febbraio 2018, n. 106 (doc. web n. 8995033) nei confronti di una società che aveva installato un sistema biometrico basato sulla rilevazione delle impronte digitali per la registrazione della presenza dei dipendenti, omettendo l'assolvimento sia dell'obbligo di presentazione di apposita istanza di verifica preliminare per il trattamento dei dati biometrici, sia dell'obbligo di notificazione al Garante, il Tribunale di Biella, con sentenza del 3 marzo 2020, n. 4, ritenuto irrilevante qualsivoglia rapporto negoziale interno tra la società e l'impresa venditrice del dispositivo, ha precisato che la responsabilità dell'autore dell'infrazione non è esclusa dal mero stato di ignoranza sul precetto normativo o sulla sanzione, occorrendo che "tale stato sia incolpevole, cioè non superabile dall'interessato con l'uso dell'ordinaria diligenza" (Cass. civ., Sez. II, 28 febbraio 2019, n. 6018). Escludendo la scusabilità dell'errore sul fatto dedotto dalla società, il Tribunale ha ritenuto l'osservanza degli obblighi in questione condotta esigibile da parte della società anche in ragione della posizione di garanzia ricoperta dal datore di lavoro quale titolare del trattamento dei dati personali dei propri dipendenti, *a fortiori*, in considerazione della "professionalità qualificata" dello stesso.

Nel confermare l'ordinanza-ingiunzione del 13 gennaio 2011, n. 9 (doc. web n. 1893533), il Tribunale di Torre Annunziata, con sentenza 20 febbraio 2020, n. 424, ha ritenuto ammissibile la domanda di querela di falso incidentale all'interno del giudizio di opposizione ad ordinanza-ingiunzione, "avendo il querelante impugnato il verbale di accertamento perché ritenuto privo della descrizione di fatti rilevanti ai fini della emanazione dell'ordinanza-ingiunzione opposta" (Cass. civ., 3705/2013; v. anche Cass. civ., Sez. un., n. 17355/2009), rigettandola poi nel merito tenuto conto che "le prove offerte non consentivano di ritenere raggiunta la prova di quanto sostenuto dal querelante".

Ulteriori casi

Con sentenza del 14 febbraio 2020, n. 237, il Tribunale di Perugia ha ridotto la sanzione comminata ad una società con l'ordinanza del 19 luglio 2018, n. 428 (doc. web n. 9047331) per la violazione delle disposizioni di cui all'art. 32, comma 1, del Codice (sanzionata dall'art. 162-*bis*), avendo la stessa conservato dati di traffico telefonico e telematico trattati per finalità di accertamento e repressione dei reati per un periodo superiore a ventiquattro mesi (traffico telefonico) e dodici mesi (traffico telematico); nonché per la violazione delle disposizioni di cui all'art. 17 del Codice (sanzionata dall'art. 162, comma 2-*bis*) per aver conservato dati di traffico telematico senza aver adottato le misure prescritte nel provvedimento del 17 gennaio 2008 in materia di sicurezza dei dati.

Richiamando il parere n. 4/2007 del 20 giugno 2007 del Gruppo Art. 29, la decisione evidenzia (tra l'altro) che i cartellini di traffico telematico conservati dalla società contengono necessariamente le informazioni relative all'indirizzo Ip e Mac del cliente e dunque sono idonei ad identificarlo, unitamente al dispositivo dal quale è stata effettuata la connessione.

Nel sottolineare che, diversamente da quanto addotto dalla società, il mancato funzionamento di uno *script* non poteva giustificare l'omessa cancellazione e che

20

non erano stati predisposti i controlli di *routine* necessari per evitare il malfunzionamento, il Tribunale ha rimarcato il dovere di diligenza cui era tenuto l'operatore in virtù dell'attività esercitata. Quanto alla condotta, il Tribunale ha chiarito che il bene tutelato dalle norme in questione non necessariamente richiede l'utilizzo illecito dei dati ma, al contrario, deve ritenersi leso dalla mera detenzione e conservazione degli stessi in violazione delle norme del Codice. Infine, il Tribunale ha provveduto ad una riduzione della sanzione poiché, ancor prima della notifica dei verbali di infrazione e dell'apertura del procedimento innanzi all'Autorità, la società aveva recepito tutte le indicazioni e raccomandazioni formulate dalla Guardia di finanza in sede ispettiva, conformando tempestivamente i processi aziendali in materia di *privacy* alle disposizioni normative e regolamentari.

Con sentenza del 13 novembre 2019, il Tribunale di Roma ha rigettato l'eccezione del ricorrente relativa alla nullità della notifica dell'ordinanza-ingiunzione del 5 aprile 2018, n. 202 (doc. web n. 9008692) comminata ad un'azienda ospedaliera per non aver designato ai sensi dell'art. 30 del Codice gli incaricati del trattamento dei dati sanitari, omettendo così di adottare le misure minime di sicurezza di cui agli artt. 33 e ss. e alle regole nn. 1-10, 12-74, 15 e 27-29 del disciplinare tecnico di cui all'all. B) del medesimo Codice.

Nel caso di specie, la relata di notifica dell'ordinanza-ingiunzione allegata alla Pec non era stata sottoscritta con firma digitale dal dirigente preposto (trattandosi invero di un documento analogico su cui è stata apposta una firma autografa, poi scansionato). Il Giudice ha tuttavia osservato che la parte ricorrente non aveva lamentato né uno specifico pregiudizio al suo diritto di difesa, né l'eventuale difformità tra la copia informatica per immagine dell'ordinanza-ingiunzione notificata a mezzo Pec e quella cartacea originale, di cui peraltro era stata depositata copia autentica con la comparsa di costituzione dell'autorità resistente; inoltre, ha affermato che la notificazione dell'ordinanza-ingiunzione non è un requisito dell'atto, ma assolve solo alla funzione di far decorrere il termine per l'opposizione giudiziale, di talché la mancanza della notifica, o la sua eventuale invalidità, non inficia la validità e l'efficacia dell'atto che essa è destinata a portare a conoscenza del contravventore, ma, semplicemente, impedisce il decorso del termine di decadenza per l'opposizione. Ne consegue che, ove il contravventore – venuto a conoscenza dell'ordinanza-ingiunzione, come nel caso in esame – intenda impugnarla davanti al giudice, non è ravvisabile un suo interesse a censurare la mancanza o l'invalidità della relativa notifica. È stata tuttavia accolta l'ulteriore doglianza del mancato rispetto del termine per la contestazione della violazione, di cui all'art. 14, l. n. 689/1981. È pendente ricorso alla Corte di cassazione.

In un'altra vicenda, il Tribunale di Lecce, annullando l'ordinanza-ingiunzione 19 luglio 2018, n. 430 (doc. web n. 9039443) con cui il Garante aveva sanzionato una società per il mancato riscontro alle richieste di informazioni formulate dal segretario generale ai sensi dell'art. 157 del Codice, ha ritenuto che l'Autorità non aveva comprovato l'avvenuta notifica a mezzo Pec alla ricorrente della contestazione della violazione prodromica alla pronuncia dell'ordinanza-ingiunzione opposta. In particolare, il Tribunale ha precisato che "in giudizio sono state depositate telematicamente non le ricevute di accettazione e consegna della notifica effettuata tramite Pec in formato *.email* o *.msg* (che un *editor* di posta elettronica avrebbe consentito di aprire e verificare cosa, quando e a chi fosse stata effettuata la notifica, atteso che la ricevuta di consegna completa contiene i medesimi *files* che il destinatario della notifica ha ricevuto tramite Pec dal mittente), ma semplici scansioni di documenti (neppure attestati conformi ai relativi originali digitali) […], inidonei a comprovare l'effettiva ricezione della Pec da parte della destinataria ed il relativo contenuto" (13 gennaio 2020, n. 53).

Complessivamente l'Autorità ha avuto notizia di 12 decisioni relative a opposizioni a propri provvedimenti, costituendosi nei relativi giudizi tramite l'Avvocatura dello Stato territorialmente competente.

Il Tribunale di Milano, 21 settembre 2020, n. 4597, ha accolto il ricorso proposto dal gestore di un motore di ricerca generalista ritenendo non sussistente il diritto del ricorrente, in capo al quale era già stato riconosciuto il diritto di ottenere l'estensione dell'ordine di deindicizzazione con riferimento a notizie non veritiere né attuali sul proprio conto da parte della società anche in relazione ai risultati della ricerca visualizzati al di fuori dei confini dell'Unione europea, e annullando il provvedimento del 26 ottobre 2017, n. 445 (doc. web n. 7323489). Il Giudice ha preso le mosse dalla sentenza 24 settembre 2019 – causa C 507/17 della CGUE – che, a fronte di Stati terzi che non tutelano o disciplinano diversamente il diritto alla deindicizzazione ed in assenza di espresse convenzioni tra gli Stati in tal senso, non ha ritenuto sussistente un potere dell'autorità di controllo di imporre il rispetto della normativa in materia dei dati personali al di fuori dei confini europei. Nella fattispecie in esame, l'organo giudicante ha ritenuto che il Garante abbia applicato una norma di derivazione europea al di fuori del perimetro riconosciuto dalla decisione della CGUE.

In altra pronuncia la Suprema Corte, confermando il provvedimento del 18 ottobre 2012, n. 296 (doc. web n. 2174351), annullato in primo grado, ha affermato che l'art. 10, comma 2, d.lgs. n. 150/2011, quando richiama la "residenza" del titolare ai fini della competenza territoriale per le controversie in materia di protezione dei dati personali, si riferisce, in modo diretto e giuridicamente proprio, alla sola persona fisica e, pertanto, se il titolare del trattamento è una persona giuridica o una p.a., è necessario avere riguardo al foro generale delle persone giuridiche, pubbliche e private, previsto dall'art. 19 c.p.c. Pertanto, salvo che la legge disponga altrimenti, qualora sia convenuta una persona giuridica, è competente il giudice del luogo dove essa ha sede, nonché il giudice del luogo in cui essa ha uno stabilimento e un rappresentante autorizzato a stare in giudizio per l'oggetto della domanda, tenuto conto che i terzi possono considerare come sede della persona giuridica, se diversa dalla sede risultante dal registro, anche quella "effettiva" (artt. 16 e 46 c.c.) ovvero "il luogo in cui hanno concreto svolgimento le attività amministrative e di direzione dell'ente ed ove operano i suoi organi amministrativi o i suoi dipendenti, ossia il luogo deputato o stabilmente utilizzato per l'accentramento dei rapporti interni e con i terzi in vista del compimento degli affari e della propulsione dell'attività dell'ente". Deve quindi ritenersi che il luogo ove risiede il titolare del trattamento alluda a una nozione collegata ad una localizzazione "dinamica" e non "statica" del titolare, espressa quindi dal suo agire rilevante secondo il Codice, identificandosi il luogo di residenza del titolare del trattamento nel luogo in cui il trattamento avviene in modo autonomo e quindi si manifesta in concreto (v. art. 79, par. 2 e cons. 22 del RGPD). La Suprema Corte si è soffermata anche sull'illecito trattamento di dati personali, riconducibile ad un'ipotesi di responsabilità oggettiva, anche alla luce dell'esplicito rinvio compiuto dalla legge all'art. 2050 c.c. (art. 15, d.lgs. n. 196/2003, applicabile pro tempore). Pertanto, il danneggiato che lamenti la lesione dell'interesse non patrimoniale può limitarsi a dimostrare l'esistenza del danno e del nesso di causalità rispetto al trattamento illecito (non essendo *in re ipsa*) anche tramite presunzioni semplici, mentre spetta al danneggiante, titolare del trattamento, eventualmente in solido col responsabile, dimostrare di aver adottato tutte le misure idonee per evitare il danno.

Questo schema è parzialmente confermato anche nel RGPD (art. 82, par. 3) che, sulla base del principio di responsabilizzazione (*accountability*), addossa al titolare

20

del trattamento – eventualmente in solido con il responsabile – il rischio tipico di impresa (2050 c.c.). In particolare, il titolare del trattamento, per non incorrere in responsabilità, deve dimostrare che l'evento dannoso non gli è in alcun modo imputabile e non può limitarsi alla prova negativa di non aver violato le norme (e quindi di essersi conformato ai precetti), occorrendo la prova positiva di aver valutato autonomamente il rischio di impresa, purché tipico, cioè prevedibile, e deve avere attuato le misure organizzative e di sicurezza tali da eliminare o ridurre il rischio connesso alla sua attività (17 settembre 2020, n. 19328).

In tema di competenza giurisdizionale sulle controversie riguardanti l'applicazione della normativa in materia di protezione dei dati personali, il Consiglio di Stato, con sentenza 22 giugno 2020, n. 3980, ha respinto l'appello proposto da un'associazione avverso la sentenza del TAR Lazio, 14 gennaio 2020, n. 382. Con tale pronuncia, il TAR aveva dichiarato il difetto di giurisdizione amministrativa nella causa concernente l'impugnazione da parte dell'associazione medesima di un codice di condotta approvato con provvedimento del 12 settembre 2019 (doc. web n. 9141941), ritenendo che, anche a seguito della modifica dell'art. 152, comma 1, del Codice, operata dal d.lgs. n. 101/2018, trattandosi nel caso di specie di impugnazione di un provvedimento adottato dal Garante, sussiste la giurisdizione esclusiva del giudice ordinario, indipendentemente dalla posizione soggettiva dedotta in giudizio, di interesse legittimo piuttosto che di diritto soggettivo, coerentemente con la considerazione che, in materia di accesso ai dati personali e di protezione degli stessi vi è una inestricabile interferenza tra diritti soggettivi e interessi legittimi, con netta prevalenza, peraltro, dei primi rispetto ai secondi, condividendo sul punto l'orientamento della Corte di cassazione (sez. un., 14 aprile 2011, n. 8487).

La Corte di cassazione, in altra decisione, si è pronunciata sul ricorso proposto da un dipendente di un'azienda ospedaliera che ha impugnato la sentenza emessa dal Tribunale di Roma il 7 ottobre 2014, n. 7822 (cfr. Relazione 2015, p. 145), di rigetto del ricorso avverso il provvedimento in materia di trattamento dati sullo stato di salute, consistente in una comunicazione di carattere interno di dati sanitari riferiti al ricorrente (provv. 23 dicembre 2010, doc. web n. 1800931). Tutti i motivi di ricorso prospettati sono stati ritenuti esorbitanti dal giudizio di legittimità e sono stati dichiarati, pertanto, inammissibili (31 luglio 2020, n. 16560).

Il Tribunale di Perugia ha rigettato il ricorso avverso il provvedimento con il quale il procedimento era stato definito (nota 21 febbraio 2019) ritenendo che la banca nei confronti della quale il reclamo era stato presentato detenesse correttamente l'utenza telefonica fornita dall'interessato all'atto dell'apertura del conto corrente e divenuta successivamente ad uso esclusivo della coniuge del titolare dello stesso. Ciò sull'assunto che fosse onere di quest'ultimo comunicare alla banca una nuova utenza personale sulla quale poter essere contattato, non potendo la banca essere tenuta a conoscere il successivo cambio di intestazione in assenza di una formale comunicazione in tal senso. Il Tribunale ha altresì ritenuto di non poter dare seguito alle richieste di aggiornamento dei dati personali provenienti da soggetto diverso dal titolare del rapporto ai sensi dell'art. 16 del RGPD e che la banca non avesse alcun obbligo di cancellazione dell'utenza telefonica fornita dall'interessato, in quanto necessaria per rintracciarlo in presenza di uno scoperto di conto corrente, poiché il "diritto alla cancellazione" può essere ottenuto solo se i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati, ai sensi dell'art. 17 del RGPD (Trib. Perugia, 3 giugno 2020, n. 645).

In un altro caso è stato proposto ricorso avverso il provvedimento di non luogo a provvedere del Garante del 29 aprile 2019 che ha ritenuto di non poter accertare le violazioni della reclamante in materia di trattamento dei dati sensibili da parte

del datore di lavoro del defunto marito alla luce del tempo trascorso e prendendo atto del riscontro fornito alla richiesta di accesso ai dati personali. In particolare, il Giudice, ha stabilito che la domanda di applicazione della sanzione amministrativa pecuniaria proposta dalla parte fosse inammissibile, trattandosi di materia di esclusiva competenza dell'autorità amministrativa (nella specie, del Garante) e potendo l'Autorità giudiziaria, ai sensi dell'art. 10, d.lgs. n. 150/2011, solo prescrivere le misure necessarie per la protezione dei dati personali (Trib. Milano, 22 ottobre 2020, n. 6614).

Con la sentenza del Tribunale di Treviso, 27 febbraio 2020, è stato accolto il ricorso avverso il provvedimento di archiviazione che aveva ritenuto legittimo il diniego di una banca nei confronti dell'erede a conoscere il nome del beneficiario di polizze assicurative, poiché si tratta di un dato necessario per esercitare azioni ereditarie, riconoscendo la prevalenza del diritto di difesa rispetto a quello concernente la riservatezza dei dati personali. Avverso tale decisione il Garante ha proposto ricorso in Cassazione.

Il Tar Lazio, 5 ottobre 2020, n. 10080, nel rigettare il ricorso avverso un provvedimento del Garante di accoglimento dell'accesso agli atti di un procedimento amministrativo e sanzionatorio nei confronti della ricorrente, ha riconosciuto l'interesse della società istante (controinteressata nel giudizio) all'accesso, consistente nella tutela della correttezza della dinamica concorrenziale "essendo contraria alle regole di correttezza la violazione delle regole giuridiche discendenti dal rapporto contrattuale intercorrente tra le due società per la fornitura di un servizio WLR (*Wholesale line rental*)". D'altro canto, è stata condivisa la stretta limitazione dei dati accessibili, a tutela della riservatezza di tutti i soggetti coinvolti. Il Tribunale ha anche rilevato che nel provvedimento impugnato non è stato riconosciuto l'accesso al procedimento sanzionatorio in astratto, perché tale procedimento coinvolge esclusivamente la parte interessata e ad esso sono giuridicamente estranei i terzi, bensì a quei documenti, pure emersi nel procedimento sanzionatorio, che sono risultati potenzialmente lesivi degli interessi della società istante, senza la necessità di dimostrare l'effettività della lesione, non potendosi escludere l'accesso a documenti anche solo potenzialmente lesivi, essendo l'accesso strumentale anche alla conoscenza della effettiva lesività.

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 alle Avvocature distrettuali dello Stato di essere comunque informata sullo svolgimento delle vicende processuali e di ricevere comunicazione in merito agli esiti.

Al riguardo si consideri che la notifica al Garante dei ricorsi in materia di protezione dei dati personali che non riguardano provvedimenti dell'Autorità amplia la casistica di possibile intervento, anche in relazione a questioni di legittimità costituzionale o di compatibilità europea di leggi, pure 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

20

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", quindi anche nei confronti dell'autorità pubblica.

Il nuovo 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.

Pertanto l'Autorità ha svolto approfondimenti sia sulla possibilità di istituire un'avvocatura interna, sia sull'istituzione di un elenco di avvocati del libero foro all'interno del quale scegliere a chi affidare di volta in volta il patrocinio delle controversie, in ragione dell'eventuale conflitto di interessi che dovesse presentarsi quando la controparte è un'autorità pubblica. Ciò tenendo conto dei recenti e rigorosi orientamenti del Consiglio di Stato (parere 9 aprile 2018, n. 2017) e della Corte dei conti (deliberazione 22 maggio 2018, n. 105) che impongono alle amministrazioni pubbliche di procedimentalizzare la scelta del professionista al quale affidare di volta in volta l'incarico di rappresentanza in giudizio, affinché sia garantito il rispetto dei principi di economicità, efficacia, imparzialità, parità di trattamento, trasparenza, proporzionalità e pubblicità, di cui all'art. 4 del codice dei contratti pubblici (d.lgs. n. 50/2016).

Occorre infine ribadire che, come si è sopra ricordato (cfr. par. 20.1), in base al nuovo testo del 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. 10 agosto 2018, n. 101). Tale comunicazione consente al Garante, "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".

21 Le relazioni comunitarie e internazionali

Anche l'attività internazionale del Garante, fondata sulle numerose riunioni all'estero cui l'Ufficio normalmente partecipa, ha dovuto subire rilevanti cambiamenti a causa della pandemia; dal mese di marzo, a seguito delle restrizioni imposte alle missioni internazionali per contenere la diffusione del Covid-19 e della impossibilità di svolgere le riunioni dei gruppi di cui il Garante è parte (a livello UE e internazionale), le attività si sono infatti svolte da remoto. Ciò non ha impedito la prosecuzione dei diversi tavoli di lavoro, che hanno continuato a svolgere (e anzi, non di rado incrementato) le proprie attività.

La modalità da remoto ha infatti consentito non solamente una più ampia partecipazione da parte dei delegati dei diversi Paesi, ma anche una maggiore frequenza di riunioni che ha permesso la trattazione di numerosi *dossier* con l'adozione di un numero considerevole di documenti. Non solo: l'emergenza sanitaria ha ridisegnato le agende di lavoro, posto che, accanto alle attività già programmate, molti sono stati gli interventi concernenti le misure imposte a livello globale per fronteggiare la pandemia.

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 riunisce le autorità nazionali di controllo dei singoli Stati membri, dei tre Paesi 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 svolto un'attività particolarmente intensa, sia con riferimento al consueto lavoro volto a favorire il processo di adeguamento al RGPD e a dare piena attuazione allo stesso, sia in risposta alle molte questioni emerse a seguito della pandemia.

Riunitosi sotto la presidenza di Andrea Jelinek nella sua composizione plenaria per due volte in presenza (28 gennaio e 18 febbraio), il Comitato ha proseguito da remoto i propri lavori dal mese di aprile in poi per altre 22 volte, continuando ad avvalersi dei diversi sottogruppi (suddivisi per materia), che si sono a loro volta riuniti in più di 130 incontri *online* (le notizie relative alle attività del Cepd, le linee guida e tutti i documenti, ivi compresa la numerosa corrispondenza intercorsa tra il Comitato e diversi *stakeholder*, sono rinvenibili al sito internet: https://edpb.europa.eu).

Lotta al Covid-19 e protezione dei dati

Il Comitato ha adottato in procedura scritta una prima dichiarazione (19 marzo 2020) con la quale, muovendo dalla premessa che le norme di protezione dei dati non mettono a rischio le misure volte a contenere la pandemia, ha richiamato l'attenzione sulla necessità di garantire in ogni caso la liceità dei trattamenti dei dati effettuati e sul fatto che qualunque misura anche restrittiva delle libertà adottata in un contesto eccezionale come quello in corso, debba essere proporzionata e limitata al periodo dell'emergenza. La dichiarazione si sofferma in particolare su alcune questioni relative ai trattamenti dei dati di localizzazione nonché su quelli effettuati in ambito lavorativo. Questa dichiarazione è stata solo il primo degli interventi effettuati dal Cepd riguardo all'emergenza sanitaria nel corso del 2020.

Linee guida 3/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica

Le linee guida 3/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al Covid-19, adottate il 21 aprile 2020, considerato l'imponente impegno della comunità scientifica internazionale nella ricerca di rimedi efficaci e sicuri contro il virus, attengono ad alcuni profili riguardanti il trattamento di dati relativi alla salute per fini di ricerca ai sensi dell'art. 4, n. 15), del RGPD, considerando in particolare la base giuridica del trattamento, la necessità di assicurare garanzie adeguate per tale trattamento e l'esercizio dei diritti dell'interessato. Nelle linee guida il Cepd ricorda che il RGPD prevede norme speciali per il trattamento dei dati relativi alla salute a fini di ricerca scientifica, applicabili anche nel contesto della pandemia da Covid-19, e che il legislatore nazionale di ciascuno Stato membro ha il potere di emanare norme specifiche ai sensi dell'art. 9, par. 2, lettere *i*) e *j*), del RGPD (interpretate alla luce dei principi dell'art. 5 del RGPD e della giurisprudenza della CGUE) al fine di consentire tali trattamenti. Le deroghe e le limitazioni relative alla protezione dei dati di cui agli artt. 9, par. 2, lett. *j*), e 89, par. 2, del RGPD devono pertanto applicarsi solo nella misura strettamente necessaria al perseguimento dello scopo. Occorre inoltre stabilire se debba essere effettuata una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e devono essere stabiliti periodi di conservazione proporzionati, tenendo conto della durata e dello scopo della ricerca.

Linee guida 4/2020 su geolocalizzazione e tracciamento nel contesto dell'emergenza da Covid-19

Nella plenaria del 21 aprile, il Cepd ha altresì adottato le linee guida 4/2020 sull'utilizzo della geolocalizzazione e di altri strumenti di tracciamento nel contesto dell'emergenza legata al Covid-19 volte a chiarire le condizioni e i principi da rispettare ai fini di un impiego proporzionato degli strumenti che utilizzano i dati di localizzazione e il tracciamento dei contatti, in rapporto a due ambiti specifici: a) l'utilizzo dei dati di localizzazione a supporto della risposta alla pandemia tramite la definizione di modelli della diffusione del virus, al fine di valutare l'efficacia complessiva delle misure di isolamento e quarantena; b) l'impiego del tracciamento dei contatti per informare le persone potenzialmente entrate in contatto ravvicinato con soggetti successivamente confermati positivi, allo scopo di interrompere tempestivamente la trasmissione del contagio. Le linee guida sottolineano che tanto il RGPD quanto la direttiva *e-privacy* contengono specifiche disposizioni sull'utilizzo di dati anonimi o personali a supporto delle autorità pubbliche e di altri soggetti, a livello nazionale ed europeo, nelle attività di monitoraggio e contenimento della diffusione del Covid-19. Tutte le misure adottate dagli Stati membri o dall'UE che comportino il trattamento di dati personali per il contrasto del Covid-19 devono essere conformi ai principi generali di efficacia, necessità e proporzionalità. Il Cepd ribadisce e sottolinea che l'impiego di *app* per il tracciamento dei contatti dovrebbe avvenire su base volontaria e non comportare il tracciamento degli spostamenti individuali, facendo invece perno sulle informazioni di prossimità relative agli utenti. Il Cepd ha adottato anche una guida per le *app* di tracciamento dei contatti, allegata alle linee guida vere e proprie; essa intende fornire indicazioni generali ai progettisti e agli sviluppatori delle *app* di tracciamento, sottolineando che ogni valutazione deve essere compiuta caso per caso.

