SENATO DELLA REPUBBLICA

XIX LEGISLATURA

Doc. **CXXXVI**
n. **1**

RELAZIONE

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

(ANNO 2022)

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

Presentata dal Presidente del Garante per la protezione dei dati personali
(STANZIONE)

Comunicata alla Presidenza il 24 luglio 2023

GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione Annuale 2022

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 2022

I numeri del 2022

Provvedimenti collegiali 442

81
Pareri su atti normativi e amministrativi

231
Decisioni su reclami e segnalazioni

1.338
Procedure IMI

1.351
Comunicazioni di violazione dei dati

9.218
Riscontri a reclami e segnalazioni

396
Riscontri a quesiti

€ 9.459.457
Sanzioni riscosse

140
Ispezioni

216
Riunioni internazionali

5
Comunicazioni all'Autorità giudiziaria

16.464 Contatti SRP

84
Comunicati e *Newsletter*

4.385.792
Accessi al sito web

Indice

Indice

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

1. Introduzione 3

2. Il quadro normativo in materia di protezione dei dati personali 13

2.1. Le leggi 13
2.2. I decreti-legge 17
2.3. I decreti legislativi 19
2.4. Le norme regolamentari 21

3. I rapporti con il Parlamento e le altre Istituzioni 23

3.1. L'attività consultiva del Garante 23
3.1.1. La consultazione del Garante nell'ambito del procedimento legislativo o dell'esercizio delle funzioni conoscitive, di indirizzo e controllo delle Camere 23
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 24
3.1.3. I pareri sugli atti regolamentari 26
3.1.4. La consultazione del Garante sugli atti normativi regionali o di province autonome 27
3.1.5. Provvedimenti decisori di segnalazioni 27
3.2. Consultazione attraverso la piattaforma IMI 28
3.3. Il contributo al Governo ai fini del riscontro ad atti di sindacato ispettivo 28

II- L'ATTIVITÀ SVOLTA DAL GARANTE

4. Il Garante e le amministrazioni pubbliche 31

4.1. L'attività fiscale, tributaria e in materia di antiriciclaggio 31
4.1.1. La