I menzionati interventi del Cepd erano stati anticipati da una lettera della Presidente Jelinek, indirizzata alla Commissione europea e adottata il 14 aprile 2020, sul progetto di linee guida della Commissione in materia di *app* a supporto della lotta contro la pandemia dovuta al Covid-19 volte ad integrare la raccomandazione della Commissione sulle *app* per il tracciamento dell'8 aprile. La lettera, che accoglie con favore l'iniziativa della Commissione di sviluppare un approccio coordinato nella lotta al virus e l'approccio volontaristico prescelto, sottolinea la necessità di garantire che la messa a punto delle *app* di tracciamento avvenga nel rispetto dei principi di

protezione dati, in particolare di minimizzazione, *accountability*, valutazione di impatto e sulla base di adeguati meccanismi di *privacy by design* e *by default*, garantendo la trasparenza del codice sorgente a vantaggio della comunità scientifica.

Numerose le lettere con cui il Cepd ha risposto a diverse sollecitazioni da parte di Istituzioni e parlamentari europei sui profili di protezione dati emersi nell'ambito delle strategie per il contenimento del Covid-19. Tra queste, la risposta alla Rappresentanza USA che aveva invitato il Cepd a chiarire gli aspetti relativi ai trasferimenti di dati nell'ambito della lotta al Covid-19 (24 aprile 2020) e la risposta alle richieste di chiarimento da parte della parlamentare europea Sophie in 't Veld in ordine al trattamento dei dati di localizzazione nel contesto della lotta contro il Covid-19. Ulteriori due lettere sono state adottate, in risposta alla parlamentare europea Ďuriš Nicholsonová (24 aprile 2020 e 17 luglio 2020), rispettivamente sulle linee guida comuni per la lotta al Covid-19 e sulle *app* per la lotta al Covid-19. Sempre in risposta alle richieste di chiarimento della parlamentare europea Sophie in 't Veld, il Cepd si è espresso anche sulle misure di contrasto della pandemia, adottate in taluni Stati membri e riguardanti la raccolta dei dati di prenotazione forniti dagli avventori di esercizi pubblici, quali ristoranti, musei, cinema e teatri ai fini del tracciamento dei contatti (15 dicembre 2020).

Sempre nell'ambito delle attività del Cepd concernenti le strategie di contrasto alla pandemia, si segnala altresì l'adozione della dichiarazione del 16 giugno 2020 nella quale si invitano gli Stati membri a valutare con attenzione le misure da intraprendere in occasione della riapertura delle frontiere (raccolta di informazioni sulla salute e sugli spostamenti sul territorio attraverso questionari, somministrazione di eventuali test, utilizzo di *app* su base volontaria) e a rispettare i principi di liceità, trasparenza, finalità, minimizzazione, sicurezza. Nella stessa data è stata adottata una dichiarazione sulla interoperabilità delle *app* per il controllo dei contagi Covid-19, secondo la quale la possibilità di condivisione di dati relativi a persone cui è stata diagnosticata o riscontrata la positività al test (dati di infezione) con applicazioni interoperabili dovrebbe essere attivata solo con un'azione volontaria da parte dell'utente e che l'interoperabilità non deve essere utilizzata per estendere la raccolta di dati personali al di là del necessario. Le *app* in questione e la loro interoperabilità sono soltanto alcune delle misure temporanee a disposizione per combattere la diffusione del virus la cui efficacia e proporzionalità devono essere comunque verificate dai titolari dei trattamenti.

Limitazioni all'esercizio dei diritti

Il Cepd è intervenuto anche a seguito della lettera di alcune Ong che avevano manifestato forti preoccupazioni riguardo al decreto ungherese contenente restrizioni all'esercizio dei diritti previsti dal RGPD ai fini del contrasto all'emergenza Covid-19 (decreto 4 maggio 2020, n. 179) che parevano non prevedere un termine per la cessazione dello stato di emergenza. La lettera di risposta alle Ong adottata il 3 giugno 2020 è accompagnata da una dichiarazione nella quale si ribadisce che il RGPD consente i trattamenti di dati nell'ambito della lotta al Covid-19 e prevede alcune limitazioni all'esercizio dei diritti di cui all'articolo 23 purché proporzionate, necessarie e nel rispetto dell'essenza dei diritti fondamentali; sottolinea che le restrizioni imposte in uno stato di emergenza per una durata non precisamente limitata, che si applichino retroattivamente o siano soggette a condizioni indefinite, non rispettano il criterio della prevedibilità della legge e che qualunque tipo di sospensione generale dei diritti (ad es. applicabile a trattamenti indipendentemente dalla loro finalità e senza limiti di tempo) non sarebbe compatibile con la salvaguardia dell'essenza degli stessi. Le questioni relative all'applicazione dell'articolo 23 sono state poi oggetto di un maggiore approfondimento da parte del Comitato e confluite in più ampie linee guida adottate nella plenaria del 15 dicembre 2020.

Linee guida 10/2020 sulle limitazioni ex art. 23 del RGPD

Le linee guida 10/2020 sulle limitazioni ai sensi dell'articolo 23 del RGPD, adottate il 12 febbraio 2021, ricordano le condizioni che regolano l'uso di tali restrizioni alla luce della CDFUE e del RGPD e forniscono un'analisi approfondita dei criteri per l'applicazione delle restrizioni, delle valutazioni che devono essere effettuate, di come gli interessati possono esercitare i loro diritti dopo la revoca delle restrizioni e delle conseguenze di eventuali violazioni dell'articolo 23. Nelle linee guida si ricorda che qualsiasi restrizione deve rispettare l'essenza del diritto che viene limitato e che non possono essere giustificate restrizioni suscettibili di svuotare il diritto fondamentale alla protezione dei dati personali del suo contenuto di base. Il documento analizza in che modo le misure legislative che stabiliscono le restrizioni devono soddisfare il requisito di prevedibilità ed esaminano i motivi delle restrizioni elencate dalla norma in questione e gli obblighi e i diritti che possono essere limitati; esso si sofferma altresì sul test di necessità e proporzionalità che le restrizioni devono superare in base all'articolo 23.

Accanto alle molte sollecitazioni che hanno portato all'adozione di numerosi documenti sul contemperamento tra diritto alla salute e protezione dei dati nell'ambito delle misure di contenimento della pandemia, il Cepd ha proseguito la sua attività di interpretazione e guida su norme e concetti-chiave del RGPD.

Valutazione del RGPD

Il Cepd ha ultimato nel corso dell'anno il proprio contributo alla procedura di valutazione del RGPD che la Commissione era chiamata ad effettuare entro il 25 maggio 2020 (e successivamente ogni quattro anni), ai sensi dell'art. 97 del RGPD. Il Cepd, 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 (cfr. Relazione 2019, p. 183).

Linee guida in materia di titolare e responsabile

Nell'ambito dell'attività volta a fornire chiarimenti sui concetti-chiave del RGPD, meritano menzione le linee guida in materia di titolare e responsabile volte ad aggiornare il parere 2/2010 del Gruppo Art. 29. Le linee guida, adottate il 2 settembre 2020 nella loro prima versione, destinata ad essere modificata nel corso del 2021 con l'adozione del testo finale all'esito della consultazione pubblica conclusasi il 19 ottobre 2020, che costituiscono un documento completamente nuovo rispetto al parere del Gruppo Art. 29. Corposo e ricco di esempi pratici, tiene in particolare considerazione le implicazioni delle norme sulla contitolarità di cui all'art. 26, così come gli obblighi del responsabile del trattamento alla luce dell'art. 28, nonché della giurisprudenza della CGUE. Le linee guida si dividono in due parti: l'una volta a spiegare i diversi concetti di cui all'art. 4 del RGPD (titolare, responsabile, contitolare, terzo e destinatario) e l'altra che chiarisce le principali conseguenze derivanti dall'assunzione dei diversi ruoli (in particolare di titolare, responsabile e contitolare). Le linee guida contengono un *executive summary* e una *flow chart* che fornisce indicazioni pratiche e riepilogative dell'articolato documento.

Con riferimento al rapporto tra titolare e responsabile del trattamento occorre inoltre segnalare l'adozione da parte del Comitato (19 maggio 2020) del parere sul progetto di clausole contrattuali standard (SCC) predisposte dall'Autorità slovena (e sottoposte al meccanismo di coerenza) per regolare il rapporto tra titolare e responsabile sulla base dell'art. 28, par. 6, del RGPD. Il parere mira a garantire l'applicazione coerente del menzionato art. 28, che impone ai titolari e ai responsabili del trattamento l'obbligo di stipulare un contratto o un altro atto giuridico che stabilisca i rispettivi obblighi delle parti e che in base all'art. 28, par. 6, del RGPD può essere basato, in tutto o in parte, sulle SCC adottate da un'autorità di controllo. Il Cepd ha formulato una serie di raccomandazioni che devono essere prese in considerazione affinché il progetto di SCC sia considerato idoneo a costituire clausole contrattuali standard ai sensi dell'art. 28, par. 8, del RGPD.

Sempre con riferimento all'interpretazione di norme-chiave del RGPD, il 4 maggio 2020, il Comitato ha adottato una nuova versione delle linee guida sul consenso che contengono alcune precisazioni sull'ambito dei trattamenti di dati *online*, volte a chiarire che i cd. *cookie walls* non permettono di configurare un consenso libero da parte dell'interessato e che il cd. *scroll* costituisce una pratica inidonea a configurare una valida manifestazione di consenso (cfr. 12.4).

Linee guida in materia di consenso

Il Cepd ha proseguito le proprie attività per assicurare un approccio uniforme anche nell'applicazione delle regole sulla cooperazione tra le autorità di protezione dei dati nei casi in cui il trattamento abbia carattere transfrontaliero: si tratta di attività che, come si è visto, impegna in modo crescente le risorse delle autorità di controllo (cfr., in relazione al Garante, i parr. 12.9 e 14.6 nonché, per indicatori numerici, la parte IV, tab. 10-12). Come noto, gli articoli 60 e ss. del RGPD disciplinano, da un lato, gli obblighi di cooperazione in capo alle autorità di protezione dei dati dell'UE (e del See) e, dall'altro, il meccanismo che, attraverso l'intervento del Cepd, è volto a garantire la coerenza delle azioni dalle stesse poste in essere.

Meccanismo di cooperazione e coerenza

La cooperazione tra le autorità avviene in larga misura grazie al sistema IMI (cfr. Relazione 2019, p. 184), le cui potenzialità e caratteristiche sono state, in fasi successive, parzialmente modificate per venire incontro alle peculiarità della cooperazione richiesta dal RGPD anche alla luce dell'esperienza via via acquisita.

L'utilizzo del sistema IMI è altresì necessario – come chiarito da ultimo nella più recente modifica del regolamento interno del Cepd avvenuta l'8 ottobre 2020 – per assicurare il coinvolgimento del Comitato anche nei casi in cui debba essere richiesta una sua decisione vincolante ai sensi dell'art. 65 del RGPD, ovvero quando l'autorità capofila decida di non tenere in considerazione le obiezioni pertinenti e motivate presentate, ai sensi dell'art. 60, par. 4, del RGPD, da una o più autorità interessate. Al fine di consentire un'applicazione coerente di tale disposizione, il Cepd ha adottato l'8 ottobre 2020 una prima versione delle linee guida 9/2020 sulle obiezioni pertinenti e motivate e le ha sottoposte a consultazione pubblica. Leggermente riviste e modificate nella loro versione definitiva (adottata il 9 marzo 2021), le linee guida si incentrano sulla nozione di obiezione "pertinente e motivata" e sottolineano la necessità di sostanziare le obiezioni con chiari riferimenti giuridici e/o fattuali da inoltrare all'autorità capofila nel rispetto dei tempi previsti dall'art. 60, par. 4, del RGPD, possibilmente accompagnandole con suggerimenti testuali di modifica. Le autorità interessate devono anche dimostrare in modo esplicito nell'obiezione, a pena dell'inammissibilità della stessa, "l'importanza dei rischi posti dal progetto di decisione" per i diritti e le libertà fondamentali degli interessati e, se del caso, per la libera circolazione dei dati personali all'interno dell'Unione (art. 4, n. 24), del RGPD).

Le linee guida hanno trovato applicazione in occasione dell'adozione della prima decisione vincolante adottata dal Cepd il 9 novembre 2020 in un caso relativo ad un *data breach* notificato a inizio 2019 (decisione 01/2020 ai sensi dell'art. 65, par. 1, lettera *a*), del RGPD relativa alla controversia sul progetto di decisione dell'Autorità di controllo irlandese concernente Twitter International) (cfr. cap. 16). La decisione ha consentito al Comitato di valutare le obiezioni presentate da diverse autorità di protezione dei dati (tra cui quella italiana) e, tra le varie presentate, di considerare accoglibili quelle relative alla natura insufficientemente dissuasiva dell'ammenda nonché di chiedere all'autorità capofila di rivalutare gli elementi su cui si basa il calcolo dell'importo dell'ammenda da infliggere alla società.

Sempre in materia di cooperazione, il Cepd è intervenuto con una nota informativa, adottata il 15 dicembre 2020 e rivista il 13 gennaio 2021 (alla luce della sottoscrizione dell'Accordo sugli scambi e la cooperazione firmato dall'UE e dal Re-

gno Unito il 30 dicembre 2020) per chiarire gli effetti della Brexit sui casi transfrontalieri che vedevano l'Autorità del Regno Unito come autorità capofila o interessata. La nota ricorda che dal 1º gennaio 2021 il meccanismo dello sportello unico non è più applicabile al Regno Unito e che, pertanto, titolari e responsabili del trattamento attualmente non stabiliti nel See potranno continuare a beneficiare dell'interlocuzione unica consentita dal meccanismo dello sportello unico (con l'autorità di controllo capofila) solo ove riorganizzino le proprie attività con la costituzione di un nuovo stabilimento principale nel See ai sensi dell'art. 4, n. 16), del RGPD. Ove invece gli stessi rimangano stabiliti nel Regno Unito ma svolgano attività di trattamento soggette all'applicazione dell'art. 3, par. 2, del RGPD, la nota ricorda l'obbligo per gli stessi di designare un rappresentante nell'Unione a norma dell'art. 27 del RGPD.

Coordinated Enforcement Framework

Al fine di intensificare le occasioni di cooperazione per garantire l'applicazione e l'attuazione coerente del RGPD, il Comitato ha adottato il 20 ottobre 2020 il cd. quadro di attuazione coordinata (*Coordinated Enforcement Framework* - CEF), un piano volto a fornire una metodologia concordata per coordinare le attività annuali ricorrenti delle autorità di protezione dei dati su un tema predefinito con l'obiettivo di facilitare azioni comuni che possano essere flessibili ma coordinate, attraverso azioni di sensibilizzazione e raccolta di informazioni o indagini a tappeto nell'ambito di un medesimo settore (cd. *sweep*) e indagini congiunte. Il quadro di attuazione coordinata – che dovrebbe coprire il periodo di tempo di un anno – lascia ovviamente impregiudicato il meccanismo di sportello unico e potrebbe essere assicurato, tra l'altro, attraverso forme di cooperazione volontaria. La prima azione coordinata dovrebbe essere avviata già nel corso del 2021.

Accreditamento degli OdM

Il Comitato si è altresì occupato di assicurare un approccio uniforme tra le autorità di protezione dei dati nella definizione ed applicazione dei requisiti di accreditamento per gli organismi di monitoraggio dei codici di condotta. L'accreditamento dell'organismo di monitoraggio costituisce una condizione necessaria per l'approvazione di un codice di condotta, con la sola eccezione del trattamento effettuato da autorità pubbliche e da organismi pubblici per il quale non è necessaria l'istituzione di tale organismo. In base al RGPD, infatti, fatti salvi i compiti e i poteri dell'autorità di controllo competente, la verifica dell'osservanza delle disposizioni di un codice di condotta, è effettuata da un organismo di monitoraggio in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento rilasciato a tal fine dalla medesima autorità. Il RGPD non fissa un unico insieme di requisiti per l'accreditamento di tali organismi, bensì demanda all'autorità di controllo competente la redazione dei propri requisiti per l'accreditamento degli organismi di monitoraggio sulla base dell'articolo 41, par. 2, del RGPD. Questi ultimi sono quindi adottati da ciascuna autorità di controllo competente in linea con il parere espresso dal Cepd, in ottemperanza al meccanismo di coerenza. Tale meccanismo, unitamente alle indicazioni fornite nelle linee guida 1/2019, assicura che i requisiti di accreditamento siano definiti dalle autorità di controllo competenti secondo un approccio armonizzato, di modo che gli organismi di monitoraggio possano effettuare la verifica dell'osservanza delle disposizioni dei codici di condotta in modo competente, coerente e indipendente, facilitando così la corretta attuazione di tali strumenti in tutta l'Unione e, di conseguenza, contribuendo alla corretta applicazione del RGPD. In tale contesto, l'Autorità ha predisposto il proprio progetto di requisiti per l'accreditamento degli organismi di monitoraggio, su cui il Cepd ha reso il parere (favorevole), previsto dall'art. 64, par. 1, lett. *c*), del RGPD, il 25 maggio 2020 (parere 13/2020); il Garante ha quindi modificato il proprio progetto di requisiti, in conformità alle osservazioni espresse, e ha definitivamente approvato i requisiti per l'accreditamento degli organismi di monitoraggio dei codici di condotta

con provvedimento del 10 giugno 2020, n. 98 (doc. web n. 9432569: cfr. par. 14.3).

Nel corso dell'anno, il Comitato si è espresso altresì in ordine ai progetti di requisiti di accreditamento presentati dalle Autorità di controllo spagnola (parere 1/2020), belga (parere 2/2020), francese (parere 3/2020), tedesca (parere 10/2020), irlandese (parere 11/2020), finlandese (parere 12/2020), olandese (parere 18/2020), danese (parere 19/2020), greca (parere 20/2020) e polacca (parere 21/2020).

Procedura per le "sessioni informali sui codici di condotta"

Sempre in materia di codici di condotta, il 10 novembre 2020, il Cepd ha adottato un documento interno che definisce la procedura per le "sessioni informali sui codici di condotta". Si tratta di una procedura di cooperazione informale tra le autorità di protezione dei dati a cui può fare ricorso l'autorità di controllo che intende sottoporre al Cepd un progetto di decisione per l'approvazione di un codice di condotta transnazionale in conformità all'art. 40, par. 7, del RGPD. La procedura è intesa a favorire l'analisi e la valutazione coordinata del progetto di codice da parte di tutte le autorità di controllo prima dell'attivazione della procedura formale finalizzata all'adozione del parere obbligatorio del Cepd previsto dal meccanismo di coerenza ai sensi dell'art. 64, par. 1, lett. *b*), del RGPD. Le sessioni si terranno pertanto al di fuori della sfera del mandato del Cepd e saranno guidate dall'autorità di controllo competente per il progetto di codice; a tali sessioni parteciperà anche il segretariato del Cepd e, su invito dell'autorità di controllo competente, potrà assistere la Commissione europea, tenuto conto del ruolo che il RGPD affida a quest'ultima, a norma dell'art. 40, ai fini della validità generale dei codici di condotta all'interno dell'UE.

Requisiti per l'accreditamento degli organismi di certificazione

Altrettanto importante è stata l'attività del Cepd volta ad assicurare la coerenza nell'applicazione del RGPD con riferimento alla definizione dei requisiti di accreditamento degli organismi di certificazione da parte delle autorità di controllo competenti ai sensi dell'art. 43, par. 3, del RGPD. Il Regolamento prevede che il rilascio di certificazioni in materia di protezione dati sia effettuato da organismi accreditati a svolgere tali funzioni dall'autorità di controllo competente o dall'organismo nazionale di accreditamento o da entrambi. In tutti i casi, in base alle linee guida del Cepd sull'accreditamento degli organismi di certificazione, al fine di contribuire ad un approccio armonizzato all'accreditamento, tali requisiti dovrebbero basarsi sulla norma tecnica internazionale EN-ISO/IEC 17065:2012 ed essere integrati dai requisiti "aggiuntivi" stabiliti dalle autorità di controllo nazionali ai sensi dell'art. 43, par. 1, lett. *b*), del RGPD, in linea con il parere espresso dal Cepd in ottemperanza al meccanismo di coerenza. Nel definire i requisiti aggiuntivi, le autorità di controllo si avvalgono del modello comune definito dal Cepd in allegato alle linee guida sull'accreditamento degli organismi di certificazione n. 4/2018.

Nel corso dell'anno, il Cepd ha reso il parere previsto dall'art. 64, par. 1, lett. *c*), del RGPD in ordine ai progetti di requisiti per l'accreditamento degli organismi di certificazione predisposti dalle Autorità di controllo del Regno Unito (parere 4/2020), del Lussemburgo (parere 5/2020), dell'Irlanda (parere 14/2020), della Germania (parere 15/2020), della Repubblica Ceca (parere 16/2020), dell'Olanda (parere 21/2020), della Grecia (parere 22/2020), della Danimarca (parere 26/2020) e dell'Austria (parere 30/2020). Sempre nel 2020, il Cepd ha esaminato il progetto di requisiti per l'accreditamento predisposto dal Garante e ha espresso il parere previsto dal meccanismo di coerenza il 23 luglio 2020 (parere 23/2020). A seguito del parere favorevole del Cepd, il Garante ha modificato il proprio progetto di requisiti in conformità alle osservazioni ivi contenute e, con provvedimento del 29 luglio 2020, n. 148 (doc. web n. 9445086: cfr. par. 14.7), ha definitivamente approvato i requisiti per l'accreditamento degli organismi di certificazione.

Il compito dell'accreditamento in Italia è svolto da Accredia, secondo quanto previsto dal legislatore.

Procedura di approvazione di criteri di certificazione riferiti a una certificazione comune europea

Sempre in materia di certificazione, il Cepd ha adottato un documento sulla procedura di approvazione di criteri di certificazione riferiti a una certificazione comune, il sigillo europeo per la protezione dei dati (28 gennaio 2020). Il documento mira ad agevolare il Cepd nel valutare ed esprimere il proprio parere in modo tempestivo e coerente in ordine all'approvazione di criteri per le certificazioni europee. Il RGPD prevede infatti che il Cepd approvi criteri di schemi di certificazione europei (cfr. artt. 43, par. 3 e 63), ma non definisce una procedura specifica per la loro approvazione. Al riguardo, il documento prevede che le autorità di controllo (competenti per il luogo ove si colloca la sede principale del titolare dello schema o dell'organismo di certificazione che gestisce lo schema) possano presentare al Cepd, per l'approvazione ai sensi dell'art. 70, par. 1, lett. *o*), del RGPD, i criteri relativi a una certificazione valida nell'intera UE (cfr. art. 42, par. 5, del RGPD) ove ritengano che questi soddisfino i requisiti stabiliti per una certificazione europea conforme al RGPD, tenendo conto delle linee guida del Cepd 1/2018 relative alla certificazione. In questo caso, prende avvio una fase informale di valutazione dei criteri di certificazione, modellata sulla procedura di approvazione delle Bcr, volta a consentire la valutazione coordinata dei criteri di certificazione da parte delle altre autorità di controllo. La valutazione consiste, in particolare, nel verificare che i criteri tengano in debita considerazione le norme nazionali applicabili. Al termine della fase di cooperazione informale, l'autorità di controllo competente, consultandosi con il titolare dello schema, può decidere se presentare i criteri di certificazione al Cepd per l'approvazione formale in conformità all'art. 63 del RGPD. In questo caso, la procedura di approvazione da parte del Cepd potrà concludersi con l'approvazione o con il rigetto della richiesta. In caso di approvazione del sigillo UE, la richiesta seguirà la procedura di adozione del parere di cui all'art. 64, par. 2, del RGPD, trattandosi di una questione che produce effetti in più di uno Stato membro. Il parere del Cepd, una volta adottato, produrrà i suoi effetti in tutti gli Stati membri e non sarà necessario darvi alcun seguito a livello nazionale.

Trasferimento dati all'estero: la sentenza Schrems II

In tema di trasferimenti di dati all'estero, attore principale sulla scena europea è stata, nel 2020, la CGUE che, il 16 luglio, con la sentenza Schrems II (causa C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems), ha confermato la validità della decisione della Commissione europea n. 2010/87/CE relativa alle clausole contrattuali tipo per il trasferimento di dati personali a responsabili del trattamento stabiliti in Paesi terzi e ha invalidato la decisione della Commissione n. 2016/1250/CE relativa all'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la *privacy* (cd. *Privacy Shield*).

La Corte, per la prima volta, si è soffermata sulla natura delle clausole contrattuali previste (ora) dall'art. 46, par. 2, del RGPD e sulla loro effettiva capacità di assicurare, attraverso gli impegni che esportatore e importatore assumono contrattualmente in termini di garanzie per la protezione dei dati personali trasferiti, un livello di tutela sostanzialmente equivalente a quello riconosciuto nell'Unione. In particolare, la Corte ha sottolineato che tali clausole "mirano unicamente a fornire ai titolari del trattamento o ai responsabili del trattamento stabiliti nell'Unione garanzie contrattuali che si applicano in modo uniforme in tutti i Paesi terzi e, pertanto, indipendentemente dal livello di protezione garantito in ciascuno di essi. Poiché tali clausole tipo di protezione dei dati non possono, tenuto conto della loro natura, fornire garanzie che vadano al di là di un obbligo contrattuale di vegliare a che sia rispettato il livello di protezione richiesto dal diritto dell'Unione, esse possono richiedere, in funzione della situazione esistente nell'uno o nell'altro Paese terzo, l'adozione di misure supplementari da parte del titolare del trattamento al fine di garantire il rispetto di tale livello di protezione" e ciò in particolare quando il diritto

di tale Paese terzo permetta alle proprie autorità pubbliche ingerenze nei diritti delle persone interessate che vadano oltre quanto strettamente necessario per conseguire l'obiettivo legittimo perseguito e non esista contro tali ingerenze una tutela giuridica efficace. Nell'utilizzo delle clausole contrattuali tipo, ruolo rilevante giocano quindi, in prima battuta, l'esportatore – che, con l'ausilio dell'importatore (che meglio conosce la disciplina del proprio Paese), deve valutare l'ordinamento del Paese terzo alla luce del caso di specie e individuare, qualora necessario, le "garanzie supplementari" rispetto a quelle offerte dalle clausole – e, in seconda battuta, le autorità di protezione dei dati: sono infatti queste ultime ad essere chiamate a verificare, su reclamo o d'ufficio, che le misure supplementari adottate assolvano al loro compito e, ove ciò, "alla luce del complesso delle circostanze proprie [del] trasferimento", non avvenga, sono tenute a sospendere o a vietare un trasferimento di dati personali verso un Paese terzo "a meno che esista una decisione di adeguatezza validamente adottata dalla Commissione". Al riguardo, nel chiarire che "fino a che tale decisione non sia stata dichiarata invalida dalla Corte, l'autorità di controllo competente non può sospendere o vietare un trasferimento di dati personali", la Corte si è quindi soffermata sul caso specifico dei trasferimenti effettuati verso gli Stati Uniti – oggetto del reclamo originario presentato da Maximillian Schrems all'Autorità irlandese con riguardo ai trasferimenti posti in essere dalla società Facebook Ireland verso la società statunitense del medesimo gruppo – e ha considerato necessario valutare anche la decisione di adeguatezza "Scudo per la *privacy*" (così come aveva fatto, nella causa C-362/14, Maximillian Schrems v. Data Protection Commissioner, con riferimento al regime posto in essere dal *Safe Harbour*, su cui cfr. Relazione 2015, p. 161). Guardando in particolare alla normativa interna degli Stati Uniti in materia di accesso e di utilizzo dei dati da parte delle autorità statunitensi di *intelligence* nell'ambito dell'attuazione di taluni programmi di sorveglianza (in particolare FISA 702 e E.O. 12333), la Corte ha stabilito quindi che le limitazioni al diritto alla protezione dei dati personali che risultano da siffatta normativa non possono considerarsi proporzionate. Parimenti la Corte ha considerato che la normativa in questione non conferisce agli interessati (stranieri) diritti azionabili dinanzi ai giudici nei confronti delle autorità statunitensi e che il meccanismo di mediazione preso in considerazione dalla decisione 2016/1250 non fornisce a tali persone un mezzo di ricorso dinanzi ad un organo indipendente e capace di adottare decisioni vincolanti nei confronti dei servizi di *intelligence* statunitensi. In assenza di questi elementi, essenziali per garantire il livello di protezione sostanzialmente equivalente a quello richiesto nel diritto dell'Unione, la Corte ha deciso quindi di invalidare la decisione di adeguatezza.

Trasferimenti dei dati all'estero e misure supplementari

Tenuto conto dell'inevitabile impatto della sentenza sui trasferimenti di dati in Paesi terzi, il Comitato ha fornito primi chiarimenti sugli effetti della stessa, già il 23 luglio 2020, con un documento recante le FAQ in merito alla sentenza della CGUE nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems e, successivamente, il 10 novembre 2020, indicazioni più dettagliate nelle raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE. Entrambi i documenti, e soprattutto le raccomandazioni, si ripromettono di aiutare gli esportatori (titolari del trattamento o responsabili del trattamento, enti privati o enti pubblici) a valutare la legislazione del Paese terzo applicabile al trasferimento da porre in essere al fine di individuare, ove necessario, le misure supplementari appropriate da adottare per consentire il rispetto delle garanzie contenute nello strumento di trasferimento prescelto. Le raccomandazioni, partendo da un richiamo al principio dell'*accountability*, forniscono un *decision tree* attraverso cui l'esportatore è accompagnato nell'individuazione degli strumenti più

21

adeguati al trasferimento dei dati in un Paese terzo. Sei sono i passi da percorrere: 1. definire l'ambito del trasferimento (*Know your transfer*); 2. verificare lo strumento più adatto al trasferimento in questione (laddove non ci sia una decisione di adeguatezza della Commissione: clausole contrattuali tipo, clausole *ad hoc*, regole vincolanti di impresa, ecc.); 3. valutare se vi sia qualcosa nella legge o nella prassi del Paese terzo che possa incidere sull'efficacia delle garanzie contenute nello strumento di trasferimento utilizzato; 4. identificare ed adottare le misure supplementari considerate necessarie per assicurare che il livello di protezione assicurato nell'Unione sia mantenuto nel Paese terzo; 5. adottare ogni eventuale passo procedurale necessario per l'adozione degli strumenti in questione; 6. rivalutare a intervalli adeguati la disciplina applicabile ai dati trasferiti per verificare che il livello di tutela assicurato dallo strumento di trasferimento prescelto e dalle misure supplementari sia mantenuto. In allegato al documento sono illustrati anche alcuni scenari/esempi relativi a possibili misure supplementari da adottare nel caso in cui la legislazione di un Paese terzo impedisca il rispetto delle garanzie già contenute negli strumenti di trasferimento utilizzati: le misure suggerite sono anzitutto di natura tecnologica, ma ve ne sono anche di natura contrattuale e organizzativa. Il documento è stato sottoposto a consultazione pubblica e sarà rivalutato e, ove del caso, rivisto, alla luce delle osservazioni ricevute.

Clausole contrattuali standard per il trasferimento dei dati all'estero

La decisione della CGUE nel caso Schrems II ha informato anche il progetto di decisione di esecuzione relativa alle clausole contrattuali tipo per il trasferimento di dati personali a Paesi terzi ai sensi del RGPD con cui la Commissione, il 12 novembre 2020, ha proposto quattro nuovi differenti set di clausole contrattuali (titolare-titolare; titolare-responsabile; responsabile-sub-responsabile; responsabile-titolare). Le clausole, nel riprendere per quanto possibile le precedenti, contengono garanzie in linea con il RGPD e includono ulteriori obblighi per le parti coinvolte funzionali a rafforzare la tutela dei dati personali nei casi in cui la legislazione del Paese terzo consenta l'accesso agli stessi da parte di soggetti pubblici.

Sul progetto di decisione è stato espresso, il 14 gennaio 2021, il parere congiunto del Cepd e del Gepd (cfr. parere congiunto 2/2021 sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo per il trasferimento di dati personali a Paesi terzi). Il parere contiene una serie di commenti generali e reca anche un allegato nel quale sono contenute specifiche proposte di emendamento delle clausole tipo proposte.

Trasferimenti di dati tra soggetti pubblici e a organizzazioni internazionali

Come anticipato, sebbene riferita a trasferimenti di dati effettuati tra soggetti privati, la sentenza Schrems II esplica i propri effetti anche con riferimento ai trasferimenti di dati posti in essere da soggetti pubblici, sia quando questi si avvalgono di responsabili (o sub-responsabili) del trattamento stabiliti in Paesi terzi, sia quando i dati sono trasferiti a soggetti pubblici nel Paese terzo. Con riferimento a tale ultima tipologia di trasferimenti, il Cepd ha rivisto, all'esito della consultazione pubblica, le proprie linee guida per il trasferimento di dati a soggetti pubblici nei Paesi terzi o ad organizzazioni internazionali adottate nel febbraio 2020 (linee guida 2/2020: cfr. Relazione 2019, p. 192). Le modifiche introdotte, alla luce dei commenti ricevuti – in maggior misura da parte di organizzazioni internazionali –, chiariscono anzitutto che le linee guida si applicano anche alla modifica degli accordi internazionali conclusi prima del 24 maggio 2016 (v. art. 96 del RGPD) e tengono conto delle specificità delle organizzazioni internazionali quando queste operano quali importatori dei dati. È ora espressamente richiamata la possibilità di prevedere, direttamente negli accordi relativi al trasferimento dei dati, il loro utilizzo ulteriore a fini di archiviazione, di ricerca scientifica, storica o a fini statistici e la possibilità di porre in essere eventuali restrizioni ai diritti degli interessati solo ove le stesse siano in linea con

quelle elencate nel RGPD. In particolare, nel caso la limitazione derivi dalla necessità di rispettare un interesse pubblico rilevante, le linee guida chiariscono che analogo interesse pubblico deve essere riconosciuto anche dall'ordinamento nazionale dello Stato membro interessato o dal diritto dell'Unione. Si evidenzia nel documento che, per l'autorizzazione di accordi amministrativi tra i soggetti pubblici ai sensi dell'art. 46, par. 3, lett. *b*), del RGPD, dovrà essere applicata la procedura di coerenza di cui all'art. 64, par. 2, del RGPD.

Alla luce della sentenza Schrems II, le linee guida richiamano l'attenzione sulla necessità per le autorità pubbliche europee di effettuare, prima di concludere definitivamente gli accordi in questione, una valutazione del livello di protezione nel Paese dell'importatore – sia esso un organismo pubblico nel Paese terzo o un'organizzazione internazionale –, compresa una verifica circa la possibilità che le garanzie concordate siano rispettate in pratica. Sono state anche rafforzate le indicazioni in ordine alle restrizioni ai trasferimenti ulteriori dei dati, in modo da escludere la comunicazione di dati personali ad altre autorità pubbliche del Paese terzo dell'organismo pubblico ricevente ove la stessa sia non necessaria e proporzionata in una società democratica. Infine, le sezioni dedicate ai meccanismi di tutela dei diritti degli interessati e di vigilanza sono state formulate in modo da richiedere chiaramente che tali meccanismi offrano all'interessato garanzie sostanzialmente equivalenti a quelle previste dall'articolo della Carta UE.

Bcr

Analoga attenzione agli effetti della sentenza Schrems II è stata rivolta dal Cepd e dalle autorità di protezione dei dati con riferimento all'utilizzo delle regole vincolanti di impresa (*Binding corporate rules*, Bcr). Come noto, al fine di assicurare la coerente applicazione del RGPD, il Cepd è tenuto a fornire un proprio parere in merito a ciascun progetto di decisione recante l'approvazione di Bcr presentato dalle autorità competenti (individuate sulla scorta dei criteri indicati nel WP 263 rev. 01: v. Relazione 2018, p. 190). Tali pareri non sono volti ad autorizzare o approvare singoli trasferimenti ma accertano che le garanzie contenute nelle Bcr offrano un livello adeguato di tutela alla luce degli elementi richiesti dall'art. 47 del RGPD e dai documenti di lavoro relativi alle Bcr per titolari e per responsabili (WP 256, rev. 01, e WP 257, rev. 01: cfr. Relazione 2017, p. 167). Tale aspetto – evidenziato già nei pareri relativi alle Bcr per titolari del trattamento e per responsabili del trattamento adottati prima del luglio 2020 (pareri nn. 6/2020, 8/2020, 9/2020) – è stato ulteriormente sottolineato in quelli successivi alla sentenza (pareri nn. 24/2020, 25/2020, 27/2020, 28/2020, 29/2020, 32/2020) al fine di ribadire come, in occasione dell'utilizzo delle Bcr quale strumento di trasferimento nei casi specifici, deve verificarsi che il quadro normativo applicabile consenta all'importatore di rispettare gli impegni assunti con l'adesione alle Bcr. Ove ciò non sia possibile, l'esportatore dovrà – come nel caso delle clausole contrattuali tipo – individuare garanzie supplementari che gli consentano di rispettare tali impegni o astenersi dal trasferire i dati.

Brexit e trasferimento dei dati all'estero

Il 1° febbraio 2020, con l'entrata in vigore dell'accordo di recesso ratificato dall'UE e dal Regno Unito, quest'ultimo è divenuto un Paese terzo e il Cepd, nel corso dell'anno, è intervenuto più volte per chiarire gli effetti con riferimento al tema dei trasferimenti di dati. Sebbene grazie alla clausola ponte contenuta nell'Accordo sugli scambi e la cooperazione firmato dall'UE e dal Regno Unito il 30 dicembre 2020, i trasferimenti di dati personali tra soggetti ai quali si applica il RGPD e soggetti stabiliti nel Regno Unito non saranno considerati come trasferimenti verso un Paese terzo fino al 30 giugno 2021, dopo tale data ogni trasferimento di dati personali verso il Regno Unito sarà possibile solo attraverso l'utilizzo di uno degli strumenti previsti dal Capo V del RGPD e, ove necessario, delle misure supplementari che ne consentano il rispetto in concreto (cfr. nota informativa sui trasferimenti di dati verso

il Regno Unito ai sensi del RGPD dopo il periodo di transizione, adottata il 15 dicembre 2020 e aggiornata il 13 gennaio 2021). Entrambe le Parti si stanno adoperando per consentire l'utilizzo del più agevole tra questi strumenti, ovvero le decisioni di adeguatezza, e in quest'ottica la Commissione ha già presentato, il 19 febbraio 2021, due proposte di decisione per l'adeguatezza del Regno Unito, rispettivamente ai sensi dell'art. 45 del RGPD e dell'art. 36 della direttiva 2016/680 sulle quali il Comitato ha espresso i propri pareri il 13 aprile 2021 (pareri nn. 14 e 15/2021).

Per assicurare una transizione più agevole per gli operatori, il Cepd ha adottato, nel luglio 2020, una nota informativa con la quale ha chiarito che le Bcr autorizzate dall'Autorità di protezione dei dati del Regno Unito in vigenza di direttiva possono essere utilizzate senza discontinuità (e senza "approvazioni" da parte della nuova *Lead*) ove le stesse vengano aggiornate (secondo le regole inserite nelle stesse Bcr) con riferimento ad alcuni elementi essenziali che sono indicati in un *Annex* dello stesso *statement* (tra cui, in particolare, indicazione della nuova *Lead* alla luce delle modifiche organizzative introdotte dai gruppi e modifiche adeguate in ogni parte delle Bcr in cui alla *Lead* si faccia riferimento; nuova società del gruppo che assume su di sé la responsabilità nel caso di violazione delle Bcr da parte di una società del gruppo stabilita fuori dall'UE e sua adeguata capacità economica; legge UE applicabile al contratto e giurisdizione per l'esercizio dei diritti in linea con l'art. 79 del RGPD). Le Bcr approvate in vigenza di RGPD sono state invece nuovamente approvate dalla nuova *Lead* SA, a seguito di nuovo parere del Cepd (parere 32/2020). Per le Bcr che erano in corso di valutazione, i gruppi interessati sono stati invitati ad individuare una nuova Bcr *Lead* e proseguire (ove già avviate) le procedure di approvazione in linea con il WP 263.

Protezione dei dati, attività finanziaria e anti-riciclaggio

È proseguita l'attività del Cepd anche riguardo all'applicazione delle norme del RGPD nel settore finanziario attraverso il sottogruppo *Financial Matters* coordinato dal Garante.

Sempre in ambito finanziario, il Cepd è tornato ad occuparsi del rapporto tra la normativa anti-riciclaggio e di contrasto al finanziamento del terrorismo (AML/CFT) e i principi di protezione dati. In particolare, a seguito della pubblicazione da parte della Commissione del proprio Piano di azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo del 7 maggio 2020, il Cepd ha adottato una dichiarazione (15 dicembre 2020) per esprimere l'interesse e la disponibilità del Comitato ad essere coinvolto nel processo di revisione della normativa AML/CFT. Questo per far sì che tale processo di revisione rappresenti l'occasione per definire i principi di protezione dei dati da rispettare, assicurando allo stesso tempo l'efficienza del sistema di contrasto al riciclaggio, anche attraverso trattamenti proporzionati e non ridondanti da parte degli istituti finanziari chiamati a svolgere il monitoraggio sulle transazioni "sospette".

Linee guida 6/2020 sul rapporto tra PSD2 e RGPD

Una delle questioni centrali affrontate dal Cepd è stata 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. Le importanti novità nel sistema dei pagamenti dettate dalla PSD2 – che consente a nuovi soggetti di attuare servizi che un tempo erano prerogativa esclusiva delle banche, permettendo ad essi l'accesso ad una mole considerevole di dati finanziari (non solo dei clienti, ma anche di soggetti terzi) – ha reso necessaria una riflessione sul corretto rapporto tra le due discipline. Il Cepd, 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 il RGPD (cfr. Relazione 2018, p. 193), ha adottato le linee guida 6/2020 nella plenaria del 17 luglio 2020. A seguito della consultazione pubblica cui il testo è stato sottoposto le

linee guida sono state adottate nella loro versione finale il 15 dicembre 2020. Esse si soffermano, in particolare, sulle basi giuridiche del trattamento effettuato dai fornitori di servizi di pagamento, sulla questione degli "ulteriori trattamenti" alla luce degli artt. 66 e 67 della PSD2 (che restringono considerevolmente la possibilità che i dati siano trattati per finalità ulteriori rispetto a quelle originariamente previste), sul tema del trattamento dei dati sensibili anche con riferimento alle cd. *silent third parties* (ad es. i beneficiari di ordini di pagamenti), sui principi di minimizzazione dei dati, sicurezza, trasparenza e *accountability*, nonché sui principi da rispettare con riferimento alle attività di profilazione.

Le "garanzie essenziali europee"

A seguito della menzionata sentenza Schrems II della CGUE, il Cepd ha adottato una serie di raccomandazioni sulle garanzie essenziali europee relativamente alle misure di sorveglianza. Le raccomandazioni aggiornano quelle individuate dal Gruppo Art. 29 dopo la prima sentenza Schrems (WP 237) e devono considerarsi complementari alle raccomandazioni sulle misure supplementari agli strumenti di trasferimento dei dati nei Paesi terzi. Nello specifico, tali raccomandazioni forniscono agli esportatori di dati elementi utili a stabilire se il quadro giuridico nel Paese terzo in materia di accesso ai dati da parte delle autorità pubbliche per fini di sorveglianza, siano queste agenzie di *intelligence* o di *law enforcement*, configuri un'ingerenza giustificata nei diritti alla vita privata e alla protezione dei dati personali e non sia quindi in contrasto con gli impegni assunti dall'esportatore e dall'importatore attraverso lo strumento utilizzato per il trasferimento fra quelli previsti dall'art. 46 del RGPD. Anche la Commissione, nel valutare l'adeguatezza del livello di protezione ai sensi dell'art. 45 del RGPD, dovrà verificare, tra gli elementi da considerare per determinare se la legislazione di un Paese terzo fornisce nel suo complesso un livello di protezione dei dati sostanzialmente equivalente a quello garantito all'interno dell'UE, che le garanzie essenziali europee siano soddisfatte. Le garanzie essenziali europee individuate nelle raccomandazioni, in quanto elementi fondamentali per determinare il livello di ingerenza nei diritti fondamentali al rispetto alla vita privata e alla protezione dei dati, sono strettamente collegate e vanno tenute in considerazione nel loro complesso, non potendo essere valutate singolarmente.

Il secondo Protocollo addizionale alla Convenzione di Budapest

Il 29 gennaio 2020, il Cepd ha adottato una lettera indirizzata al Consiglio d'Europa sulla bozza di secondo Protocollo addizionale alla Convenzione di Budapest. Nel novembre 2019 il Cepd aveva già fornito il proprio contributo alla consultazione pubblica lanciata dal Comitato *Cybercrime* del Consiglio d'Europa (T-CY) sulla bozza del menzionato Protocollo addizionale e, attraverso alcuni suoi rappresentanti, aveva presentato la propria posizione nel corso della *Octopus Conference* tenutasi a Strasburgo il 20-22 novembre 2019 (cfr. Relazione 2019, p. 194). Tale contributo era stato tuttavia limitato al testo provvisorio del Protocollo che allora non includeva le previsioni relative alla protezione dei dati, successivamente divenute oggetto di negoziazione. A tale riguardo, la lettera sottolinea l'importanza di integrare rigorose salvaguardie volte ad assicurare un alto livello di protezione dei dati nel testo del Protocollo stesso. La lettera evidenzia altresì la necessità di garantire piena coerenza tra il Protocollo addizionale e la Convenzione 108, nonché la compatibilità del Protocollo stesso con i Trattati UE e la Carta europea dei diritti fondamentali. Infine, viene auspicato l'avvio di una consultazione specifica sulle garanzie di protezione dati prima della finalizzazione del Protocollo addizionale, ribadendo la disponibilità a fornire un contributo costruttivo e oggettivo alle negoziazioni.

Clearview AI

Con un'altra lettera, adottata il 10 giugno 2020, il Cepd ha fornito riscontro a un gruppo di parlamentari europei sul presunto uso di Clearview AI da parte delle autorità di *law enforcement* e dei servizi di *intelligence* nell'UE. Secondo alcune notizie di stampa (apparse a gennaio sui *media*), la società statunitense raccoglierebbe

mediante *scraping* fotografie e immagini del viso pubblicate *online*, in particolare sui *social network*, e fornirebbe alle Forze dell'ordine e alle agenzie di *intelligence* di tutto il mondo un servizio di riconoscimento facciale. A seguito di tali notizie, diverse autorità di protezione dei dati europee hanno avviato indagini sull'uso di tali tecnologie nel proprio Paese. Nella lettera il Cepd sottolinea i rischi derivanti in generale dall'uso della tecnologia di riconoscimento facciale per i diritti e le libertà fondamentali, ricordando che il quadro giuridico applicabile per il trattamento dei dati biometrici da parte delle autorità di *law enforcement* è quello previsto dalla direttiva (UE) 2016/680. La lettera richiama l'attenzione sul fatto che l'eventuale utilizzo di un servizio come Clearview AI comporterebbe, nell'ambito di un'indagine di polizia o penale, la condivisione di dati personali con un soggetto privato al di fuori dell'Unione e un confronto biometrico con le fotografie e immagini del viso contenute in una banca dati privata, popolata su larga scala, in modo arbitrario e indiscriminato. Alla luce della legislazione dell'UE e degli Stati membri e fatte salve le risultanze degli approfondimenti in corso da parte delle autorità di protezione dei dati nazionali, il Cepd nutre notevoli dubbi sulla liceità dell'utilizzo di tale servizio da parte delle autorità di *law enforcement* anche sotto il profilo del rispetto delle stringenti garanzie previste dalla direttiva (UE) 2016/680 per il trasferimento di dati al di fuori dell'Unione. Sebbene le questioni relative al trattamento di dati nel settore della sicurezza nazionale rientrino solo in parte nell'ambito di applicazione del diritto dell'UE (e quindi nella competenza del Cepd), nella lettera si sottolinea altresì che il trattamento di questi dati da parte dei servizi di *intelligence* deve essere sempre effettuato in conformità alla Convenzione 108 e alla Convenzione europea dei diritti dell'uomo come interpretata dalla CEDU.

Accordo UE-USA ai fini del TFTP

Ulteriori preoccupazioni sono state espresse dal Cepd in una lettera di risposta al parlamentare europeo Moritz Körner (3 dicembre 2020) riguardante l'Accordo tra l'UE e gli USA sul trattamento e il trasferimento dei dati di messaggistica finanziaria nell'ambito del *Terrorist Finance Tracking Program* (il cd. accordo TFTP). In particolare, il Cepd ha sollevato dubbi in merito all'effettiva possibilità per gli interessati di chiedere la correzione o la cancellazione dei propri dati personali trattati dal Dipartimento del tesoro degli USA e alla massiccia quantità di dati di messaggistica finanziaria regolarmente trasferiti e conservati dalle autorità statunitensi, ribadendo la necessità di una revisione dell'accordo.

Veicoli connessi

Con riferimento alle nuove tecnologie, in data 28 gennaio 2020 il Cepd ha adottato le linee guida sul trattamento dei dati personali nel contesto dei veicoli connessi e della mobilità correlata alle applicazioni (*Guidelines* 1/2020). Il documento è stato sottoposto a consultazione pubblica e adottato, nella sua versione definitiva, il 9 marzo 2021. Con detto documento il Cepd ha inteso affrontare il tema del trattamento dei dati personali relativo all'uso non professionale dei veicoli connessi da parte di vari soggetti. In particolare, il trattamento riguarda i dati personali trattati all'interno del veicolo e scambiati tra il veicolo e i dispositivi personali ad esso collegati (es., lo *smartphone* dell'utente) o raccolti all'interno del veicolo e trasmessi ad entità esterne per ulteriori elaborazioni (es. costruttori di veicoli, gestori di infrastrutture, compagnie di assicurazione, autoriparatori). Le linee guida si riferiscono altresì alle molteplici applicazioni mobili indipendenti dal veicolo, quali quelle in materia di gestione della mobilità, gestione del veicolo, sicurezza stradale, intrattenimento, assistenza alla guida e benessere. Sull'assunto che la maggior parte dei dati generati da un veicolo connesso si riferiscono a una persona fisica identificata o identificabile (costituendo quindi dati personali), il documento si rivolge prioritariamente alla larga platea di soggetti che potrebbero trattarli (produttori di veicoli e di apparecchiature, fornitori, riparatori e concessionari di automobili, fornitori

di servizi per veicoli, fornitori di intrattenimento, operatori di telecomunicazioni, gestori di infrastrutture stradali e autorità pubbliche) richiamando l'attenzione sui rischi connessi a tali tipologie di trattamento e alle misure da adottare per assicurare il rispetto della disciplina in materia di protezione dei dati personali.

Regolamento *e-privacy* e autorità di controllo

Il 19 novembre 2020 è stata adottata dal Cepd una dichiarazione sul regolamento *e-privacy* e sul futuro ruolo delle autorità di controllo nella quale si sottolinea la necessità di affidare il controllo delle disposizioni recate dal regolamento *e-privacy* e relative al trattamento dei dati personali alle autorità di protezione dei dati, trattandosi di ambiti connessi rispetto ai quali le rispettive discipline non possono formare oggetto di applicazione isolata. Il documento evidenzia la necessità che il regolamento *e-privacy* non debba abbassare il livello di protezione offerto dall'attuale direttiva 2002/58/CE, ma piuttosto integrare il RGPD, fornendo ulteriori tutele per la riservatezza e la protezione dei dati in relazione a tutti i tipi di comunicazione elettronica. La dichiarazione richiama l'attenzione su alcuni orientamenti emersi in occasione delle discussioni svoltesi in seno al Consiglio concernenti le preoccupazioni per la frammentazione della vigilanza, la complessità procedurale e la mancanza di coerenza e certezza del diritto per le persone e le imprese. In relazione alle discussioni in corso relative all'ulteriore trattamento dei metadati delle comunicazioni elettroniche, il Cepd ha ribadito il suo sostegno all'approccio del regolamento *e-privacy*, basato su ampi divieti, eccezioni ristrette e sull'uso del consenso, sottolineando che i metadati delle comunicazioni elettroniche possono essere trattati senza consenso dopo che sono stati effettivamente resi anonimi.

Linee guida sul *targeting* degli utenti di *social media*

Il 2 settembre 2020 il Cepd ha adottato le linee guida sul *targeting* degli utenti di *social media* (linee guida 8/2020). Partendo dalla constatazione che il *targeting* degli utenti dei *social media* crea rischi per i diritti e le libertà fondamentali delle persone e può coinvolgere una varietà di attori (fornitori di *social media*, loro utenti, destinatari e altri soggetti che possono essere coinvolti nel processo di *targeting*), le linee guida – sulla scorta del RGPD e della giurisprudenza della CGUE – si pongono quale obiettivo principale quello di chiarire i principi applicabili e la base giuridica, individuare i principali attori, i loro ruoli e le relative responsabilità, identificando anche i potenziali rischi per i diritti e le libertà delle persone partendo da esempi concreti (distinguendo tra *targeting* sulla base dei dati forniti, *targeting* sulla base dei dati osservati e *targeting* sulla base dei dati dedotti). Le linee guida forniscono indicazioni anche in ordine alle circostanze in cui risulta necessario porre in essere una valutazione d'impatto sulla protezione dei dati, ai casi in cui il *targeting* porta all'applicazione dell'art. 9 del RGPD e all'obbligo per i contitolari di concludere un accordo ai sensi dell'art. 26 del RGPD, tenendo conto del grado di responsabilità del *targeter* e del fornitore del servizio di *social media*.

Numerose le lettere adottate dal Cepd in risposta alle sollecitazioni di diversi *stakeholder* con riferimento al trattamento dei dati nell'ambito delle nuove tecnologie. Tra di esse si ricorda la risposta del 29 gennaio 2020 alla richiesta dell'europarlamentare Sophie in't Veld relativa all'uso di algoritmi iniqui – nella quale viene fornita un'analisi delle problematiche, dal punto di vista della protezione dei dati, che possono emergere dall'impiego degli algoritmi, in particolare la mancanza di trasparenza e i possibili profili discriminatori che da essi possono derivare – nonché una sintetica panoramica delle norme del RGPD e delle linee guida rilevanti adottate dal Cepd. La lettera chiarisce che più che sull'elaborazione di una normativa specifica sugli algoritmi (con riferimento alla protezione dei dati) è opportuno focalizzarsi sull'implementazione delle norme esistenti, in particolare sui requisiti di trasparenza, *accountability* e valutazione d'impatto *privacy*, anche in vista dell'elaborazione di possibili future linee guida su tale tema.

21

Con una dichiarazione adottata il 19 febbraio 2020, il Cepd si è infine espresso sulle implicazioni per la protezione dei dati derivanti da fusioni o acquisizioni di grandi società che operano nella rete. In particolare con riferimento all'annuncio di acquisizione della società Fitbit da parte di Google, il Cepd ha sottolineato la necessità che le Parti conducano in modo trasparente una completa valutazione dei requisiti di protezione dei dati e delle implicazioni in tale ambito derivanti della fusione, provvedendo a mitigare i possibili rischi per la protezione dei dati prima di notificare la fusione alla Commissione europea.

Le sanzioni amministrative

Come è noto, il RGPD impone un rigoroso regime sanzionatorio; in proposito, il Cepd sta lavorando su linee guida che forniscano una base chiara per la fissazione delle sanzioni da parte delle autorità di controllo, fondate sui criteri di valutazione stabiliti nel RGPD al fine di garantire una coerente applicazione delle sanzioni da parte della autorità di protezione dei dati.

21.2. *La cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

Europol Cooperation Board

In virtù del nuovo quadro normativo introdotto dal regolamento (UE) 2016/794, entrato in vigore il 1° maggio 2017, la supervisione sull'attività svolta dall'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) è svolta dal Gepd. Rimane di competenza delle autorità nazionali di protezione dei dati la vigilanza sulla comunicazione di dati ad Europol da parte delle autorità di contrasto (*law enforcement*) e la verifica circa il rispetto dei diritti degli interessati. Al fine di assicurare una stretta cooperazione tra il Gepd e le autorità nazionali è stato istituito, con funzioni consultive, un Consiglio di cooperazione (*Europol Cooperation Board*-ECB) che nel 2020 si è riunito due volte in videoconferenza (il 16 giugno e il 24 novembre).

Nel corso della prima riunione, il Consiglio ha invitato un rappresentante della Commissione europea a presentare la valutazione d'impatto iniziale per la revisione del regolamento Europol e ha invitato due rappresentanti dell'ICANN (*Internet Corporation for Assigned Names and Numbers*) per uno scambio di opinioni sulla banca dati WHOIS, tenuta da ICANN. L'ECB ha continuato a lavorare all'aggiornamento del manuale delle unità nazionali dell'Europol e sulla guida all'accesso; ha altresì adottato, con procedura scritta, la raccomandazione e il parere sulla soluzione europea di tracciamento (20 febbraio 2020) e una nota informativa e di discussione interna in tema di interconnessione attraverso l'interoperabilità (3 marzo 2020).

Nella seconda riunione, il Gepd ha informato l'ECB sulle sue attività di vigilanza, ed in particolare: sull'ispezione annuale inizialmente programmata per novembre 2020 poi rinviata a causa della pandemia; sul *follow-up* delle raccomandazioni, dopo le ispezioni del 2017 e del 2018; sulle violazioni dei dati e su una consultazione sulle richieste di accesso degli interessati nel Regno Unito. Inoltre, sono stati presentati i risultati principali delle risposte ricevute dalle Unità Nazionali Europol (EUN), in seguito all'indagine adottata dall'ECB con procedura scritta l'8 luglio 2020.

Nel corso della riunione, è stata approvata una versione modificata della guida all'accesso, adottata con procedura scritta nel mese di settembre.

Infine, i membri dell'ECB hanno condiviso informazioni relative alle attività di vigilanza svolte dalle loro autorità di protezione dei dati in relazione alle attività di Europol, e discusso sia il progetto di relazione di attività 2019-2020 che quello relativo al programma di lavoro 2021-2023.

Gruppo di coordinamento della supervisione del 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 di competenza del Gruppo di coordinamento della supervisione SIS II, di cui fanno parte le autorità di protezione dati dei Paesi membri – che assicurano la supervisione delle autorità nazionali competenti per il sistema SIS II – e il Gepd – che supervisiona il trattamento dati posto in essere dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (EU-LISA), cui è rimessa la gestione del sistema centrale.

Nel corso del 2020 il Gruppo di coordinamento della supervisione SIS II si è riunito due volte in videoconferenza (il 17 giugno e il 25 novembre; la documentazione rilevante può essere consultata presso il sito del Gruppo alla pagina: https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en).

Durante la riunione di giugno, in cui sono stati eletti Gert Vermeulen alla carica di presidente e Clara Guerra a quella di vicepresidente, il Gruppo ha discusso dei risultati delle ispezioni SIS e VIS che hanno avuto luogo nei locali di EU-LISA e del numero sempre crescente di istanze di accesso al sistema da parte degli interessati (principalmente riguardanti segnalazioni di respingimento).

Nel corso della seconda riunione, la Commissione europea ha informato il Gruppo sul Nuovo patto sulla migrazione e l'asilo – con il quale si intende, attraverso l'avvio di iniziative legislative e non legislative, rafforzare le misure alle frontiere – e sulla proposta di regolamento sullo *screening* che si applicherebbe a tutti i cittadini non UE che attraversano una frontiera esterna senza autorizzazione, ai richiedenti asilo durante i controlli alla frontiera o che arrivano sul territorio degli Stati membri dopo un'operazione di ricerca e salvataggio in mare.

Il gruppo ha discusso anche delle modalità per la composizione dei *team* di esperti per le valutazioni periodiche sull'applicazione del Sistema Schengen nei diversi Paesi membri e delle difficoltà incontrate da molte autorità che non riescono a mettere a disposizione propri esperti per mancanza di risorse adeguate.

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 ad assicurare il rispetto della protezione dei dati personali all'interno del sistema istituito per la comparazione delle impronte digitali dei richiedenti asilo.

Il Gruppo si è riunito in videoconferenza due volte nel 2020 (il 18 giugno e il 26 novembre). Nel corso delle due riunioni – in cui si è proceduto all'elezione di Evelyne Schuurmans (DPA Paesi Bassi) per la posizione di vice presidente – è stato presentato e discusso il monitoraggio del sistema effettuato da EU-LISA e il gruppo ha sottolineato l'importanza di rimuovere tempestivamente dal sistema i dati personali dei richiedenti asilo allorché l'esigenza di protezione internazionale venga meno. Il Rpd di EU-LISA ha presentato gli ultimi aggiornamenti che hanno visto un incremento del 4% dei dati inseriti nel sistema Eurodac rispetto all'anno precedente, nonostante l'impatto significativo dell'emergenza da Covid-19 e che ha comportato un complessivo rallentamento del sistema. È continuato il lavoro sull'opuscolo destinato alle autorità nazionali e volto a informare gli interessati sui loro diritti e, in proposito, il Gruppo è stato aggiornato in merito allo stato di avanzamento della collaborazione con l'Agenzia per i diritti fondamentali (FRA) per la traduzione dell'opuscolo in più lingue.

Nel suo programma di lavoro 2019-2021, il Gruppo ha concordato di lavorare sul *follow-up* degli sviluppi politici e legislativi relativi al sistema Eurodac e di continuare a favorire lo scambio di esperienze e assistenza reciproca.

Gruppo di coordinamento della supervisione del 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.

Nel corso del 2020, il Gruppo di supervisione (i cui documenti sono rinvenibili sul sito internet: https://edps.europa.eu/data-protection/european-it-systems/visa-information-system_en) si è riunito in videoconferenza due volte, il 18 giugno ed il 26 novembre.

Nel corso della prima riunione, Caroline Gloor Scheidegger (DPA svizzera) e Eleni Maragkou (DPA ellenica) sono state confermate rispettivamente come presidente e vicepresidente del VIS SCG per un mandato di altri due anni. Il Gruppo ha discusso della proposta di modifica del regolamento VIS presentata dalla Commissione nel maggio 2018 e delle modifiche piuttosto importanti in essa contenute, come l'abbassamento dell'età per il rilevamento delle impronte digitali per i richiedenti bambini da 12 anni a 6 anni e la conservazione di una copia del documento di viaggio del richiedente nel VIS per sostenere le procedure di rimpatrio. La Commissione è stata invitata nell'ultima riunione a presentare al Gruppo la proposta VIS e le sue principali modifiche. Il Gruppo ha altresì discusso, nell'ambito del suo programma di lavoro 2019-2021, la natura, la portata e il contenuto per la predisposizione di un quadro comune per i controlli di sicurezza del sistema tenendo conto dell'esperienza analoga con il sistema d'informazione Schengen e il sistema Eurodac in questo contesto.

Durante la seconda riunione, il Gruppo è stato informato circa lo stato di avanzamento della revisione del regolamento VIS e sui recenti aggiornamenti riguardo alla gestione del sistema centrale VIS da parte di EU-LISA. Enisa ha poi aggiornato il Gruppo sullo stato di attuazione dell'EES (*Enter Exit System*), che ha subito ritardi a causa della pandemia.

Il Gruppo ha altresì discusso dei meccanismi di cancellazione dei dati dal VIS in caso di acquisto della cittadinanza o di annullamento del rifiuto di un visto (art. 25 del regolamento (UE) 767/2008) che intervengano prima dei 5 anni previsti ordinariamente per la conservazione dei dati nel VIS. È stata fatta circolare una bozza di documento, sulla base della quale ciascun partecipante è stato invitato a fare approfondimenti a livello nazionale, al fine di individuare buone pratiche e indicazioni, sia di tipo organizzativo che tecnico, per assicurare la tempestiva cancellazione dei dati nel VIS nelle ipotesi previste dalla norma.

SID

Il Sistema informativo doganale (SID) 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 contrastarne le violazioni di natura amministrativa (sulla base del regolamento (CE) 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).

Anche la riunione del Gruppo di coordinamento della supervisione del Sistema d'informazione doganale si è tenuta in videoconferenza il 15 giugno 2020. Il

Gruppo ha continuato a lavorare all'aggiornamento della guida all'accesso del SID a seguito dell'entrata in vigore del RGPD e della scadenza del termine per il recepimento della direttiva (UE) 2016/680. Le persone, i cui dati personali sono raccolti, detenuti o altrimenti trattati nel SID, hanno diritto alla correzione dei dati inesatti e alla cancellazione dei dati memorizzati illegalmente. La predetta guida ha lo scopo di aiutare le persone interessate a identificare l'autorità competente e le modalità di esercizio di tali diritti in relazione al SID. Inoltre, il Gruppo ha convenuto di avviare un lavoro specifico che esamini la preparazione del personale delle autorità che accedono ai dati del SID al fine di fornire una formazione specifica sulla protezione dei dati. I membri del Gruppo hanno aggiornato i loro colleghi con informazioni sulle loro ispezioni nazionali o altri sviluppi rilevanti a livello nazionale. Infine, è stato adottato il programma di lavoro per l'anno 2020-2022.

21.3. *La partecipazione dell'Autorità in seno al Consiglio d'Europa, all'OCSE e ad altri gruppi di lavoro internazionali*

T-PD

È proseguita l'attività dell'Autorità nell'ambito del Consiglio d'Europa, in particolare attraverso la partecipazione al Comitato consultivo della Convenzione 108/1981 (cd. T-PD), del quale la rappresentante del Garante ha conservato la presidenza per il terzo mandato consecutivo (confermato nelle elezioni della plenaria di novembre).

Nonostante la cancellazione di una riunione plenaria (prevista per il 1°-3 luglio) e dell'incontro del *Bureau* del Comitato (T-PD *Bureau*) del 25-27 marzo 2020 a causa delle restrizioni per il contrasto alla pandemia, i lavori del T-PD sono proseguiti in una prima fase attraverso scambi scritti e quindi, per la seconda plenaria dell'anno (18-20 novembre) e le successive riunioni del *Bureau* (28-30 settembre e 16-18 dicembre 2020), con modalità telematiche. Anche nel caso del Consiglio d'Europa la modalità remota ha permesso un'ampia partecipazione da parte dei delegati – 182 in totale nel caso della plenaria – che costituisce un traguardo significativo per l'evidente attenzione ai lavori del T-PD prestata da Parti e Osservatori.

Convenzione 108+ e lotta alla pandemia

Anche il T-PD è intervenuto sulla questione della tutela dei dati personali nell'ambito della gestione della crisi sanitaria. Il 30 marzo 2020 è stata pubblicata una dichiarazione congiunta della presidente del T-PD e del Commissario per la protezione dei dati del Consiglio d'Europa sulla necessità di assicurare il rispetto dei principi di protezione di dati anche nell'ambito dell'emergenza da Covid-19. La dichiarazione parte dal presupposto che la Convenzione 108 offre margini di flessibilità che permettono di contemperare l'esigenza di garantire la salute pubblica con il rispetto dei diritti fondamentali e sottolinea la necessità che situazioni particolari (come l'emergenza sanitaria) debbano essere affrontate con misure proporzionate che non portino ad una acritica limitazione delle libertà fondamentali. Si sofferma inoltre sulle restrizioni ed eccezioni ai principi di protezione dati previste dalla stessa Convenzione e sottolinea che in ogni caso occorre predisporre procedure volte a consentire un tempestivo pieno ripristino delle garanzie non appena venga meno la situazione emergenziale. Lo *statement* si sofferma anche sulla questione del trattamento dei dati in ambito lavorativo e nella didattica a distanza, nonché sui dati di localizzazione, richiamando i principi dettati dalla raccomandazione (2019)2 in materia di dati relativi alla salute e dalle linee-guida rispettivamente in materia di *big data* e di intelligenza artificiale adottate nel 2017 e 2019 dal T-PD.

Questo prima *statement* è stato seguito da un'altra dichiarazione congiunta della presidente del T-PD e del Commissario per la protezione dei dati del Consiglio

d'Europa, del 28 aprile 2020, che ha riguardato l'impiego da parte degli stati di nuove tecnologie nella lotta al Covid-19, in particolare delle applicazioni di tracciamento. La dichiarazione sottolinea la necessità di effettuare preliminarmente una verifica dell'idoneità ad assicurare il perseguimento della finalità mediante tali tecniche, la cui efficacia deve peraltro collocarsi all'interno di strategie integrate. Altresì importante è reputata l'esigenza di assicurare la volontarietà del ricorso alle *app* di tracciamento, anche al fine di incrementare, insieme alla trasparenza e ad un sistema sicuro di trattamento dei dati, una piena fiducia rispetto all'impiego di tali applicazioni. La necessità di una preliminare valutazione di impatto, di garantire che siano trattati solamente i dati strettamente necessari, per una finalità specifica e determinata, di assicurare la cancellazione dei dati una volta esaurito il legittimo scopo del trattamento, nonché di garantire l'esercizio dei diritti degli interessati, in particolare quello di non essere sottoposto a decisioni automatizzate senza avere la possibilità di esprimere il proprio punto di vista, sono gli aspetti imprescindibili perché il trattamento dei dati sotteso all'impiego delle applicazioni di tracciamento possa dirsi conforme ai principi di protezione dati previsti dalla Convenzione 108+.

Trasferimenti dei dati e tutela delle persone nell'ambito delle attività di *intelligence*

Lo strumento della dichiarazione congiunta è stato altresì utilizzato in tema di trasferimenti di dati per finalità di *intelligence*, in particolare a seguito della sentenza Schrems II (v. *supra*). Lo *statement* del commissario per la protezione dei dati del Consiglio d'Europa e della presidente del T-PD del 7 settembre 2020 si è concentrato in particolare sulla necessità che siano meglio garantiti i diritti delle persone nell'ambito dei trasferimenti dei dati e che sia assicurato un effettivo controllo sui trattamenti effettuati nell'ambito delle attività di *intelligence*. La Convenzione 108+ può giocare un ruolo cruciale in tal senso in quanto standard internazionale sulla protezione dei dati nell'era digitale nonché strumento praticabile per facilitare i trasferimenti internazionali di dati garantendo un livello adeguato di protezione per le persone a livello globale.

Convenzione 108+

Il T-PD ha continuato a seguire con attenzione il processo di firma e ratifica del Protocollo emendativo della Convenzione 108/1981, adottato il 18 maggio 2018 e aperto alla firma il 10 ottobre dello stesso anno (cd. Convenzione 108+), volto ad attualizzare i principi dell'originaria Convenzione alla luce del mutato scenario tecnologico e globale. Nel 2020 è giunto a 33 il numero di nuovi stati firmatari del Protocollo emendativo (tra cui l'Italia, che lo ha sottoscritto il 5 marzo 2019), e a 9 il numero di ratifiche. L'auspicio è che vi sia un numero crescente di tempestive ratifiche, compresa quella dell'Italia, tenendo presente che il Protocollo emendativo può entrare in vigore (oltre che nel caso della ratifica di tutte le attuali Parti della Convenzione 108), anche ove nei 5 anni successivi all'apertura alla firma si raggiunga la ratifica di almeno 38 Parti. Si sottolinea che 5 Parti, nel ratificare il Protocollo, si sono avvalse dell'art. 37.3 dichiarandone l'applicabilità temporanea in vista della sua entrata in vigore.

Sempre con riferimento alla Convenzione 108+, il T-PD ha continuato il lavoro sui meccanismi di valutazione (*evaluation*) dei futuri candidati ad accedere alla 108+, la cui competenza sarà attribuita al futuro Comitato convenzionale, e di periodico riesame (*follow up*) per verificare la persistente aderenza ai principi della Convenzione degli Stati che già ne faranno parte. Il T-PD ha proseguito tale attività tenendo conto del fatto che, se da una parte l'entrata in vigore della Convenzione 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 norma prevede infatti che a partire dall'apertura alla firma del Protocollo qualunque nuova richiesta di accedere alla 108 debba essere accompagnata dalla richiesta di accessione alla 108+, rendendosi così necessaria una pronta predisposizione dei meccanismi valutativi previsti da quest'ultima.

Particolarmente tempestiva ed opportuna, considerata la grande diffusione della didattica a distanza determinata a livello globale dalla necessità di disporre la chiusura delle scuole per contrastare la pandemia, è stata l'adozione da parte del Comitato delle linee guida sulla protezione dei dati dei minori nei contesti educativi. Queste linee guida si rivolgono ai legislatori, alle scuole e all'industria affinché, in un settore delicato come quello scolastico, siano garantiti i diritti fondamentali dei minori, che non devono essere compromessi dalla crescente digitalizzazione la quale, pur offrendo opportunità importanti per l'istruzione, deve essere accompagnata da adeguate garanzie per i diritti delle persone. Le linee guida raccomandano il rigoroso rispetto dei principi di protezione dei dati previsti dalla Convenzione 108+, e tra questi il principio di finalità (che deve essere esclusivamente scolastica e non commerciale), la trasparenza, la necessità di una adeguata base normativa del trattamento e la sicurezza dei dati. Particolare attenzione è rivolta all'esercizio dei diritti considerati imprescindibili anche al fine di garantire un equilibrato e libero sviluppo dei minori, scevro dai condizionamenti significativi che possono derivare da forme crescenti di profilazione (anche da parte dei cd. giganti della rete) delle attività *online* in ambito scolastico.

Linee guida sulla protezione dei dati dei minori nei contesti educativi

Il T-PD ha proseguito gli approfondimenti in materia di riconoscimento facciale. Dopo la discussione sul *report* dei due esperti scientifici sulle implicazioni tecniche e giuridiche di tale tecnologia alla luce dei criteri previsti per i dati biometrici dalla Convenzione modernizzata (art. 6 della 108+), è stata avviata la predisposizione di specifiche linee guida. Queste ultime, poi adottate in occasione della Giornata europea per la protezione dei dati (28 gennaio 2021), forniscono una serie di misure di riferimento che governi, sviluppatori di sistemi di riconoscimento facciale, produttori, aziende e p.a. dovrebbero adottare per garantire che l'impiego di queste tecnologie non pregiudichi la dignità della persona, i diritti umani e le libertà fondamentali. Le linee guida a fronte dei pericoli che possono derivare da tecniche particolarmente invasive come il riconoscimento facciale, richiamano la necessità di un dibattito pubblico e di un approccio ispirato al principio di precauzione. Il documento segnala i particolari rischi derivanti dal riconoscimento facciale volto a rilevare i tratti della personalità, i sentimenti o le reazioni emotive dall'immagine del volto, stabilendone il divieto nelle procedure di assunzione di personale, nell'accesso ai servizi assicurativi e all'istruzione. Analogamente, non dovrebbe essere consentito l'uso del riconoscimento facciale al solo scopo di determinare il colore della pelle di una persona, le convinzioni religiose o di altro tipo, il sesso, l'origine etnica, l'età, le condizioni di salute o le condizioni sociali. Le linee guida si soffermano altresì sull'uso di sistemi di riconoscimento facciale da parte delle Forze dell'ordine, che dovrebbe essere consentito solamente ove strettamente necessario per prevenire un rischio imminente e grave alla sicurezza pubblica. Esse si rivolgono agli sviluppatori di tecnologie di riconoscimento facciale affinché prestino specifica attenzione all'attendibilità degli algoritmi e all'accuratezza dei dati trattati, al fine di evitare disparità e possibili ricadute discriminatorie e raccomandano ad aziende e p.a. che intendano avvalersi di tecniche di riconoscimento facciale di garantire il rispetto dei principi di protezione dati.

Riconoscimento facciale

Un ruolo importante a tutela dei diritti delle persone possono svolgerlo le autorità di protezione dei dati che, in base all'art. 15.3 della Convenzione 108+, devono essere consultate riguardo a proposte legislative e amministrative che comportino il trattamento dei dati personali mediante tecnologie di riconoscimento facciale, nonché prima di possibili sperimentazioni o utilizzi.

Il T-PD ha continuato a seguire le negoziazioni per la stesura del secondo Protocollo addizionale alla Convenzione di Budapest, che toccherà, tra gli altri, anche il tema dell'accesso diretto da parte delle autorità di *law enforcement* ai dati trattati da

Convenzione di Budapest

soggetti privati. Ha a tal proposito riaffermato la posizione già espressa in passato secondo cui il regime di protezione dei dati di detto Protocollo deve essere in linea con la Convenzione 108+ anche per garantire piena coerenza tra i diversi strumenti del Consiglio d'Europa e ha invocato trasparenza nelle negoziazioni proprio per garantire il proprio contributo alla elaborazione delle parti del protocollo che abbiano un impatto sulla protezione dei dati.

È proseguito il lavoro di revisione della raccomandazione in materia di profilazione (2010)13 volto ad aggiornarne il testo anche al fine di dar conto dei cambiamenti nel frattempo intervenuti nell'ambito dell'intelligenza artificiale (peraltro oggetto di specifiche linee guida adottate dal T-PD il 25 gennaio 2019) e della necessità di ampliare i riferimenti alle forme di profilazione effettuate in ambito pubblico, nonché di tener conto delle più recenti e frequenti forme di manipolazione degli utenti della rete fondate sulla raccolta di dati personali.

Il T-PD ha dato inizio anche all'esame di nuovi argomenti presenti nel programma di lavoro che saranno oggetto di future linee guida: sulla base di *report* di esperti scientifici sono stati avviati approfondimenti sul trattamento dei dati personali nell'ambito delle campagne politiche, sulla identità digitale, nonché sull'art. 11 della Convenzione 108+ relativo ai criteri che devono accompagnare le possibili restrizioni ed eccezioni ai principi della stessa Convenzione per garantire che, anche in questo caso, sia assicurato il rispetto dell'essenza del diritto alla protezione dei dati.

È stato altresì affrontato il tema degli scambi automatizzati di dati tra Stati per finalità amministrative e di tassazione, già oggetto di un parere del T-PD del 2014 (T-PD (2014)05), per tener conto delle novità nel frattempo intervenute.

È stata inoltre definita la bozza di dichiarazione del Comitato dei ministri sulla necessità di intensificare gli sforzi per la protezione della *privacy* dei minori in ambito digitale, frutto del lavoro congiunto dei segretariati del T-PD e del Comitato sui diritti dei minori (CDENF) in vista della sua trasmissione al Comitato dei ministri.

Si segnala infine che il Comitato dei ministri ha adottato in procedura scritta la raccomandazione (2020)1 sull'impatto degli algoritmi sui diritti umani sulla cui bozza il T-PD aveva fornito parere (T-PD (2019)09).

In occasione della Giornata europea della protezione dei dati (28 gennaio 2020) è stato assegnato il Premio Stefano Rodotà istituito dal T-PD per ricordare il grande giurista, già Presidente del Garante e *Chair* del Gruppo Art. 29. Il Premio, destinato a ricercatori e studenti e volto a valorizzare progetti di ricerca innovativi nel campo della protezione dei dati personali, è stato assegnato a Camilla Tabarrini per il suo articolo "Comprendere la "*Big Mind*". Il GDPR sana il divario di intelligibilità uomo-macchina?".

È proseguita l'attività del CAHAI, il Comitato *ad hoc*, istituito dal Comitato dei ministri del Consiglio d'Europa ed incaricato di esaminare la fattibilità di un quadro giuridico per lo sviluppo, la progettazione e l'applicazione dell'intelligenza artificiale, basato sugli standard del Consiglio d'Europa sui diritti umani, la democrazia e lo stato di diritto. In particolare, l'attività del CAHAI si è articolata in diversi gruppi di lavoro tra cui il *Policy Development Group* (CAHAI-PDG) di cui Guido Scorza, componente del Collegio, è rappresentante per l'Italia. Il CAHAI-PDG, riunitosi il 15-16 ottobre 2020, ha discusso di un documento di lavoro volto, tra l'altro, ad identificare i possibili strumenti giuridici per poter delineare il quadro di regole sull'intelligenza artificiale. Tra le ipotesi in discussione si segnala la possibilità che sia in futuro avviata la preparazione di una convenzione internazionale in materia di intelligenza artificiale che fissi i principi generali per garantire il rispetto dei diritti umani. Nelle more della realizzazione di tale ambizioso progetto, potrebbero essere parallelamente predisposti più agevoli strumenti di *soft law*, anche in ambito settoriale.

OCSE-DGP

È proseguita l'intensa attività dell'Autorità in ambito OCSE, in particolare attraverso la partecipazione al DGP (*Working Party on Data Governance and Privacy*), di cui il rappresentante del Garante è vicepresidente dal 2012 (già WPSPDE - *Working Party on Security and Privacy in Digital Economy*) ed ha conservato la vicepresidenza per il 2021 (confermata nelle elezioni della plenaria di novembre).

Il lavoro svolto in piena pandemia da Covid-19 è stato quanto mai prezioso in termini di risposte globali che un'organizzazione internazionale come l'OCSE ha potuto fornire in relazione all'impatto dell'emergenza da Covid-19 sulla *data governance* e *privacy*. In particolare, si è tenuto un *high level workshop* (15 aprile), organizzato congiuntamente dal DGP dell'OCSE e dalla *Global Privacy Assembly* (GPA), in precedenza nota come *International Conference of Data Protection and Privacy Commissioners*, per discutere le tendenze emergenti e le prime lezioni apprese sull'emergenza da Covid-19. Dal seminario è emerso che la risposta mondiale al Covid-19 ha dato origine ad una serie di sfide in materia di *governance* dei dati che destano notevoli preoccupazioni. Ad esempio, sono state sollevate preoccupazioni circa l'uso innovativo delle tecnologie digitali – in particolare le tecnologie che tracciano i movimenti della popolazione (*tracing app*) – combinato con un'ampia condivisione di dati personali come possibile strumento di contenimento della pandemia. Queste misure possono avere un impatto sproporzionato sulla *privacy* delle persone e alimentare incertezze sul trattamento dei dati mediante le menzionate *app*. Tale lavoro è proseguito nel corso dell'anno in una serie di *workshop* tematici e tavole rotonde (che hanno accompagnato l'intensificarsi del livello di emergenza globale); particolarmente significativo il *workshop* del 16 settembre 2020, su Covid e *data protection*, volto a consentire la condivisione delle conoscenze tra i responsabili politici, le autorità per la protezione dei dati e altre parti interessate in relazione alle sfide per la *privacy* e la protezione dei dati connesse alla pandemia.

Linee guida dell'OCSE sulla *privacy*

Le due riunioni plenarie del DGP, tenutesi virtualmente il 21 e 22 aprile 2020 ed il 9 e 17 novembre 2020, cui si sono come di consueto aggiunte le relative riunioni del *Bureau* (il gruppo ristretto del DGP), sono state caratterizzate da un'altissima partecipazione delle delegazioni dei Paesi membri, agevolata dalla partecipazione da remoto e dalla forte motivazione data dal comune obiettivo di vincere la pandemia nel rispetto dei diritti individuali. Il lavoro si è concentrato sulla revisione delle linee guida dell'OCSE sulla privacy del 2013 (*Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*), accelerato al fine di progredire nella realizzazione dell'*Interim report* relativo ai risultati del questionario sul gradimento delle *Privacy Guidelines*. Da tale documento è emerso che: tutti i Paesi considerano ancora le *Privacy Guidelines* del 2013 uno strumento utile; dal 2013 si registra un *trend* crescente di Paesi che hanno aggiornato la propria normativa in materia di protezione dei dati; per molti Paesi la sfida principale per attuare quanto previsto dalle *Privacy Guidelines* resta l'insufficienza di risorse. Partendo da tali risultati il segretariato del Gruppo ha presentato un nuovo *draft* che include: le risposte di 31 Paesi al citato questionario, i commenti dei delegati dei Paesi membri e degli esperti del PGEG (*Privacy Guidelines Expert Group*, Gruppo di esperti che ha guidato la revisione cui il Garante partecipa sin dalla sua costituzione); i principali punti emersi dalle varie tavole rotonde tematiche susseguitesi nel corso del 2019/2020 – con particolare riferimento ai *workshop* sulla *data localisation,* sul *trusted government access*, sui *regulatory sandboxes*, sulla *data portability* e sull'impatto del Covid-19 –; infine, una lista di possibili azioni di *follow-on.*

È emerso un supporto generale per: un'ulteriore guida per l'attuazione di specifiche parti delle *Privacy Guidelines*; la revisione effettiva del solo *Memorandum* supplementare (*Supplementary Explanatory Memorandum*); un ulteriore lavoro analitico

(*Regulatory sandboxes* e PETs); un lavoro su tematiche trasversali (es. identificazione di collegamenti tra *privacy, consumers* e *policy* di concorrenza).

Per quanto riguarda il tema dell'*accountability*, da sempre centrale nelle *Privacy Guidelines*, il lavoro di revisione ha confermato quanto sia cruciale il rispetto di tale principio e ha evidenziato la necessità di lavorare ad un'ulteriore guida volta a favorire la sua concreta attuazione.

Raccomandazione OCSE sulla protezione dei minori *online*

Il WP-DGP ha parimenti portato avanti la revisione della Raccomandazione OCSE sulla protezione dei minori *online* (*Recommendation on Children in the Digital Environment*), adottata dal Consiglio OCSE nel 2012. Nel corso dell'anno, il Gruppo ha lavorato sulla nuova tipologia di rischi per i minori anche alla luce dell'emergenza da Covid-19, correlata al crescente uso di *smartphone* e altri *smart devices*. Dalla discussione è altresì emerso che la corretta gestione dei dati personali, in particolare nella didattica a distanza, rappresenta il presupposto indispensabile per rendere lo strumentario digitale una risorsa per la garanzia del diritto allo studio, al riparo da rischi di abusi o violazioni senza abbassare la guardia sulla protezione dei dati personali dei minori, soggetti più fragili e vulnerabili. All'esito di più consultazioni e dei commenti formulati dai delegati del DGP e del *Committee on Digital Economy Policy* (CDEP) sono state redatte una nuova bozza di raccomandazione e di linee guida per i fornitori di servizi digitali con il supporto del Gruppo informale di esperti (inclusi i rappresentanti dei Paesi membri dell'OCSE e delle economie *partner*, BIAC, CSISAC nonché di altre organizzazioni internazionali e università).

Quanto ai prossimi passi, a seguito del contributo ricevuto dai delegati DGP e CDEP, nonché all'esito delle consultazioni cui la bozza di raccomandazione sarà sottoposta, la stessa sarà presentata al DGP e al CDEP per l'esame e l'approvazione finale; sarà quindi trasmessa al Consiglio OCSE, tramite il Comitato esecutivo, per l'adozione, indicativamente nel secondo trimestre del 2021. Ad avvenuta adozione della nuova raccomandazione, al fine di supportare l'attuazione del documento stesso, il segretariato del DGP ha proposto di sviluppare un documento di accompagnamento, stante la difficoltà di attuazione, riconosciuta dai delegati del DGP sin dall'inizio del lavoro di analisi avviato nel 2017.

Data Governance

Tra gli altri temi che il DGP ha trattato con particolare attenzione nel 2020 si segnala quello del *Data Governance: Enhanced Access and Sharing of Data* (EASD): si è in particolare discusso della bozza di raccomandazione, che presenta termini e concetti consolidati, nonché delle opzioni per garantire la coerenza e la costante pertinenza delle attuali raccomandazioni OCSE su accesso e condivisione dei dati. Al riguardo i vari Paesi hanno convenuto sulla necessità di rafforzare l'elemento della fiducia (*trust*) che, soprattutto nella fase attuale di emergenza globale, diventa strumento fondamentale per il *data sharing* consapevole e per i flussi di dati. Scopo principale dell'EASD resta quello di elaborare principi generali e *policy guidance* su come i governi possono rafforzare l'accesso e la condivisione di dati sia per massimizzare i benefici che per individuare i rischi potenziali (ad es. affrontare temi sociali condivisi globalmente come l'emergenza da Covid-19). L'importante lavoro *in fieri* – condotto dal DGP con la collaborazione di altri Comitati, quali il CDEP ed il *Committee for Scientific and Technological Policy* (CSTP), nonché del *Public Governance Committee* (PGC) – sarà adottato per procedura scritta, previa consultazione degli *stakeholders* interessati.

Accesso affidabile dei governi ai dati dei privati

Si segnala l'importante lavoro sull'accesso affidabile dei governi ai dati dei privati (*trusted government access to data*), fortemente voluto dalla delegazione giapponese nell'ambito del processo di revisione delle *Privacy Guidelines*. Al riguardo il CDEP ha discusso in una sessione chiusa del 19 novembre 2020 la proposta del DGP di seguire i lavori ed ha elaborato e adottato una dichiarazione di alto livello che ri-

conosce l'importanza della questione, il ruolo del CDEP nell'affrontarla e i punti comuni tra i Paesi dell'OCSE. La dichiarazione ha altresì comportato l'istituzione di un Gruppo di redazione *ad hoc* per ulteriori approfondimenti sul tema dell'accesso governativo al fine di sviluppare uno strumento OCSE basato su ampie aree di consenso (ad es. dichiarazione ministeriale, raccomandazione, ecc.). Il lavoro parte dalla constatazione che i flussi transfrontalieri di dati sono parte integrante dell'economia digitale globale e passaggio inevitabile per cogliere appieno i vantaggi della digitalizzazione. Pertanto si rendono necessarie una *governance* adeguata e idonee garanzie sull'accesso da parte dei governi ai dati personali detenuti dai privati allo scopo di creare fiducia e ridurre al minimo i rischi connessi ai flussi dei dati.

21.4. *Le Conferenze internazionali ed europee*

Global Privacy Assembly

L'Autorità ha preso parte *online* alla Conferenza internazionale delle autorità di protezione dati (*Global Privacy Assembly*, 13-15 ottobre 2020), che ha dedicato una particolare attenzione alla riflessione sulla strategia della stessa GPA e ai profili di protezione dati in relazione alla lotta alla pandemia. Nello specifico, la prima sessione è stata dedicata alla direzione strategica da dare alla GPA, come stabilito nella relativa risoluzione del 2019, mettendo in evidenza i risultati del primo anno di strategia politica e i piani futuri. La Conferenza è stata l'occasione per illustrare come la GPA sia stata ascoltata nel corso del 2020 in diversi contesti attraverso un forte impegno esterno e come la stessa possa essere ancora più attiva mediante dichiarazioni congiunte su questioni globali emergenti, come avvenuto per la pandemia da Covid-19 (si veda ad es. il grande lavoro sinergico GPA/OCSE). La seconda giornata è stata dedicata al tema della pandemia da Covid-19 ed è stato messo in luce come l'attuale emergenza sanitaria abbia introdotto modalità di raccolta dati che in precedenza non figuravano nelle agende dei membri del GPA. La sanità elettronica e la condivisione dei dati nel settore pubblico come nel settore privato sono ormai diventate priorità in larga parte degli ordinamenti poiché tutti i governi cercano di affrontare rapidamente ed efficacemente l'emergenza sanitaria. Sono stati quindi presentati i principali risultati delle attività della *Task force* GPA Covid-19, istituita a maggio 2020 ed incaricata di esaminare le sfide emergenti in materia di protezione dei dati e *privacy* poste nel contesto della pandemia, facilitando la condivisione di informazioni con la comunità dei membri GPA al fine di identificare opportunità di coinvolgimento rilevanti per influenzare il dibattito internazionale sulla *privacy* in merito alla risposta globale al Covid-19. È seguita una presentazione del *Privacy Commissioner for Personal Data* di Hong Kong che ha elaborato un Compendio delle migliori pratiche da adottare durante la riunione annuale della GPA. In tale contesto si è inserito l'intervento del Garante, in qualità di co-sponsor della risoluzione su Covid-19 e *privacy*, che ha illustrato l'esperienza italiana nel difficile equilibrio tra lotta al Covid-19 e protezione dei dati personali. All'esito dei lavori, oltre alla menzionata risoluzione sulle sfide per la protezione dei dati da affrontare nell'ambito della gestione dela pandemia, sono state adottate altre risoluzioni in particolare sui seguenti temi: a) riconoscimento facciale; b) il ruolo della protezione dei dati nella gestione degli aiuti umanitari internazionali; c) *accountability* nello sviluppo e utilizzo dell'intelligenza artificiale; d) comunicati congiunti in merito a questioni globali.

CPC-DPA
Joint Workshop

Con il coordinamento della DG JUST *Unit* della Commissione europea e del segretariato del Comitato si è svolto a novembre in videoconferenza un incontro fra rappresentanti delle autorità di protezione dati e delle autorità di tutela del consu-

matore. Nel corso del *meeting* i relatori hanno evidenziato come l'emergenza causata dal Covid-19 abbia determinato una crescita esponenziale del mercato digitale, con un parallelo aumento delle infrazioni alle norme sulla tutela dei consumatori. Inoltre è stato evidenziato come i due approcci regolamentari, quello del RGPD e quello relativo alle norme sulla protezione dei consumatori, presentino aree di sovrapposizione e si fondino su principi comuni in materia di trasparenza e corretta informazione, ma al contempo si differenziano, soprattutto per il fatto che il RGPD tutela un diritto fondamentale della persona (non riducibile alla sola veste di consumatore). Pur sussistendo spazi di collaborazione, le due discipline vanno comunque considerate in maniera olistica come idonee a fornire una tutela integrata. Sono stati posti in evidenza i punti di contatto e le differenze tra i due sistemi, sintetizzabili come segue:

- con riguardo alle sanzioni, il sistema di cooperazione per la tutela dei consumatori (CPC), di cui ora al regolamento (UE) 2017/2394, non ne prevede di proprie ma applica quelle previste in ogni Stato membro per la violazione delle disposizioni di competenza;
- sussistono differenze sia nei meccanismi di cooperazione previsti dai due sistemi, sia in relazione ai requisiti necessari per considerare un'infrazione transfrontaliera (coinvolgimento di 2/3 della popolazione UE nel caso del sistema CPC; solamente di due stati membri nel caso del RGPD).

Sono state presentate diverse esperienze nazionali da parte sia di autorità operanti nell'ambito della concorrenza che della protezione dei dati. Per l'Italia, l'Agcm ha presentato il caso Facebook del 2018 e gli esiti della sentenza del TAR di gennaio 2020 (oggetto di conferma da parte del Consiglio di Stato con la sentenza del 29 marzo 2021, n. 2631). Il caso presentato da Agcm ha fornito un esempio del fatto che una medesima condotta – l'uso di dati personali in occasione dell'offerta di un servizio gratuito – è suscettibile di valutazione alla luce di due diversi quadri regolamentari. Tra gli esempi di collaborazione tra autorità, è stato menzionato il rapporto finale dell'indagine conoscitiva sui *big data* condotta congiuntamente da Agcom, Agcm e Garante, pubblicato nel febbraio 2020.

AUDITOR

Il 15 giugno 2020 si è svolto in modalità virtuale il secondo *workshop* sul progetto AUDITOR (*Evaluation and Certification Schemes for Security Products*, consultabile all'indirizzo www.auditor-cert.eu) al fine di coinvolgere sul tema le autorità di protezione dati europee. Si tratta di un progetto, iniziato nel novembre 2017 e finanziato dal Ministero dell'economia ed energia tedesco con l'obiettivo di sviluppare un catalogo di criteri per fornire ai *provider* di servizi *cloud* uno strumento di certificazione volto a dimostrare la *compliance* delle operazioni di trattamento ai requisiti della protezione dei dati personali (RGPD) anche in vista di una sua presentazione quale proposta per un *European Data Protection Seal*. Tale catalogo, sviluppato sulla base del *Trusted Cloud Data Protection Profile Certification* (TCDPPC) e basato sul *Bundesdatenschutzgesetz,* è stato esteso per considerare i requisiti del RGPD oltre a standard internazionali quali ISO 27001, ISO 27002, ISO 27018. Lo *scheme owner* è il *Competence Center Trusted Cloud* e l'oggetto della certificazione è individuato nel "*processing operations of personal data in the context of cloud services*".

21.5. *I progetti per l'applicazione del RGPD finanziati dall'UE: SMEDATA e* twinning *con l'Albania*

SMEDATA

Nel 2020 si è concluso il Progetto SMEDATA, cofinanziato all'80% dalla Commissione europea con l'obiettivo di garantire l'effettiva applicazione del RGPD attraverso la sensibilizzazione, la moltiplicazione della formazione e lo sviluppo soste-

nibile delle capacità per le piccole e medie imprese (Pmi) e le professioni legali (v. anche par. 23.4). Nel corso dell'anno, gli obiettivi di progetto sono stati:

- il *Workshop*, tenutosi il 17 gennaio presso la Facoltà di giurisprudenza di Roma Tre, al fine di testare il contenuto e la funzionalità dell'applicazione mobile "*GDPR in your pocket*";
- la cd. formazione dei formatori (*Training the trainers*), svolta in collaborazione con l'Università degli studi di Roma Tre, mediante due eventi di formazione in videoconferenza gratuiti di alto livello (il 17-18 e il 24-25 settembre) sulle più rilevanti tematiche della protezione dati aventi l'obiettivo di fornire strumenti teorici e pratici completi e aggiornati per quanti svolgono attività di formazione e sensibilizzazione per il personale di piccole e medie imprese. All'iniziativa, che ha visto la partecipazione del vice presidente dell'Autorità, prof.ssa Ginevra Cerrina Feroni, del Componente del Collegio avv. Guido Scorza, di personale del Garante, di docenti dell'Università degli studi Roma Tre e di esperti in ambito *privacy* (complessivamente 21 relatori), hanno partecipato più di 2.000 iscritti. Numerosi i *focus* di approfondimento su temi specifici (come la sicurezza del trattamento, i rischi per i diritti degli interessati, la valutazione d'impatto *privacy*, la gestione dei *data breach*, l'attività ispettiva e sanzionatoria del Garante), alternati alla presentazione di casi pratici;
- la Conferenza internazionale per le Pmi e le loro organizzazioni: più di 280 rappresentanti di piccole e medie imprese ed esperti in protezione dei dati personali hanno preso parte alla Conferenza internazionale finale nell'ambito del progetto SMEDATA, tenutasi *online* il 28 ottobre 2020. L'evento ha presentato i risultati delle attività svolte nell'ambito del progetto, volto a sensibilizzare i rappresentanti delle Pmi sulla protezione dei dati personali. Sono state anche discusse le attuali sfide al trattamento dei dati personali, compresi gli aspetti imposti dalla pandemia Covid-19. La Conferenza è stata aperta dalla vice presidente del Garante prof.ssa Ginevra Cerrina Feroni, dal presidente del CPDP, sig. Ventsislav Karadjov, e dal prof. Luca Pietromarchi, Rettore dell'Università Roma Tre. La Conferenza comprendeva quattro *panel*, ai quali hanno partecipato relatori internazionali, sui seguenti argomenti:
- l'esperienza del progetto SMEDATA: risultati dell'attività di sensibilizzazione e di moltiplicazione della formazione sul RGPD per le Pmi;
- il trattamento dei dati personali nelle Pmi, anche alla luce dei requisiti imposti dalla pandemia Covid-19: esperienze a confronto;
- buone pratiche per il corretto trattamento dei dati personali da parte delle Pmi;
- pseudonimizzazione, sicurezza e *data breach*.

Gemellaggio con l'Albania

Il Garante, con il coinvolgimento della *Ludwig Boltzmann Gesellschaft - Institute of Human Rights* (BIM) (in qualità di *junior partner*) e Csi-Piemonte (Consorzio per il sistema informativo), è impegnato quale *leader* del progetto della durata annuale iniziato nell'ottobre 2020 in un gemellaggio (*Twinning*) che ha come beneficiario l'*Information and Data Protection Commissioner* albanese. L'obiettivo generale del progetto consiste nel rafforzare la capacità dell'Autorità di controllo albanese nell'assolvimento dei suoi compiti sia nel settore pubblico che in quello privato; quello specifico è di supportare l'Autorità di controllo albanese e allineare ulteriormente la legislazione nazionale (in particolare la legge n. 9887/2008 sulla protezione dei dati personali, nel testo vigente) con l'*acquis* dell'Unione nel settore della protezione dei dati personali. Il progetto è suddiviso in tre componenti, ciascuna delle quali coordinata da un membro del Consorzio, concernenti l'allineamento della legislazione nazionale con il RGPD e la direttiva 680/2016, nonché un'intensa attività di for-

21

mazione e sensibilizzazione del personale dell'Autorità di protezione dati albanese.

Ancorché i gemellaggi – finanziati dall'UE con l'obiettivo di carattere generale di assicurare uno sviluppo moderno ed efficiente delle amministrazioni dei Paesi beneficiari – siano normalmente svolti attraverso missioni degli esperti effettuate nella sede del beneficiario, la situazione di emergenza sanitaria ha determinato lo svolgimento delle attività da remoto.

22 L'attività di normazione tecnica internazionale e nazionale

Collaborazione con organismi di standardizzazione

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 ha seguito gli aspetti di sicurezza nella gestione delle identità relativamente alle tecnologie biometriche e alla protezione dei dati personali. Armonizzando la propria posizione con quelle delle altre autorità di protezione dati tramite il Cepd, che ha una *liason* in proposito con ISO, l'Autorità ha seguito lo sviluppo delle norme tecniche di seguito riportate:

- 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 e di requisiti di implementazione, nonché si soffermano su processi e responsabilità;
- ISO 27556 - *User-centric framework for the handling of PII based on privacy preference*, che definisce un quadro di riferimento per la gestione delle scelte riguardanti le informazioni personali con un approccio *user-centric*;
- ISO TS 27006 - *Requirements for bodies providing audit and certification of privacy information management systems according to ISO/IEC 27701 in combination with ISO/IEC* 27001, che definisce requisiti aggiuntivi alla ISO 17021 e 27006 per gli organismi di certificazione che e svolgono *audit* e rilasciano certificazioni secondo la nuova ISO 27701 (*Privacy Information Management System*);
- ISO TS 27559 - *Privacy enhancing data de-identification framework*, che fornisce una guida sull'implementazione della de-identificazione e la valutazione dei rischi di reidentificazione e relativi al ciclo di vita dei dati de-identificati;
- ISO 27557 - *Organizational privacy risk management*, che fornisce linee guida per la gestione del rischio *privacy* delle organizzazioni titolari e responsabili del trattamento integrando la valutazione dell'impatto sugli interessati nel *privacy risk management program* delle medesime;
- ISO TS 27560 - *Consent Receipt and Record Standard*, che definisce una struttura e formato comune per *consent receipt* e *consent record*.

Collaborazione è stata assicurata nell'ambito del *Project Committee* (PC) 317 di ISO, istituito dal *Technical Management Board* a febbraio 2018, per lo sviluppo di una norma tecnica internazionale su *Consumer protection: Privacy by design for consumer goods and services* e nell'ambito del comitato tecnico 215 di ISO durante i lavori dell'*Ad Hoc Group Application of AI Technologies* in *Health Informatics* e per la stesura del *report* conclusivo.

L'Autorità ha continuato a collaborare all'elaborazione di norme tecniche europee nell'ambito del comitato tecnico JTC13 del CEN CENELEC che si occupa di *Data Protection, Privacy and Identity Management.*

Del pari, è stato seguito lo sviluppo delle norme tecniche di seguito riportate:

- EN 17529 - *Privacy Protection by design and by default*, 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,* con i relativi rapporti tecnici *Privacy management in products and services – Biometric for access control including face recognition e Privacy management in products and services – Videosurveillance products and services;*
- *Personal data protection requirements for processing operations*, basato sulla prassi di riferimento UNI 43.2:2018 *"Guideline for personal data management within ICT according to Regulation EU 679/2016 (GDPR) - Requirements for the protection and conformity assessment of personal data within ICT"* riguarda il tema della standardizzazione a supporto dell'articolo 42 del RGPD;
- *Requirements for professional profiles related to personal data processing and protection*, basato sulla norma UNI 11697, definisce requisiti armonizzati a livello europeo e in accordo con il *European Qualifications Framework* (EQF) dei professionisti che svolgono attività nell'ambito del trattamento e della protezione dati personali.

Infine, prosegue la proficua collaborazione con le diverse commissioni tecniche UNINFO (Ente Nazionale di Normazione per le Tecnologie e loro Applicazione), l'Ente di normazione federato all'Uni (Ente nazionale italiano di unificazione).

23 L'attività di comunicazione, informazione e di rapporto con il pubblico

23.1. *La comunicazione del Garante: profili generali*

In un anno segnato dalla pandemia, l'attività di comunicazione si è concentrata sui numerosi pareri che l'Autorità è stata impegnata a rendere, in tempi rapidissimi, sulle misure di contenimento del contagio, al fine di assicurare che il trattamento dei dati, in particolare di quelli sulla salute, avvenisse nel rispetto delle persone. In tale categoria rientrano i diversi provvedimenti adottati sul sistema di tracciamento dei contagi (*app* Immuni); sui test sierologici; sulla raccolta dei dati sanitari di dipendenti e clienti; sulla raccolta dei rifiuti Covid-19; sulla ricetta elettronica; sulla sperimentazione clinica e sulla ricerca medica. L'attività di comunicazione del Garante ha riguardato anche gli effetti che l'emergenza sanitaria ha determinato sulla collettività, dal ricorso ai sistemi di didattica a distanza, al lavoro agile, al processo penale, amministrativo e tributario telematico.

Attraverso tutti i provvedimenti adottati nel corso dell'anno, ed in sintonia con le altre autorità europee, il Garante ha ricercato sempre un giusto bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali.

In questo scenario pandemico, in cui la tutela del diritto alla protezione dei dati personali è diventata ancora più cruciale, l'azione di comunicazione istituzionale del Garante è stata ulteriormente potenziata. Per aiutare singoli, imprese, enti, pubbliche amministrazioni e *mass media* ad attuare le numerose misure anti-Covid-19, che hanno avuto impatto sul diritto alla protezione dei dati personali, è aumentata la produzione di schede informative e *vademecum*. A tutti gli interventi del Garante è stata data grande visibilità, anche grazie al rafforzamento della presenza sui *social media* e alla sperimentazione di nuovi contenuti e canali multimediali, con particolare attenzione alla realizzazione di campagne e prodotti video destinati al web. Continui i contatti con i *media* nazionali e, in misura crescente, con quelli stranieri, per assicurare una compiuta interpretazione dei provvedimenti adottati dall'Autorità, fornire risposte e materiale documentale. Rilevante è stata anche l'attività di scrittura di comunicati stampa condivisa con il Comitato e altre autorità di protezione dei dati nonché la gestione comune dei casi di valenza transnazionale.

Con la diffusione della pandemia da Covid-19 si è registrato un incremento dell'attività di *cybercrime* in tutto il mondo, con una particolare diffusione di attacchi *ransomware*. Lo stesso ricorso massivo al lavoro agile, alla didattica a distanza, alla telemedicina, al commercio elettronico ha accresciuto enormemente la quantità dei dati personali in rete. Secondo gli esperti il 2020 è stato un *annus horribilis* a causa degli attacchi alle infrastrutture strategiche e verso il settore della ricerca e delle istituzioni scolastiche, registrando anche un incremento degli attacchi rivolti alle stesse istituzioni governative.

Sul tema della cybersicurezza il Garante ha svolto un'intensa attività di informazione e prevenzione concentrando il proprio impegno sulle diverse forme di *cybercrime:* dal *ransomware* al furto d'identità, dalle frodi informatiche, come il *phishing*, alle intrusioni informatiche e alle violazioni di dati (*data breach*). E proprio *di cybercrime*, prevenzione contro gli attacchi informatici e tutela dei diritti fondamentali di fronte alle forme sempre più evolute di sorveglianza massiva da parte dei governi, si

23

è discusso a gennaio, al convegno intitolato "Spazio cibernetico bene comune: protezione dei dati, sicurezza nazionale", organizzato in occasione della Giornata europea per la protezione dei dati personali.

L'attività di divulgazione dell'Autorità ha promosso l'uso trasparente degli algoritmi e la limitazione nell'utilizzo dei dati biometrici, segnalando i gravi rischi e le criticità derivanti dalle derive autoritarie nelle raccolte massive di dati, anche attraverso *app*, nonché l'influenza negativa delle *fake news* sulla vita delle democrazie.

Da sempre impegnata a garantire la massima tutela ai minori, anche *online*, l'Autorità ha seguito con particolare attenzione il rapporto tra minori e *social network*, con speciale riguardo a TikTok, la piattaforma di video *sharing* usata da milioni di utenti, in gran parte giovanissimi (alla quale ulteriore risonanza ha dato il tragico evento che ha visto coinvolta la bambina di Palermo). Il Garante ha chiesto e ottenuto la costituzione di una specifica *task force* nell'ambito del Comitato (doc. web n. 9249688), segnalando le vulnerabilità del *social network*. Successivamente è stato avviato un procedimento formale nei confronti di TikTok, con la contestazione di una serie di violazioni e l'adozione di un provvedimento d'urgenza, ai sensi dell'art. 66 del RGPD contenente un ordine di limitazione del trattamento dei dati personali degli utenti di cui non è possibile accertare l'età ex art. 58, par. 2, lett. *f*), del RGPD (cfr. par. 9.4).

Sempre sul fronte dei *social network*, il Garante è intervenuto su altri rischi legati al cyberbullismo e al *sexting* come pure su fenomeni particolarmente pericolosi quali il *deepfake*, il *revenge porn* e l'*hate speech*, richiamando alla necessità di un uso responsabile della rete e dello sviluppo di un'educazione digitale in grado di rendere tutti, adulti e giovani, consapevoli delle grandi opportunità, ma anche dei rischi che caratterizzano la dimensione digitale.

Nell'attività di divulgazione non sono stati tralasciati altri importanti ambiti: il *telemarketing* selvaggio, da tempo ormai nella lente dell'Autorità; i *cookie*; la conservazione dei dati di traffico telefonico e telematico (*data retention*); il trasferimento dei dati tra l'Unione europea e gli Stati Uniti dopo la sentenza della CGUE cd. Schrems II; il contrasto all'evasione fiscale; il reddito di cittadinanza; il *bonus* Covid; la sanità digitale; il *whistleblowing*; il mondo del lavoro; il censimento permanente della popolazione; i sistemi di videosorveglianza; la scuola; il giornalismo.

A febbraio è stato pubblicato il Rapporto finale dell'indagine conoscitiva sui *big data*, che il Garante ha condotto congiuntamente ad Agcom e Agcm. La ricerca ha approfondito, anche attraverso audizioni e richieste di informazioni a imprese, associazioni di categoria ed esperti della materia, i cambiamenti derivanti dal ricorso ai *big data* sugli utenti che forniscono i dati, sulle aziende che li utilizzano e, dunque, sui mercati. Il Rapporto è suddiviso in cinque capitoli più uno conclusivo; il quarto riporta la posizione del Garante sul possibile impatto derivante dall'utilizzo dei *big data* sul diritto alla protezione dei dati personali e sulle misure e cautele da adottare; il testo integrale è consultabile sul sito web anche in versione inglese (doc. web n. 9264297).

A marzo 2020 sono stati pubblicati i risultati del *Privacy Sweep* 2019; l'indagine annuale del *Global Privacy Enforcement Network* (GPEN) si è concentrata sulla gestione dei *data breach* da parte di soggetti pubblici e privati con il coinvolgimento di 16 autorità di protezione dei dati, tra le quali il Garante. Dall'indagine, che ha preso in esame diversi aspetti della violazione dei dati personali, ivi compresa la gestione delle notifiche e l'implementazione di misure volte a prevenire il ripetersi della violazione, è emerso che, riguardo alla gestione dei *data breach*, ci sia una conoscenza approfondita, ma limitata a pochi organismi.

Sempre riguardo ai *data breach*, il Garante ha reso disponibile sul proprio sito una pagina tematica, con indicazioni normative, schede informative e documentazione

di approfondimento, finalizzata a chiarire gli aspetti principali sull'adempimento previsto dal RGPD e contenente istruzioni per procedere alla notifica attraverso il servizio telematico predisposto dall'Autorità (https://www.garanteprivacy.it/regolamentoue/databreach).

È proseguita l'attività svolta nell'ambito della rete di comunicatori del Comitato, istituita per assicurare una coordinata attività di comunicazione tra i Paesi dell'UE. Si è partecipato alla definizione e alla realizzazione del *corporate video* del Comitato e alla scrittura di schede informative specifiche come le FAQ relative all'art. 65 del RGPD, prima nella versione comune in lingua inglese e quindi nella traduzione italiana. Si è partecipato alla stesura del piano di comunicazione (EDPB 2020 *Comms Plan*) e alla definizione di regole di comunicazione condivise tra le autorità, al fine di affrontare in maniera coordinata e collaborativa anche casi di comunicazione di crisi, qualora sussistano posizioni divergenti su temi rilevanti di carattere transfrontaliero.

Nell'ambito del gruppo di comunicazione del Cepd, l'Autorità ha partecipato al gruppo ristretto del *Data Protection Day Taskforce* per lo sviluppo condiviso di iniziative comuni su scala europea da lanciare in occasione della Giornata europea della protezione dei dati personali 2021. Tale collaborazione ha portato alla realizzazione di un video istituzionale multilingua utilizzato dal Cepd e dalle singole autorità nazionali. Sono stati inoltre forniti numerosi aggiornamenti, con informazioni sia puntuali sia di carattere statistico, sull'attività del Garante, così da consentire un'attività di comparazione del lavoro tra le autorità europee e assicurare una più efficace collaborazione sui settori critici.

Allo scopo di sensibilizzare la comunità sulle tematiche della protezione dei dati e della *privacy*, per spiegare il valore dei dati e l'importanza di proteggerli nonché illustrare il ruolo dell'Autorità, il Garante ha inaugurato una nuova e più emozionale forma di comunicazione realizzando un video istituzionale dal titolo "I tuoi dati sono un tesoro", andato in onda sulle reti televisive e reso disponibile sui *social media*.

Largo spazio è stato dedicato dai *media* all'attività del Garante. Il Servizio relazioni con i mezzi di informazione ha selezionato oltre 59.000 articoli nazionali di interesse dell'Autorità e 2.300 articoli provenienti da testate e siti web esteri. Dalla rassegna stampa elaborata quotidianamente è emerso che 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 16.590, delle quali 6.234 dedicate esclusivamente all'attività dell'Autorità.

Il 2020 è stato anche l'anno in cui il Garante ha rinnovato la sua immagine coordinata e adottato un nuovo logo per raccontare un passaggio decisivo nel ruolo che è chiamato a svolgere nel nostro Paese: quello di una Istituzione sempre più strategica, dinamica e operativa in un mondo in cui i dati e la rete sono gli elementi cardine di ogni attività e in cui la persona appare sempre più esposta e vulnerabile. Il nuovo logo vuole rappresentare graficamente l'innovazione nella continuità: l'acronimo GPDP per rendere immediatamente associabile l'Autorità al suo nome ufficiale; un linguaggio più distintivo, caratterizzato dal simbolo del *pixel* all'interno delle lettere "G" e la "D" che riconduce immediatamente al mondo digitale; un *design* tipografico forte e moderno che denota la capacità di intervenire nei processi di cambiamento in atto.

23.2. *I prodotti informativi*

Nell'anno sono stati diffusi 54 comunicati stampa e 11 *Newsletter* e sono state trasmesse 11 puntate della rubrica "Il Bollettino del Garante della *Privacy*", in onda

su Radio Radicale, contributo informativo che illustra i principali provvedimenti adottati dal Garante e, più in generale, le tematiche legate alla protezione dei dati personali (cfr. parte IV, tab. 2). La *Newsletter* del Garante, giunta al XXII anno di diffusione (per un totale di 471 numeri e di 1.607 notizie), è stata rinnovata nella sua veste grafica. Nata in forma cartacea, oggi è inviata esclusivamente via *e-mail* a redazioni, professionisti, amministrazioni pubbliche, imprese e singoli 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 circa 15.000 destinatari effettivi. La *Newsletter* continua a costituire un valido strumento funzionale alla divulgazione dei più importanti provvedimenti adottati dall'Autorità, alla sua attività in ambito nazionale, 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, la redazione opera una scelta e rielabora in chiave giornalistica quelli di maggiore interesse generale. Nel corpo di ciascuna notizia sono inseriti *link* che rimandano direttamente ai provvedimenti citati, facilitando così l'approfondimento dell'argomento trattato. Ogni numero della *Newsletter* è composto da 3-4 notizie che, nella versione *online*, sono corredate da immagini illustrative. Sul sito è possibile consultare l'archivio tematico che raccoglie i 22 anni di articoli prodotti dalla redazione nonché l'archivio dei comunicati stampa.

23.3. *Il sito istituzionale, i prodotti multimediali e le pubblicazioni*

La nuova *corporate identity* del Garante adottata nel 2020 è parte di una serie di iniziative di comunicazione che prevede, nel 2021, il lancio di un sito web rinnovato e l'impiego di nuovi strumenti, linguaggi, contenuti e canali per raggiungere la comunità e supportare l'azione dell'Autorità, nello spirito del nuovo Regolamento europeo, che vede nella comunicazione e nell'informazione un elemento fondamentale dell'azione di tutela dei dati personali.

È stato portato a termine il progetto di revisione completa del *thesaurus* tematico del sito web del Garante per aggiornare le voci alle novità normative e tecnologiche, riorganizzarle e ridurne il numero, allo scopo di migliorare le *performance* della ricerca.

Nell'anno è stato ulteriormente incrementato il numero delle notizie e dei prodotti grafici e multimediali da destinare alla diffusione sul web e sui canali *social* istituzionali del Garante aperti su Linkedin, YouTube, Telegram e Instagram. In particolare, è proseguita 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 oltre 49.000 *follower.* Sul *social network* Youtube le visualizzazioni complessive hanno raggiunto quota 409.000.

Per le sue campagne informative, il Garante ha ideato e realizzato prodotti di-

vulgativi con contenuti caratterizzati da chiarezza e sinteticità espressiva, grafica innovativa e forte vocazione *social*, che rappresentano un canale comunicativo che il Garante privilegia per veicolare le informazioni. Sono stati realizzati 7 *vademecum* digitali pubblicati e diffusi sui *social* (dedicati al *phishing*, al *deepfake*, alle *app*, alle foto e ai filmati *online*, al *ransomware*, al Covid-19) e 3 infografiche (dedicate al bilancio sull'applicazione del RGPD, alle novità sul Fascicolo sanitario elettronico, al *ransomware*).

Numerose anche le sezioni e le pagine tematiche del sito create o totalmente ristrutturate con interventi su contenuti, grafica, usabilità e organizzazione dei contenuti: coronavirus e protezione dei dati; uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza da Covid-19; Fascicolo sanitario elettronico; riconoscimento facciale; *wearable device*; referti *online; dossier* sanitario; *ransomware; phishing*; pseudonimizzazione; diritto all'oblio; *fintech*; IoT; cyberbullismo; videosorveglianza; intelligenza artificiale; *big data; app; cookie; cybersecurity; deepfake; telemarketing*.

Numerose e molto apprezzate le pagine FAQ messe a punto dal Garante sulle problematiche connesse all'emergenza sanitaria in vari ambiti (sanità, lavoro, scuola, ricerca, enti locali) predisposte per chiarire dubbi e fornire indicazioni sintetiche per un corretto trattamento dei dati personali da parte di pubbliche amministrazioni.

Nella parte finale dell'anno, il Garante ha varato una nuova serie di prodotti informativi che affrontano, con un linguaggio semplice, il tema del diritto di accesso. L'iniziativa fa parte di un più ampio progetto dell'Autorità, che punta ad offrire strumenti per comprendere facilmente quali diritti sono riconosciuti alle persone in materia di protezione dei dati personali e ad illustrare le modalità per un concreto esercizio di tali diritti. Le schede prodotte saranno pubblicate sul sito internet del Garante alla pagina https://www.garanteprivacy.it/home/diritti.

Riguardo alla produzione editoriale è stato pubblicato in versione *online* il volume "Spazio cibernetico bene comune: protezione dei dati, sicurezza nazionale" (doc. web n. 9251880), che raccoglie i contributi degli studiosi e degli esperti intervenuti al Convegno organizzato dall'Autorità in occasione della celebrazione della XIV Giornata europea per la protezione dei dati personali, svoltosi quest'anno in modalità *streaming*.

In collaborazione con l'*International Association of Privacy Professionals* (IAPP), è stato pubblicato il volume "*Privacy* 2030. Una nuova visione per l'Europa" (doc. web n. 9457003), che raccoglie le riflessioni e gli appunti del consigliere Giovanni Buttarelli, già Segretario generale dell'Autorità e poi Garante europeo della protezione dei dati, prematuramente scomparso nel 2019. Edito in formato elettronico, *Privacy* 2030 costituisce il testamento spirituale di uno dei pionieri della protezione dati contenente un forte richiamo a trasformare un diritto del singolo in un diritto collettivo, in grado di fare la differenza nelle sfide sociali, culturali, politiche e ambientali che ci attendono o che si vanno configurando.

Buttarelli si chiede, e ci chiede, come rendere possibile un nuovo umanesimo tecnologico e combattere il culto della massimizzazione dei dati; attraverso questi interrogativi, intendeva stimolare un ampio dibattito pubblico che non fosse limitato ai giuristi e alle autorità di protezione dati. Per questo la pubblicazione, che si apre con la prefazione del Presidente del Garante, si compone di due sezioni distinte: l'una basata sugli scritti e le riflessioni di Buttarelli, che si conclude con una sorta di decalogo per la *privacy* del nuovo decennio; l'altra, fondata su contributi di studiosi di fama ed esperti internazionali (fra cui Marc Rotenberg, il fondatore dell'*Electronic Privacy Information Center*, e Shoshana Zuboff, studiosa e autrice di un recente saggio sul Capitalismo della sorveglianza), i quali partono dal pensiero e dalle proposte

di Buttarelli per elaborare un'analisi più ampia sui rischi per libertà e diritti nell'epoca del digitale e sulle soluzioni possibili o auspicabili.

23.4. *Manifestazioni e convegni*

La campagna di comunicazione ha accompagnato l'attività di formazione svolta nell'ambito del progetto SMEDATA (cfr. par. 21.5) – co-finanziato da fondi della Commissione europea e nato nel 2018 da una *partnership* tra il Garante, il Dipartimento di giurisprudenza dell'Università degli studi Roma Tre e l'Autorità per la protezione dati della Bulgaria – che si è concluso il 28 ottobre 2020, con una conferenza internazionale i cui lavori sono accessibili sul canale Youtube dell'Autorità (all'indirizzo https://www.youtube.com/watch?v=I9hp3RBh8M4&t=68s).

Con l'obiettivo di riportare al centro dell'attenzione la funzione dell'informativa relativa al trattamento dei dati personali, il Garante ha deciso di patrocinare e promuovere, nell'ambito del primo *legal hackathon* italiano *online* lanciato da *Legal Hackers* Roma, una sfida, aperta alla partecipazione di chiunque abbia le necessarie competenze giuridiche e di *design*. La competizione ha avuto come oggetto quello di ridurre, di almeno il 50%, la lunghezza delle cd. informative *privacy* di una qualsiasi delle grandi piattaforme *social* e web, anche utilizzando icone, simboli e altre soluzioni grafiche. *HacktheDoc* si è svolto *online* dal 10 al 12 dicembre.

Numerose anche le partecipazioni del Presidente e dei Componenti a convegni ed eventi di rilievo nazionale e internazionale. Tra le più importanti, il 15 maggio 2020, Antonello Soro, presidente del Garante in carica fino al 28 luglio 2020, è intervenuto al *webinar* organizzato dall'Università degli studi di Perugia su "Emergenza coronavirus: spunti per un bilanciamento tra tutela della salute e garanzia delle libertà fondamentali", soffermandosi sulle caratteristiche del sistema di *contact tracing* italiano e sul contributo dell'Autorità nel procedimento legislativo al fine di garantire il rispetto dei diritti e delle libertà individuali.

Il nuovo presidente del Garante, Pasquale Stanzione, partecipando il 13 novembre al "Premio Vincenzo Dona 2020: *What's next"*, ha sottolineato che sulla sinergia tra salute, innovazione e *privacy* si giocherà una sfida sempre più determinante per la nostra società e che dobbiamo impegnarci a vincere nel segno, ancora una volta, della centralità della persona e della sua dignità. Al convegno "Banche e sicurezza", organizzato dall'Abi il 2 dicembre, il presidente Stanzione ha evidenziato il ruolo della protezione dati che, ostacolando le condizioni per la concentrazione del potere, non solo informativo, si è dimostrata una valida alleata tanto della disciplina consumeristica quanto di quella concorrenziale. Alla 15ª edizione del *Consumers' Forum Workshop*, tenuto il 9 dicembre sul tema "*LockUp Economy* e cittadini. Mercati e regole al tempo della pandemia, tra sostenibilità e solidarietà", il Presidente del Garante ha ribadito l'importanza dell'educazione digitale, un necessario presupposto di scelte libere e consapevoli, tanto difficili quanto indispensabili al tempo della *zero-price economy*, in cui servizi apparentemente gratuiti sono invece pagati al caro prezzo dei dati personali e, quindi, della libertà individuale. Al *web event*, organizzato in collaborazione con Il Sole 24 Ore Eventi-Radiocor, hanno partecipato le maggiori *Authority* italiane.

Il 12 novembre, la vice presidente Ginevra Cerrina Feroni è intervenuta nel ciclo di *webinar* organizzati dalla Fondazione Centro di iniziativa giuridica Pietro Calamandrei "Verso il *Digital Services Act* - Dialoghi sul futuro dei servizi digitali", e il 14 dicembre, sempre in *streaming*, ha partecipato al Seminario italo-spagnolo V Congresso internazionale, presiedendo la sessione "Il cittadino e le innovazioni: i

diritti nella società digitale".

Agostino Ghiglia, componente del Garante, ha aperto il *webinar* "Le novità che impattano nel futuro delle imprese", organizzato da Associazione ICT Dott Com – *Privacy* & GDPR il 20 novembre, illustrando il ruolo dell'Autorità nel rapporto con le imprese ed i professionisti.

Nell'ambito della settimana dell'Internet *Governance Forum* Italia, Youth IGF Italy, Guido Scorza, componente del Garante, è intervenuto il 7 e il 9 ottobre, nella sessione dedicata a "La Carta dei diritti di Internet" e al *Report "The Age of Interdependence.* Principi e sfide", soffermandosi, a conclusione dei lavori, sul concetto di *privacy*. Il 9 dicembre Scorza ha partecipato anche all'Internet Festival di Pisa, dedicato quest'anno a "Il mondo digitale tra codice informatico e regole giuridiche", intervenendo nel dibattito su "L'uomo e la macchina tra *data protection* e *contact tracing*", mentre dal 10 al 12 dicembre ha preso parte all'evento *HacktheDoc*, primo *hackathon online* di *legal design* lanciato con l'obiettivo di rendere le *privacy policy* qualcosa che tutti possano leggere e capire.

23.5. *L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi*

L'Autorità ha svolto la propria attività di assistenza al pubblico, per il tramite dell'Urp, continuando a promuovere la conoscenza e la crescita della consapevolezza in merito alle tematiche connesse alla disciplina sulla protezione dei dati personali. Notevole è stato l'incremento delle richieste di chiarimento ricevute, a conferma dell'attenzione nei confronti delle questioni afferenti ai trattamenti di dati personali nei diversi contesti, in particolare in quello sanitario, maggiormente interessato dalle misure disposte dalle pubbliche autorità ai fini del contenimento dell'emergenza sanitaria da Covid-19.

La situazione pandemica ha influito, oltre che sull'entità e sull'oggetto delle istanze pervenute, anche sulle modalità di assistenza al pubblico che, a partire dagli inizi di marzo, nel rispetto della normativa emergenziale, è stata fornita esclusivamente tramite i canali telefonico e telematico, essendo stata preclusa l'attività di ricevimento degli utenti presso la sede del Garante.

Ai fini del potenziamento degli strumenti informativi a disposizione del pubblico, sono state predisposte FAQ in materia di videosorveglianza (https://www.garanteprivacy.it/faq/videosorveglianza) allo scopo di fornire chiarimenti sulla disciplina applicabile ai trattamenti a vario titolo effettuati mediante l'uso di videocamere, chiarimenti da più parti richiesti anche in considerazione del tempo trascorso dall'adozione provvedimento generale adottato in materia (provv. 8 aprile 2010, doc. web n. 1712680).

Allo stesso scopo, l'Urp ha realizzato e messo a disposizione sul sito web dell'Autorità quattro schede relative ad altrettante differenti tipologie di accesso ai dati personali e un modello per le richieste di accesso al Garante ex art. 22 e ss., l. n. 241/1990.

Le comunicazioni e i quesiti pervenuti hanno avuto ad oggetto molteplici questioni riguardanti la normativa in materia di protezione dati e, in particolare, come si è detto, il tema del bilanciamento tra la protezione dei dati personali e la tutela della salute nell'ambito delle misure disposte dalla normativa emergenziale. La grande attenzione dell'opinione pubblica rispetto a tali temi è dimostrata dai dati numerici relativi alle richieste pervenute (cfr. parte IV, tab. 15 e 16), che ammontano in totale a 15.040, delle quali 10.695 via *e-mail* e 3.981 tramite telefono (32 sono stati i visitatori ricevuti sino al 10 marzo e 332 i *dossier* esaminati). Nella gestione di tali

richieste, l'Ufficio ha avuto cura di conciliare l'efficienza, la professionalità e una aggiornata conoscenza delle implicazioni di natura giuridica delle questioni esaminate, operando da "filtro" rispetto alle altre unità organizzative dell'Autorità.

Tematiche d'interesse

Tra le tematiche di carattere generale sottoposte all'Urp si segnalano in primo luogo quelle concernenti gli adempimenti introdotti dal RGPD (circa 2.160 *e-mail* ricevute, delle quali circa 1.500 hanno riguardato la designazione del Responsabile della protezione dei dati e la procedura *online* realizzata dal Garante per la comunicazione dei dati di contatto dello stesso).

Altre questioni oggetto di interesse hanno riguardato i trattamenti di dati personali per finalità di *direct marketing* (oltre 950 *e-mail*) e, in particolare, di *telemarketing* (530 *e-mail*); la videosorveglianza in ambito privato, lavorativo e scolastico (oltre 340 *e-mail*); l'accesso ai dati bancari (oltre 620 *e-mail*) e la tutela degli interessati in relazione ai trattamenti effettuati dai sistemi di informazione creditizia (192 *e-mail*); ulteriori ambiti di interesse sono rappresentati dai trattamenti di dati personali effettuati in internet, nei *social network*, tramite le *app*, nonché in ambito giornalistico, con particolare riferimento alle richieste di deindicizzazione dei dati personali dai motori di ricerca volte all'esercizio del cd. diritto all'oblio di cui all'art. 17 del RGPD (in totale 928 *e-mail*).

Il maggior numero delle richieste pervenute ha riguardato la tutela dei dati personali nei diversi ambiti economico-sociali interessati dalle misure previste dai decreti adottati al fine di contrastare l'emergenza da Covid-19. In tale contesto si segnalano, in particolare, le istanze relative al rispetto della normativa in materia di protezione dei dati personali con riferimento alla attribuzione dei contributi economici (in particolare, dei cd. buoni spesa) da parte dei comuni ai soggetti in condizioni di disagio economico.

L'Urp si è occupato del tema dell'erogazione da parte dell'Inps dei cd. *bonus* Covid a sostegno del reddito, questione esaminata dal Garante con riguardo alle violazioni dei dati personali verificatesi in occasione dell'avvio delle procedure per la richiesta di erogazione dei suddetti *bonus* nei confronti di un numero rilevante di beneficiari che hanno tentato di accedere contemporaneamente ai servizi *online* erogati tramite il portale dell'Inps, determinandone il blocco. Numerosi i reclami e le segnalazioni pervenuti che, da un lato manifestavano le proprie preoccupazioni sulla tutela dei diritti e delle libertà delle persone coinvolte nel *data breach*, dall'altro segnalavano di aver visualizzato in prima persona dati di terzi. La medesima vicenda è stata poi oggetto di numerose richieste di informazioni in relazione agli articoli di stampa apparsi nel mese di agosto, dai quali è emerso che il *bonus* Covid per lavoratori autonomi e "partite Iva" era stato richiesto (e in alcuni casi ottenuto) anche da alcuni parlamentari e amministratori locali, profili sui quali l'Ufficio ha condotto accertamenti istruttori (cfr. cap. 16).

L'attenzione dell'Ufficio, anche alla luce della sentenza della CGUE 16 luglio 2020 (cd. Schrems II) sul regime di trasferimento dei dati tra l'UE e gli USA, si è incentrata sui trattamenti in ambito scolastico – con particolare riguardo ai trattamenti dei dati personali riferiti a studenti, docenti e famiglie effettuati mediante piattaforme digitali per la didattica a distanza – nonché sulle richieste (indirizzate dagli istituti scolastici ai genitori degli alunni) volte a sottoscrivere i patti di corresponsabilità per la tutela della salute in ambito scolastico come pure sulle implicazioni sui diritti individuali delle misure destinate al contenimento del Covid (quali la misurazione della temperatura dei minori e la sottoposizione degli stessi ai cd. tamponi). Le questioni più delicate hanno riguardato i trattamenti dei dati relativi alla salute, inevitabilmente correlati alle misure di contrasto dell'emergenza sanitaria, ad esempio quelle previste dal Protocollo condiviso del 14 marzo 2020 (ed aggiornato

il successivo 24 aprile), nonché dalle linee guida per la riapertura delle attività economiche, produttive e ricreative dell'11 giugno 2020 (all. 9 al d.P.C.M. 11 giugno 2020), in merito alle quali sono pervenute circa 600 *e-mail*.

Particolarmente numerose le richieste di verifica del rispetto della disciplina di protezione dei dati personali nel contesto dei sistemi di tracciamento dei contatti finalizzati al contrasto della diffusione del Covid-19, sia nazionale realizzato mediante l'*app* Immuni, sia in ambito regionale con proprie *app*.

Frequenti sono stati i chiarimenti relativi alla sospensione dei termini dei procedimenti dinanzi al Garante fino al 15 maggio 2020 ai sensi dell'art. 103, d.l. 17 marzo 2020, n. 18, come modificato dall'art. 37, d.l. 8 aprile 2020, n. 23 (provv. 30 aprile 2020, n. 80, doc. web n. 9333182).

24 Studi e documentazione

Studio, documentazione e supporto giuridico

L'attività di studio e ricerca si è incentrata su molteplici questioni tecnico-giuridiche di attualità – in particolare occasionate dalla pandemia, sia in relazione al trattamento dei dati connesso all'utilizzo di piattaforme di *e-learning*, sia alle implicazioni correlate all'art. 14, d.l. n. 14/2020 con riguardo al trattamento dei dati sanitari nonché (più in generale) sulle materie di interesse dell'Autorità, anche oggetto di rinvio pregiudiziale alla Corte di giustizia dell'Unione europea (cfr. Causa C-184/20, C-245/20, C-534/20 e Cause riunite C-339/20 e C-397/20) o di procedure di infrazione (cfr. PI 2020/4051).

Approfondimenti mirati sono stati dedicati all'evoluzione della giurisprudenza della Corte costituzionale tedesca in materia di diritto alla protezione dei dati personali come pure al tema del trattamento dei cd. dati di traffico, oggetto di plurime domande di decisione pregiudiziale indirizzate alla Corte di giustizia che, proprio nel 2020, è tornata a pronunciarsi sulla materia: in particolare con le sentenze della Grande Camera del 6 ottobre 2020 (C-623/17, Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e Cause riunite C-511/18, La Quadrature du Net and Others; C-512/18, French Data Network and Others e C-520/18, Ordre des barreaux francophones et germanophone and Others), nelle quali, ripercorrendo largamente le argomentazioni formulate in precedenza (nelle sentenze dell'8 aprile 2014, Digital Rights Ireland e a., del 21 dicembre 2016, Tele2 Sverige e Watson e a. e del 2 ottobre 2018, Ministerio Fiscal), è stata ribadita la illiceità delle pratiche concernenti la conservazione massiva delle informazioni sul traffico e sull'ubicazione relative alle comunicazioni elettroniche in vista del loro utilizzo per finalità di polizia e *intelligence*: orientamento da ultimo oggetto di conferma nella sentenza del 2 marzo 2021, C-746/18, H. K./Prokurator, che presenta profili ulteriori, anch'essi di interesse per l'ordinamento nazionale (in merito v. già i rilievi del Garante sintetizzati nella Relazione 2018, p. 18 e 21 e nella segnalazione a Parlamento e Governo del 22 dicembre 2017, doc. web n. 7464029).

Costante attenzione è stata infine prestata agli sviluppi (giurisprudenziali e dottrinali) concernenti l'istituto dell'accesso civico generalizzato – profilo rispetto al quale anche l'Autorità è chiamata a fornire riscontro su sollecitazione degli interessati (cfr. parr. 13.8 e 25.4) e lo stesso Garante è destinatario di richieste di parere da parte dei Responsabili della prevenzione della corruzione e della trasparenza (cfr. par. 4.4.3) – nonché nella materia del *whistleblowing* (sulla quale v. pure par. 13.9), anche in vista del prossimo recepimento della direttiva (UE) 2019/1937 del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

Unitamente a tale attività di ricerca, la predisposizione di un osservatorio ad uso interno (nell'anno di riferimento con cadenza mensile) – frutto del costante monitoraggio, nella cornice nazionale ed eurounitaria, di normativa, giurisprudenza e dottrina, in particolare in materia di protezione dati – assicura l'aggiornamento, tempestivo e ad ampio spettro, di quanti operano in Autorità.

LeADS

Il Garante è tra i *partner* del Progetto di ricerca denominato *Legality Attentive Data Scientist* (LeADS) che mira a formare esperti in *data science* e diritto in grado di operare all'interno delle due discipline; l'iniziativa, finanziata a partire dal 2021

nell'ambito del programma *Horizon 2020 – Research and Innovation Framework*, è coordinata da Giovanni Comandé (Scuola Superiore Sant'Anna) e vede la partecipazione dell'Università del Lussemburgo, dell'Università Paul Sabatier Tolosa III, della VriJE Universiteit di Bruxelles, dell'Università del Pireo, dell'Università Jagellonica e del Consiglio Nazionale delle Ricerche, nonché di alcune (piccole, medie e grandi) imprese attive nel settore dell'intelligenza artificiale.

La predisposizione del testo della Relazione annuale costituisce un compito importante che la legge pone in capo al Garante (cfr. art. 154, comma 1, lett. *e*), del Codice nonché l'art. 59 del RGPD) al fine di rendere conto, anzitutto al Parlamento e al Governo, dell'attività svolta dall'Autorità. La pubblicazione del testo della Relazione sul sito istituzionale del Garante consente inoltre di perseguire una più ampia finalità di trasparenza sull'attività svolta dall'Autorità 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) e consente un aggiornamento su specifici profili o istituti attinenti alla protezione dati.

A ciò si aggiunga che, 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 (adempimento che con regolarità è stato attuato dal 2014), nonché alla Commissione europea e al Comitato (come stabilito dall'art. 59 del RGPD).

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

L'Ufficio del Garante

Relazione annuale
2020

III - L'Ufficio del Garante

25 La gestione amministrativa e dei sistemi informatici

25.1. *Il bilancio e la gestione economico-finanziaria*

La gestione delle attività di natura amministrativo-contabile del Garante è stata improntata ad una prudente valutazione delle entrate e all'osservanza dei generali principi di attenta programmazione della spesa nel rispetto delle specifiche disposizioni legislative e regolamentari in materia di contabilità pubblica che si informano ai requisiti della veridicità, pubblicità e trasparenza, nonché del pareggio di bilancio.

Nell'anno 2020 il finanziamento statale complessivamente erogato al Garante è stato pari a 30,1 milioni di euro, entità individuata dalla legge 27 dicembre 2019, n. 160. In conseguenza dell'applicazione delle sanzioni irrogate dal Garante, sono affluiti direttamente al bilancio dello Stato pagamenti per complessivi 38,4 milioni di euro. In relazione a tale importo, ben 36,2 provengono da versamenti spontanei dei contravventori e 2,2 dalla riscossione coattiva. Occorre al riguardo evidenziare che i proventi delle sanzioni irrogate affluiscono direttamente al bilancio dello Stato e, nella misura del 50% del totale annuo, devono essere riassegnati all'Autorità per essere destinati alle attività di sensibilizzazione e ispettive nonché ai compiti di attuazione del Regolamento rimessi al Garante (art. 166, comma 7, del Codice).

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 disposizioni vigenti.

La gestione amministrativa del Garante ha risentito degli inevitabili riflessi dei provvedimenti legislativi che, in occasione della naturale scadenza dell'organo di vertice, si sono succeduti e per effetto dei quali, a partire dal decreto-legge 7 agosto 2019, n. 75, il Collegio, nella composizione al tempo in carica, è stato autorizzato a continuare a svolgere le 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 comunque l'operatività dell'Autorità, ne ha tuttavia limitato le potenzialità, con particolare riguardo alla programmazione della spesa. In tale contesto, caratterizzato da successive proroghe delle funzioni per periodi limitati, il procedimento di spesa è stato infatti preordinato ad assicurare soltanto adempimenti gestionali di natura ordinaria e quelli configurabili come indifferibili ed urgenti.

Nel corso dell'esercizio il Garante non ha conferito incarichi di studio e di consulenza, secondo una politica gestionale consolidata, orientata ad una valorizzazione delle risorse interne.

Nel periodo considerato sono stati approvati dall'Autorità il bilancio consuntivo

25

relativo all'anno 2019 e il bilancio preventivo relativo all'esercizio finanziario 2021. Se abitualmente il documento contabile di rendiconto della gestione deve essere approvato entro il 30 aprile dell'anno successivo a quello cui lo stesso si riferisce, la proroga di tale termine di due mesi in virtù delle disposizioni contenute nel decreto-legge n. 18/2020 ha sortito l'effetto del completamento dell'*iter* di approvazione del bilancio consuntivo per l'anno 2019, oggetto della delibera 24 giugno 2020, n. 109 (doc. web n. 9438123).

L'Ufficio ha inoltre elaborato gli atti preordinati all'approvazione di una variazione al bilancio di previsione 2020 di cui alla delibera 26 febbraio 2020, n. 37.

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.

In conformità all'art. 14 del regolamento del Garante n. 3/2000, inoltre, è stato puntualmente predisposto e presentato all'organo di controllo il previsto rendiconto trimestrale sulla corretta gestione del fondo interno di cassa.

Sotto il profilo più strettamente contabile, il risultato finanziario dell'esercizio ha fatto registrare un importante avanzo di amministrazione, pari a oltre 6,6 milioni di euro. Tale risultato è stato determinato da una pluralità di fattori: una dinamica della spesa più contenuta rispetto a quanto ipotizzato in sede di previsione, una politica gestionale tendenzialmente volta a valorizzare la salvaguardia delle risorse erariali non ultime, le inevitabili conseguenze che la pandemia ha determinato a carico della gestione amministrativa e delle relative procedure di spesa.

Nel 2020, al netto delle partite di giro, le entrate complessivamente acquisite dall'Autorità sono state di 30,4 milioni di euro a fronte delle quali sono stati registrati impegni di spesa per 23,8 milioni di euro (cfr. parte IV, tab. 18).

Le risorse finanziarie acquisite al bilancio del Garante sono rappresentate, in misura largamente prevalente, da trasferimenti posti a carico del bilancio dello Stato, il cui importo è quantificato annualmente nell'ambito della legge di bilancio. In via residuale e per importi poco significativi la gestione ha fatto registrare l'acquisizione al bilancio di ulteriori somme a titolo di meri rimborsi spese erogati da parte di amministrazioni e organismi dell'Unione europea. Rispetto al precedente esercizio finanziario, l'incremento delle entrate registrato nel 2020 è stato di 0,9 milioni di euro, con una variazione di poco superiore al 3%.

Con riferimento alla spesa, invece, gli oneri complessivi registrati nell'anno, pari a 23,8 milioni di euro, risultano in diminuzione di 0,8 milioni di euro rispetto alla spesa complessiva del precedente anno 2019, corrispondente ad una variazione di circa il 3,29%. La spesa complessiva è da imputare in massima parte alla gestione corrente, nella misura di 23,3 milioni di euro, mentre la parte residuale di 0,5 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 2020 la struttura della spesa fa emergere, come per il passato ed in analogia rispetto alla generalità delle 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'80% rispetto a quanto riconosciuto al personale di altre autorità amministrative indipendenti.

L'indennità di carica riconosciuta al Presidente ed ai componenti del Collegio è stata definita nei limiti e sulla base di parametri specificati dalla legge ed alla relativa

erogazione si è provveduto nel rispetto dei vincoli e delle prescrizioni vigenti.

Con riferimento, infine, agli oneri strettamente connessi alle esigenze gestionali, nel corso dell'anno l'Autorità ha rispettato i prescritti limiti di legge: per una puntuale illustrazione dei valori sintetici delle entrate correnti e delle spese, suddivise tra quelle correnti, in conto capitale e per meri trasferimenti, si rinvia alla parte IV, tab. 18; 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*

L'anno 2020 è stato caratterizzato dall'introduzione di disposizioni emergenziali in materia di appalti pubblici, come il decreto-legge 16 luglio 2020, n. 76, convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120; il contesto pandemico ha infatti indotto il legislatore a ridurre taluni vincoli ordinariamente previsti dal codice dei contratti pubblici, di talché si è resa necessaria la rapida revisione di alcune procedure al fine di adeguarle alle sopravvenute esigenze. In questo quadro di eccezionalità, sono stati costantemente impiegati gli strumenti di negoziazione ed acquisto offerti da Consip, sia sul Mercato elettronico della p.a. (Richiesta di offerta, Trattativa diretta, Ordine diretto) sia esternamente ad esso (Convenzioni, Accordi quadro e Sistemi dinamici), utilizzati in prevalenza rispetto ad altri strumenti negoziali. L'Autorità ha cercato di ricorrere comunque – nel rispetto delle stringenti tempistiche richieste vuoi dalla normativa applicabile, vuoi dalle esigenze sottese all'azione amministrativa – a strumenti procedurali a carattere comparativo, sì da continuare a perseguire l'ottimizzazione del rapporto tra la qualità del bene o servizio richiesto ed il suo prezzo.

Per quanto attiene alle gare sopra soglia comunitaria, è proseguita l'attività relativa alla gara per la fornitura dei servizi di pulizia, igiene ambientale e *reception* bandita nel 2019 nell'ambito del Sistema dinamico di acquisizione della p.a. gestito da Consip giungendo, dopo lungo ed elaborato percorso, all'aggiudicazione definitiva; il relativo contratto ha avuto esecuzione a partire da febbraio 2021. Nel contempo, assistiti dal servizio di consulenza tecnica prestato dal *broker* dell'Autorità, è stata bandita una gara a procedura aperta avente ad oggetto la gestione del piano sanitario del personale del Garante, andata deserta per assenza di offerte, non diversamente da altre consimili bandite da altre autorità amministrative indipendenti. Nel secondo semestre dell'anno sono state pertanto avviate le attività conseguenti per l'indizione di una nuova procedura di gara, opportunamente rimodulata, previa condivisione da parte delle organizzazioni sindacali.

Gare

Tra le procedure caratterizzate invece da importi inferiori alla soglia comunitaria, è stata svolta una gara a procedura aperta per la fornitura del servizio di monitoraggio delle attività delle Istituzioni nazionali in relazione agli sviluppi che interessano la materia della protezione dei dati personali; è stata poi effettuata una procedura comparativa sul Mepa avente ad oggetto la fornitura di arredi per sala convegni e altre sedute per ufficio, che – in ragione della situazione emergenziale – è stata revocata e nuovamente indetta con diversa base di gara e opportune modifiche rispetto all'oggetto contrattuale e alle modalità di gara.

Un importante impegno dell'Ufficio ha riguardato la procedura sotto soglia comunitaria, relativa al servizio di brokeraggio assicurativo precedentemente menzionato, che è stata esperita – come previsto dalla Convenzione sottoscritta con altre autorità amministrative indipendenti ai sensi dell'art. 22, comma 7, d.l. 24 giugno

2014, n. 90, convertito con modificazioni dalla legge 11 agosto 2014, n. 114 – come gara telematica aperta in tre distinti lotti, nella quale l'Autorità ha rivestito il ruolo di stazione appaltante anche per conto delle altre autorità che hanno manifestato interesse a partecipare (Agcom e Autorità di regolazione dei trasporti): l'aggiudicazione è avvenuta all'inizio del 2021.

Infine, nell'ultimo trimestre 2020 è stata bandita sul Mepa una Richiesta di offerta concernente il servizio di cassa.

Molteplici procedure d'acquisto sono state dedicate all'adeguamento dell'infrastruttura *hardware* e *software* dell'Autorità alle nuove esigenze manifestatesi nel contesto emergenziale, con particolare riferimento al lavoro agile ed al suo prevedibile protrarsi: sono stati pertanto disposti acquisti di dispositivi elettronici per il lavoro in mobilità, nonché di apparecchiature e *software* di supporto ad un'infrastruttura sempre più indirizzata ad architetture di tipo *cloud.* A tal fine, laddove disponibile, è stato utilizzato lo strumento dell'adesione ad Accordi quadro di Consip (SPC *Cloud* e SPC Connettività). Giova ribadire che la maggioranza dei contratti relativi al settore in esame, anche per importi inferiori ai limiti previsti per l'obbligatorietà del ricorso a procedure comparative, si è svolta previa effettuazione di ricerche di mercato dirette (tramite esecuzione di specifiche trattative con più operatori economici) oppure indirette (tramite consultazione dell'offerta presente sul Mepa), al fine della massima applicazione dei principi di economicità, efficacia, libera concorrenza, rotazione e trasparenza stabiliti dal codice dei contratti pubblici.

È proseguita l'attività di costante aggiornamento dell'elenco di avvocati del libero foro cui l'Autorità può ricorrere per gli incarichi di patrocinio legale nell'interesse del Garante nei casi in cui la difesa non possa essere assunta dall'Avvocatura dello Stato.

La gestione del patrimonio

La sede degli uffici è condotta in locazione e l'Autorità non detiene immobili adibiti ad abitazione o foresteria. Per quanto attiene alla logistica e manutenzione dell'immobile, sono state effettuate attività di adeguamento funzionale e miglioramento dei locali e dei relativi arredi, di concerto con la società proprietaria dell'immobile e con il Rspp dell'Autorità, che ha costantemente coadiuvato l'Ufficio al fine di assicurare il rispetto della normativa sulla sicurezza nei luoghi di lavoro; è stata completata la sistemazione dei locali adibiti ad archivio documentale. In particolare, l'Ufficio ha vigilato in ordine alla corretta esecuzione delle iniziative di manutenzione e gestione dell'immobile con specifico riferimento alla pianificazione e alla realizzazione dell'adeguamento alle norme antincendio con la sostituzione, ove necessario, di portoni e finestre esistenti con porte e finestre tagliafuoco.

Per quanto riguarda l'impianto elettrico, è stata avviata la procedura volta alla sostituzione degli attuali corpi illuminanti con luci a LED che garantiscono il risparmio energetico.

Sono stati altresì realizzati i lavori per allestire nella sede una sala consultazione dotando lo spazio di moduli per la custodia dei libri e di scrivanie per le attività di studio.

25.3. *L'organizzazione dell'Ufficio*

Lavoro agile

In conformità alla decretazione d'urgenza che si è susseguita a partire dal decreto-legge 17 marzo 2020, n. 18 (cd. Cura Italia: cfr. par. 2.1, n. 8) fino al d.P.C.M. 14 gennaio 2021, l'Autorità ha prontamente fatto fronte alla grave situazione emergenziale dovuta alla diffusione della pandemia adeguando le dotazioni tecnologiche e le procedure interne (ivi comprese le modalità di rilevazione delle presenze) in modo da consentire al personale di continuare a svolgere l'attività lavorativa da remoto,

senza alcuna soluzione di continuità rispetto all'insorgere dell'emergenza. In questa prospettiva, tenendo conto della cornice di riferimento nazionale con riguardo all'andamento della pandemia, sono state adottate una pluralità di delibere volte a consentire in via ordinaria, salvo lo svolgimento di attività essenziali o indifferibili da realizzarsi necessariamente in presenza, l'espletamento dell'attività lavorativa secondo la modalità agile (cd. *smart working*).

Inoltre, nell'ottica di fornire al personale una mirata proposta formativa, seppure a distanza, sono state vagliate le opportunità offerte dalla Sna e si è provveduto alla individuazione di alcuni istituti di formazione sul Mepa per l'erogazione di corsi di lingua inglese al personale in modalità *online*.

In materia di assicurazioni si è provveduto ad aggiornare le liste anagrafiche dei rami sanitaria e vita/invalidità permanente.

Considerata la situazione emergenziale, costanti sono stati i contatti con il Rspp – che ha provveduto ad aggiornare il Documento di valutazione dei rischi in relazione al Covid-19 – e con il medico competente, sia per la gestione delle attività ordinarie, sia per agevolare la predisposizione delle misure di tutela della salute dei dipendenti prescritte nelle fonti normative di riferimento (d.P.C.M. Cura Italia e ss.).

Procedure concorsuali

Nel periodo considerato è stata svolta un'intensa attività per la prosecuzione delle procedure concorsuali in corso: in particolare, è giunta a conclusione sia la procedura che ha portato all'assunzione di 4 dipendenti nel ruolo degli impiegati operativi, sia la procedura relativa alla copertura di 2 posti di dirigente nel ruolo del Garante (cfr. parte IV, tab. 17).

Relazioni sindacali

Anche la gestione delle relazioni con le organizzazioni sindacali è stata particolarmente intensa: numerose le interlocuzioni per perfezionare le modalità, adottate in prima battuta in via emergenziale, di espletamento della prestazione di lavoro agile; gran parte dell'attività si è focalizzata sull'adozione di un Protocollo sulla sicurezza, sintesi delle misure da osservare sul luogo di lavoro al fine di fronteggiare e contenere la diffusione del virus da Covid-19. Numerose sono state altresì le interlocuzioni in vista dell'adozione di un nuovo piano sanitario dell'Autorità.

Sicurezza sanitaria

In ragione della situazione pandemica è stata condotta un'attività di vigilanza sul corretto utilizzo dei dispositivi di sicurezza (con l'acquisto di *termoscanner* collocati in corrispondenza degli ingressi all'ufficio nonché di ulteriori strumenti preordinati a garantire la sicurezza e la salute del personale) e sulle operazioni di sanificazione della sede.

Controllo di gestione

Il controllo di gestione presso l'Autorità continua ad incentrarsi sull'analisi periodica degli affari assegnati alle diverse unità organizzative mediante il sistema di protocollazione Archiflow e sulla conseguente produzione di una reportistica mensile di carattere statistico che si focalizza sull'andamento della trattazione degli affari, dando conto dei flussi relativi agli affari assegnati ed evasi dalle unità organizzative.

Rpd

Anche presso il Garante è stata individuata la figura del Responsabile della protezione dei dati personali (Rpd) per lo svolgimento dei compiti indicati agli artt. 38 e 39 del Regolamento e sono state oggetto di valutazione nuove misure volte a rendere più efficace la sua azione all'interno dell'Autorità.

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" del sito web istituzionale, all'interno della quale sono state tempestivamente pubblicate sia la relazione annuale del Responsabile della prevenzione della corruzione e della trasparenza (Rpct) per l'anno 2020,

in conformità a quanto previsto dall'art. 1, comma 14, l. n. 190/2012 (doc. web n. 9255597) – relativa all'efficacia delle misure di prevenzione definite nel Piano triennale di prevenzione della corruzione e della trasparenza 2020-2022 –, sia la griglia di rilevazione di cui all'allegato 2 della delibera Anac 21 febbraio 2018, n. 141, che, in assenza di Oiv o strutture equivalenti presso l'Autorità, il Rpct è tenuto a pubblicare.

Ptpct

Dando continuità all'attuazione delle misure generali, nel 2020 è stato adottato il nuovo Piano triennale di prevenzione della corruzione e della trasparenza (Ptpct) 2020-2022 con deliberazione del Garante 30 gennaio 2020, n. 22 (doc. web n. 9265074): si tratta del secondo Ptpct dell'Autorità il quale, sulla base delle aree di rischio previamente individuate, si è soffermato sulle misure di prevenzione della corruzione già attuate e su quelle da continuare ad attuare. Ai fini della sua predisposizione, anche in considerazione del rinnovato quadro normativo "interno" conseguente all'adozione dei regolamenti nn. 1 e 2/2019 (concernenti, rispettivamente, le procedure aventi rilevanza esterna finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante nonché l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante), si è provveduto ad una rinnovata mappatura dei processi dell'Autorità.

Tenendo conto delle risorse disponibili, delle complessive esigenze di funzionamento dell'Ufficio durante l'emergenza sanitaria nonché dei carichi di lavoro gravanti sull'Autorità, è proseguita (ancorché in misura più contenuta) l'attività formativa del personale anche nel settore dedicato alla prevenzione della corruzione e della trasparenza tramite la partecipazione ai corsi organizzati dalla Scuola nazionale dell'amministrazione (Sna).

Accesso civico

Con riguardo alla disciplina in materia di accesso civico introdotta con decreto legislativo n. 33/2013, gli uffici dell'Autorità hanno dato riscontro a tutte le istanze pervenute nell'anno (pari a nove); non diversamente, il Rpct ha fornito riscontro alla sola istanza di riesame ex art. 5, comma 7, d.lgs. n. 33/2013, portata alla sua attenzione; non sono state presentate istanze di accesso civico relative a dati soggetti a pubblicazione obbligatoria (ex art. 5, comma 1, d.lgs. n. 33/2013).

25.5. *Il settore informatico e tecnologico*

Interventi a supporto dell'emergenza pandemica

In corrispondenza dell'insorgere della pandemia, l'Ufficio (per il tramite del Dipartimento tecnologie digitali e sicurezza informatica) è stato fortemente impegnato nel creare i presupposti tecnici e organizzativi per consentire a tutto il personale e all'Autorità nel suo complesso di mantenere la piena operatività, assicurando lo svolgimento dei compiti istituzionali pur nello stato di isolamento sanitario che si andava a delineare, poi concretizzatosi con i provvedimenti governativi dell'inizio di marzo 2020.

Gli strumenti disponibili per assicurare la capacità di intervento e controllo nonché per garantire la sicurezza perimetrale della rete dell'Ufficio, basati sulla tecnologia VPN (*Virtual Private Network*) di cui l'Autorità si è dotata fin dal settembre 2000 (e nel tempo aggiornati) hanno garantito la possibilità di accesso remoto con diverse tipologie di VPN. Essi si sono rivelati determinanti nella fase di emergenza in quanto, con alcune opportune configurazioni, sono stati trasformati da strumenti volti a un utilizzo prettamente tecnico in vere e proprie porte d'accesso ai servizi del sistema informativo dell'Autorità a vantaggio della generalità del personale e dei collaboratori.

Attraverso le opportune configurazioni dei dispositivi disponibili, l'Ufficio è stato così in grado di non subire interruzioni di operatività pur in presenza di una situa-

zione di emergenza mai prima d'ora neanche ipotizzata.

Alla buona riuscita dell'operazione *smart working* ha contribuito, dal punto di vista tecnologico, la transizione effettuata già nel 2016 dalla telefonia tradizionale a quella VoIP che, grazie alla sua flessibilità, ha permesso di assicurare il servizio telefonico interno, consentendo così al personale di operare con piena connessione alla rete informatica e ai servizi telefonici, al pari di quanto avviene nella normale operatività in sede.

Al fine di permettere a tutto il personale l'immediata transizione alla modalità di lavoro agile richiesta dall'emergenza pandemica è stato redatto un manuale operativo, messo a disposizione fin dal 9 marzo 2020 (e successivamente aggiornato sulla base dell'evoluzione degli strumenti e delle configurazioni adottate) allo scopo di consentire a tutta l'utenza l'operatività da remoto con propri strumenti in connessione alla rete dell'Ufficio, realizzando così una prima esperienza collettiva, ancorché forzata, di *smart working*.

Nella fase iniziale, durata due settimane, il settore tecnico ha altresì garantito un servizio di supporto interno straordinario funzionale all'assistenza al personale che si confrontava per la prima volta con le procedure e gli strumenti caratteristici dello *smart working*: sono così stati svolti, nel periodo dal 10 marzo al 30 aprile 2020, più di mille interventi telefonici e in connessione remota, assicurando l'assistenza al personale per l'uso delle tecnologie di accesso remoto, *desktop* remoto, videoconferenza, telefonia VoIP e firma digitale, nonché lo svolgimento di adunanze collegiali, per la prima volta tenutesi con la piena partecipazione telematica dei componenti del Collegio.

Transizione al digitale

A sostegno del menzionato diffuso ricorso a forme di lavoro agile, intensa è stata l'attività di sviluppo dei sistemi con riguardo sia ad aspetti infrastrutturali e tecnologici, sia funzionali sia, ancora, applicativi, attraverso la configurazione dei sistemi in dotazione. I principali interventi hanno riguardato la digitalizzazione della procedura di notifica delle violazioni dei dati personali, arricchita da uno strumento di autovalutazione propedeutico alla notifica vera e propria.

Si è provveduto poi alla migrazione della piattaforma web a supporto del sito istituzionale presso un fornitore *cloud* nell'ambito del contratto esecutivo Consip SPC Lotto 4 e all'implementazione della nuova veste grafica integrata dell'Autorità (nuovo logo, nuovo monogramma e palette di colori), curando nel contempo la progettazione del nuovo portale che verrà avviato nel primo semestre del 2021.

È proseguito lo sviluppo dell'applicazione *online* per la comunicazione dei dati di contatto dei Rpd, avviata nel 2018 e progressivamente arricchita di nuove funzionalità. Tale applicazione consente di mantenere una relazione continua con la *community* dei Rpd/Dpo e di monitorare l'andamento del recepimento di questa importante figura nell'ambito dei trattamenti in ambito nazionale.

Sono state condotte attività di aggiornamento su sistemi *server* Microsoft Windows, sulle applicazioni gestite ed è stato portato a compimento il progetto della nuova carta multiservizi dell'Autorità, a tecnologia mista *contact e contactless.*

È stato altresì aggiornato (alla versione 9.8) il sistema di protocollo informatico Archiflow, nucleo centrale del sistema documentale dell'Ufficio, arricchito da nuove funzionalità connesse all'implementazione delle linee guida AgID sul documento informatico del settembre 2020.

Sicurezza informatica

Non si sono registrate situazioni pregiudizievoli rispetto alla sicurezza informatica sulle postazioni individuali e sui sistemi *server*, né su altre componenti dell'infrastruttura. Sono stati eseguiti periodici *vulnerability assessment* e *penetration test* mirati sul portale web e sui servizi *online* esposti al pubblico che non hanno rivelato vulnerabilità significative. La continuità dei servizi *online* è stata in linea con i valori

25

degli anni precedenti ovvero con *downtime* dei servizi intorno alle otto ore complessive nell'arco dell'anno per cause esterne (*black-out* elettrici o di rete di lunga durata) o per manutenzione programmata.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

I dati statistici

RELAZIONE ANNUALE
2020

IV - I dati statistici 2020

Tabella 1. Sintesi delle principali attività dell'Autorità

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	278
Pareri su norme di rango primario statale, delle regioni e delle autonomie	7
Pareri su atti regolamentari e amministrativi	60
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	18
Parere ai sensi dell'art. 110 del Codice per la realizzazione di un progetto di ricerca medica, biomedica e epidemiologica nonché ex art. 36 del RGPD	2
Autorizzazione di accordi amministrativi ai sensi degli artt. 46, par. 3, lett. *b*), 58, par. 3, lett. *i*) e 63, del RGPD	1
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché a seguito di accertamenti d'ufficio	92
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché a seguito di accertamenti d'ufficio con contestuale ordinanza-ingiunzione	56
Provvedimenti collegiali a seguito di notifica di violazione di dati	9
Provvedimenti collegiali a seguito di notifica di violazione di dati con contestuale ordinanza-ingiunzione	1
Provvedimenti di approvazione di codici di condotta	1
Ordinanze-ingiunzioni adottate dal Garante	3
Riscontri a segnalazioni e reclami (art. 11, reg. Garante n. 1/2019)	8.984
Riscontri a quesiti (art. 11, reg. Garante n. 1/2019)	422
Audizioni del Presidente del Garante o memorie scritte trasmesse al Parlamento	7
Risposte ad atti di sindacato ispettivo e controllo	1
Riscontri dell'Urp a quesiti e ad altre istanze	15.040
Accertamenti e controlli effettuati *in loco* (artt. 157-158, d.lgs. n. 196/2003)	21
Pagamenti derivanti dall'attività sanzionatoria	38.448.895
Comunicazioni di notizia di reato all'Autorità giudiziaria	8
Opposizioni (trattate) a provvedimenti del Garante	156
Ricorsi giurisdizionali trattati ex art. 152, d.lgs. n. 196/2003	56
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 1, d.lgs. n. 33/2013	0
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 2, d.lgs. n. 33/2013	9
Istanze di riesame a seguito di diniego all'accesso civico presentate al Rpct e riscontrate ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	1
Misure correttive e sanzionatorie (art. 58, par. 2, del RGPD)	184
Misure correttive e sanzionatorie (d.lgs. n. 51/2018)	6
Riunioni del Comitato europeo per la protezione dei dati personali	22
Partecipazione a sottogruppi di lavoro del Comitato europeo per la protezione dei dati personali	127
Riunioni e ispezioni delle autorità comuni di controllo/organismi di supervisione (Europol, SIS II, Dogane, Eurodac, VIS)	9
Conferenze internazionali	1
Riunioni presso il Consiglio d'Europa e l'Ocse	10
Altre conferenze e incontri	10

Tabella 2. Attività di comunicazione dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	54
Newsletter	11
Bollettino radiofonico del Garante	11
Prodotti editoriali	3
Prodotti web	12
Video *spot*	6

Tabella 3. Pareri ex art. 36, par. 4, del RGPD su norme di rango primario statale, delle regioni e delle autonomie

Pareri ex art. 36, par. 4, del RGPD su norme di rango primario statale, delle regioni e delle autonomie	
Temi	**Riscontri resi nell'anno***
Ambiente	1
Digitalizzazione p.a.	2
Sanità	1
Sanità - Covid-19	2
Trasporti	1
Totale	**7**

Tabella 4. Pareri ex art. 36, par. 4, del RGPD resi al Governo su atti regolamentari e amministrativi

Pareri ex art. 36, par. 4, del RGPD resi al Governo su atti regolamentari e amministrativi	
Temi	**Riscontri resi nell'anno***
Ambiente	2
Banche	1
Digitalizzazione p.a.	1
Diritti fondamentali	1
Fisco	7
Funzioni di interesse pubblico	1
Giustizia	2
Istruzione	1
Marketing	1
Minori stranieri non accompagnati	1
Sanità	2
Sanità - Covid 19	8
Trasporti	6
Totale	**34**

(*) inerenti anche ad affari pervenuti anteriormente al 2020

Pareri ex art. 36, par. 4, del RGPD resi ad altre Istituzioni	
Temi	**Riscontri resi nell'anno***
Banche	1
Digitalizzazione p.a.	6
Fisco	11
Funzioni di interesse pubblico	1
Giustizia	1
Sanità	1
Statistica	5
Totale	**26**

Tabella 5. Pareri ex art. 36, par. 4, del RGPD resi ad altre Istituzioni

Misure correttive e sanzionatorie	
Avvertimenti a titolare/responsabile del trattamento (art. 58, par. 2, lett. *a*), del RGPD)	6
Ammonimenti a titolare/responsabile del trattamento (art. 58, par. 2, lett. *b*), del RGPD)	45
Ingiunzioni a titolare/responsabile del trattamento di soddisfare le richieste dell'interessato concernenti l'esercizio dei diritti riconosciuti dal RGPD (art. 58, par. 2, lett. *c*), del RGPD)	23
Ingiunzioni a titolare/responsabile del trattamento di conformare i trattamenti alle disposizioni del RGPD (art. 58, par. 2, lett. *d*), del RGPD)	16
Ingiunzioni a titolare del trattamento di comunicare all'interessato una violazione dei dati personali (art. 58, par. 2, lett. *e*), del RGPD)	2
Imposizioni di limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento (art. 58, par. 2, lett. *f*), del RGPD)	22
Ordine di rettifica/cancellazione di dati personali o limitazione del trattamento ex artt. 16, 17 e 18 e altre misure previste dall'art. 58, par. 2, lett. *g*), del RGPD	14
Sanzioni amministrative pecuniarie ex art. 83 (art. 58, par. 2, lett. *i*), del RGPD)	56
Totale	**184**

Tabella 6. Misure correttive e sanzionatorie (art. 58, par. 2, del RGPD)

Misure correttive e sanzionatorie (d.lgs. n. 51/2018)	
Ordine di rettifica/cancellazione di dati personali o limitazione del trattamento (art. 12, comma 1, d.lgs. n. 51/2018)	1
Avvertimenti a titolare/responsabile del trattamento (art. 37, comma 3, lett. *c*), d.lgs. n. 51/2018)	1
Ingiunzioni a titolare/responsabile del trattamento di conformare i trattamenti alle disposizioni del d.lgs. n. 51/2018 (art. 37, comma 3, lett. *d*), d.lgs. n. 51/2018)	2
Sanzioni amministrative pecuniarie (art. 42, d.lgs. n. 51/2018)	2
Totale	**6**

Tabella 7. Misure correttive e sanzionatorie (d.lgs. n. 51/2018)

Comunicazioni di notizia di reato all'Autorità giudiziaria	
Trattamento illecito dei dati (art. 167, d.lgs. n. 196/2003)	2
Violazioni in materia di controlli a distanza dei lavoratori (art. 171, d.lgs. n. 196/2003)	3
Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.)	2
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168, d.lgs. n. 196/2003)	1
Totale	**8**

Tabella 8. Comunicazioni di notizia di reato all'Autorità giudiziaria

(*) inerenti anche ad affari pervenuti anteriormente al 2020

Tabella 9. Pagamenti derivanti dall'attività sanzionatoria

Pagamenti derivanti dall'attività sanzionatoria	
Pagamenti spontanei dei contravventori	36.263.113
Riscossione coattiva	2.185.782
Totale	**38.448.895**

Tabella 10. Cooperazione tra autorità nazionali di protezione dei dati personali in IMI (Capo VII del RGPD)*

Cooperazione tra autorità nazionali di protezione dei dati personali - procedure IMI (Capo VII del RGPD)		
1) Decisioni finali adottate nell'ambito dell'attività di cooperazione rispetto alle quali il Garante ha agito in qualità di:		**292**
a) "autorità capofila" (LSA)	1	
b) "autorità interessata" (CSA)	291	
2) Procedure preliminari ex art. 56 del RGPD		**713**
a) procedure preliminari pervenute rispetto alle quali l'Autorità si è dichiarata "autorità interessata"	360	
b) procedure preliminari pervenute rispetto alle quali l'Autorità si è dichiarata "autorità non interessata"	266	
c) procedure preliminari pervenute rispetto alle quali l'Autorità ha assunto il ruolo di "autorità capofila"	8	
d) procedure preliminari pervenute rispetto alle quali l'Autorità ha fornito altro riscontro	63	
e) procedure preliminari promosse dall'Autorità	7	
f) altro	9	
3) Procedure di cooperazione ad impatto esclusivamente locale ex art. 56, par. 2, del RGPD		**7**
4) Procedure di cooperazione informale ex art. 60 del RGPD rispetto alle quali vi è stata una partecipazione dell'Autorità in qualità di:		**102**
a) "autorità interessata"	98	
b) "autorità capofila"	4	
5) Progetti di decisione ex art. 60 del RGPD rispetto ai quali l'Autorità ha cooperato in qualità di:		**131**
a1) "autorità interessata"	107	
a2) "autorità interessata" e rispetto ai quali sono state sollevate "obiezioni pertinenti e motivate" o commenti ex art. 60, par. 4, del RGPD	21	
b) "autorità capofila"	3	
6) Richieste di assistenza reciproca ex art. 61 del RGPD		**129**
a) ricevute da altre Autorità	105	
b) inviate ad altre Autorità	24	

Tabella 11. Procedure IMI nell'ambito del meccanismo di coerenza (Capo VII del RGPD)

Meccanismo di coerenza - procedure IMI (Capo VII del RGPD)	
Procedure relative all'attività consultiva dell'EDPB ex art. 64 del RGPD su progetti di decisione del Garante	1

*in relazione a procedure pervenute dal 01/01/2020

Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza	
Credito	33
Imprese	370
Reti telematiche	533
Libertà di espressione e di informazione	20
Notificazioni di violazione dei dati	140
Altro	35

Tabella 12. Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza

Segnalazioni e reclami		
	Pervenuti nell'anno	**Riscontri resi nell'anno (*)**
Dipartimento attività ispettive	3	317
Affari legali e giustizia	135	75
Libertà di manifestazione del pensiero e cyberbullismo	696	411
Realtà economiche e produttive	2.533	2.503
Realtà pubbliche	1.213	700
Reti telematiche e *marketing*	4.059	4.211
Sanità e ricerca	275	248
Tecnologie digitali e sicurezza informatica	751	519
Totali	**9.665**	**8.984**

Tabella 13. Segnalazioni e reclami

Quesiti		
	Pervenuti nell'anno	**Riscontri resi nell'anno (*)**
Affari legali e giustizia	17	7
Libertà di manifestazione del pensiero e cyberbullismo	9	3
Realtà economiche e produttive	97	122
Realtà pubbliche	337	196
Reti telematiche e *marketing*	47	17
Sanità e ricerca	69	76
Tecnologie digitali e sicurezza informatica	2	1
Totali	**578**	**422**

Tabella 14. Quesiti

(*) inerenti anche ad affari pervenuti anteriormente al 2020

Tabella 15. Ufficio relazioni con il pubblico

Ufficio relazioni con il pubblico	
E-mail esaminate	10.695
Contatti telefonici	3.981
Persone in visita all'Urp	32
Trattazione pratiche relative a fascicoli	332
Totale	**15.040**

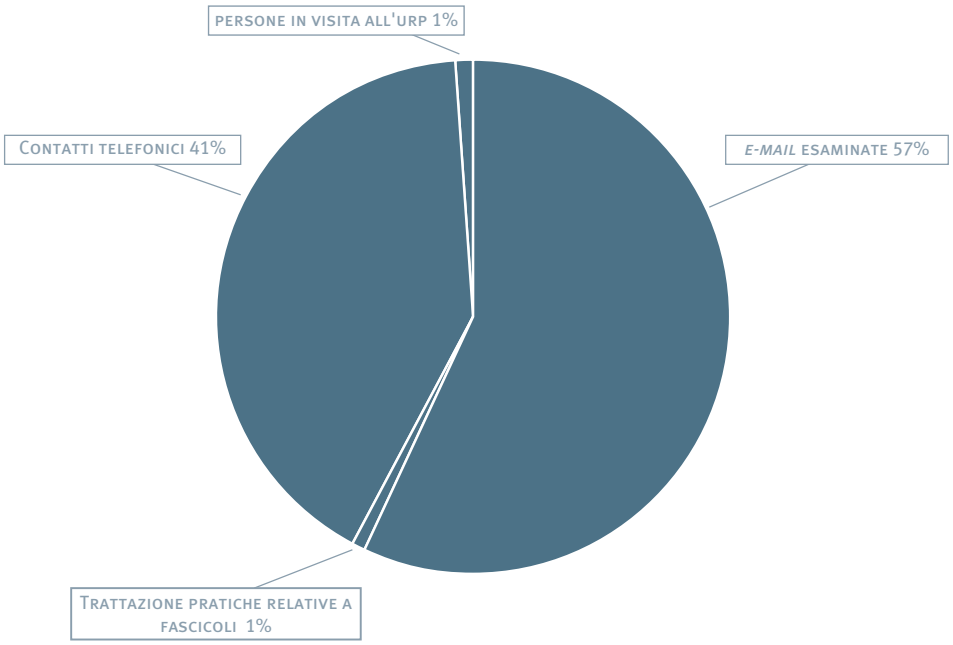
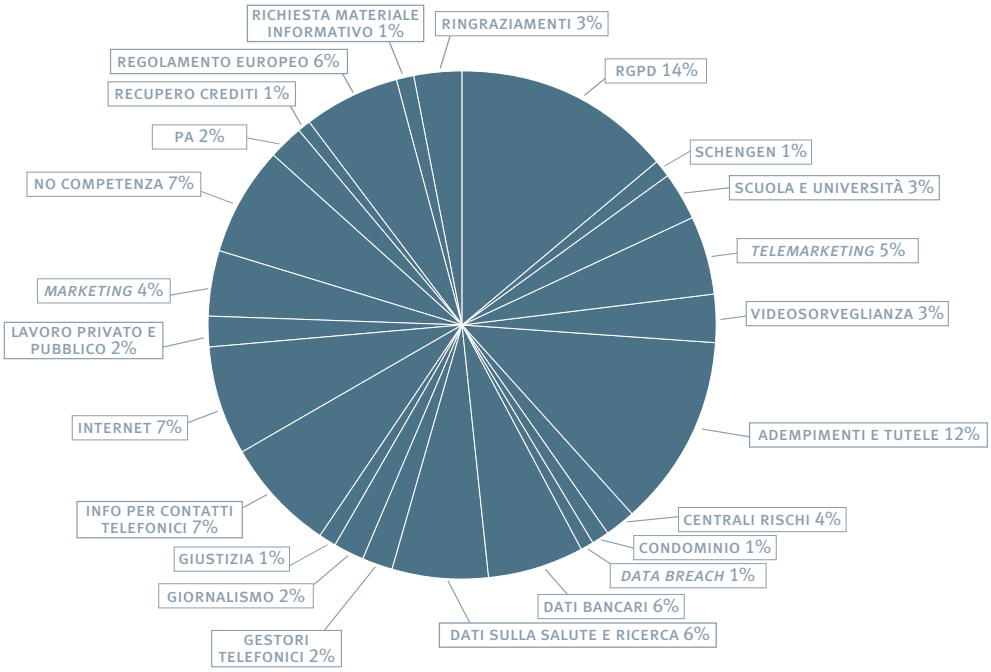


Grafico 16. Oggetto delle *e-mail* esaminate dall'Urp



Personale in servizio (*)				
Area	In ruolo (a)	Fuori ruolo (b)	In comando presso altre amm.ni o in aspettativa (c)	Impiegato dall'Ufficio (a+b-c)
Segretario generale	0	1		1
Dirigenti	16	1	2	15
Funzionari	88	5	3	90
Operativi	25			25
Esecutivi	0			
Totale	**129**	**7**	**5**	**131**
Personale a contratto (art. 156, comma 5, del Codice)				3

Tabella 17. Personale in servizio

Risorse finanziarie				
Entrate accertate	**Anno 2020**	**Anno 2019**	**Variazione**	
Entrate correnti	30.447.905	29.557.763	890.142	3,01%
Totale entrate	**30.447.905**	**29.557.763**	**890.142**	**3,01%**
Spese impegnate	**Anno 2020**	**Anno 2019**	**Variazione**	
Spese di funzionamento	22.973.973	23.799.145	-825.172	-3,47%
Spese in c/capitale	509.823	433.168	76.655	17,70%
Trasferimenti ad amministrazioni	330.486	392.825	-62.339	-15,87%
Totale spese	**23.814.282**	**24.625.138**	**-810.856**	**-3,29%**

Valori in euro

Tabella 18. Risorse finanziarie

(*) Situazione alla data del 31/12/2020

Tabella 19. Attività internazionali dell'Autorità

Unione europea			
COMITATO EUROPEO PER LA PROTEZIONE DEI DATI	**Sessioni plenarie**		28 gennaio 18 febbraio 17, 21 e 24 aprile 5, 8, 12, 19 e 26 maggio 2, 9, 16 e 30 giugno 17 e 22-23 luglio 2 e 14 settembre 7 e 20 ottobre 9 e 19 novembre 15 dicembre
	Riunioni dei sottogruppi	**Sottogruppo questioni strategiche e attività consultiva (SAESG)**	6 luglio 28 ottobre 5 novembre 1° e 16 dicembre
		***Border Travel Law Enforcement* (BTLE)**	6 febbraio 16 aprile 7 maggio 4 giugno 1° luglio 3 e 29 settembre 29 ottobre 18 novembre 10 dicembre
		Cooperation	4 febbraio 24-25 marzo 29 aprile 27 maggio 24 giugno 13-15 luglio 10 e 16 settembre (con *enforcement)* 22 settembre 23 settembre (con *enforcement*/linee guida RRO) 21 ottobre 10 e 24 novembre 9 dicembre
		Compliance, E-Government and Health	13 gennaio 11 marzo 2, 16 e 20 aprile 7 e 14 maggio 15, 18 e 22 giugno 7 e 9 luglio 10-11 settembre 8-9 ottobre 5, 6 e 23 novembre 7-8 dicembre
		Financial Matters	21 gennaio 5 marzo 30 marzo 5 e 25 giugno 15 settembre 5 novembre
		Drafting Team Rules of Procedure	10 e 18 settembre 2 ottobre

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI	**Riunioni dei sottogruppi**	***Key Provisions***	14-15 gennaio 3-4 e 31 marzo 5-6 e 26 maggio 9 e 29-30 giugno 9 settembre 7 ottobre 3 e 8 dicembre
		International Transfers,* BCR *Session, Taskforce on Supplementary Measures	11-12 febbraio 31 marzo 1° aprile 11-13 e 20 maggio 16-17 e 23 giugno 1° luglio 8-10, 18 e 25 settembre 5 e 12-14 ottobre 3-5 novembre 8, 11 e 14 dicembre
		Technology	15-16 gennaio 4-5 marzo 1° aprile 13 maggio 3 e 10-11 giugno 2-3 luglio 17-18 settembre 15-16 ottobre 13 novembre 4 dicembre
		IMI-GDPR *Users Group*	5 febbraio 18 giugno 14 ottobre 3 dicembre
		Enforcement	5 febbraio 26 marzo 19 maggio 10 giugno 14 luglio 10, 15-16, 23 e 30 settembre 1, 15, 22 e 29 ottobre 6 e 18-19 novembre 10 dicembre
		Fining Task Force	6 febbraio 25 marzo 11 giugno 9 ottobre 16 dicembre
		Gruppo di volontari CPC-DPA (Autorità di tutela dei consumatori e Autorità di protezione dei dati)	8 luglio 24 novembre
		Gruppo dei coordinatori	15 luglio
		Social Media Working Group	7 febbraio 15 maggio 8 giugno 6 luglio 6 ottobre 2 dicembre

Unione europea	
Gruppo di coordinamento della supervisione SIS II	17 giugno e 25 novembre
Gruppo di coordinamento della supervisione VIS	18 giugno e 26 novembre
Gruppo di supervisione del sistema Eurodac	18 giugno e 26 novembre
Gruppo di coordinamento della supervisione del sistema di informazione doganale - SID	15 giugno
Europol Coordination Board	16 giugno e 24 novembre

Altri *forum* internazionali		
Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	**Comitato DGP** ***(Data Governance and Privacy in the Digital Economy)***	21-22 aprile (plenaria) 9 e 17 novembre (plenaria)
	DGP *Bureau*	21 luglio (DGP *Bureau*) 8 ottobre (*Joint Meeting* CDEP *Bureau*/DGP *Bureau*)
Consiglio d'Europa	**Comitato Consultivo Convenzione n. 108/1981 (T-PD)**	18-20 novembre (plenaria)
	T-PD *Bureau*	28-30 settembre 16-18 dicembre
	Comitato *ad hoc* in materia di intelligenza artificiale (CAHAI)	6-8 luglio (plenaria) 15-16 ottobre (PDG - Gruppo di lavoro sullo sviluppo di *policy*)

Conferenze internazionali	
GPA *Closed Session* 2020 (Conferenza internazionale delle autorità di protezione dati)	13-15 ottobre 2020

Altre conferenze e *meeting*	
CPDP *Conference*	30 gennaio
OCSE e GPA ***Online Workshop on Addressing the Data Governance and Privacy Challenges in the Fight against* Covid-19**	15 aprile 16 settembre
Progetto SMEDATA **Conferenza internazionale (in *streaming*)**	28 ottobre
ISO 27701 *and* GDPR *Certification Workshop*	21 gennaio
Project Commitee* (PC) 317 di ISO** ***"Consumer protection – Privacy by design for consumer goods and services"	17-20 marzo
***Working Group* 5 del JTC 13 del CEN CENELEC** **(ex CEN/CLC/TC8)**	24-25 marzo
***Working Group* 5 – ISO/IEC JTC1/SC27**	20-24 aprile 12-16 settembre
Workshop* progetto AUDITOR** ***(Evaluation and Certification Schemes for Security Products)	15 giugno

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Redazione
Garante per la protezione dei dati personali

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

stampa:
Tiburtini Srl


GPDP
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI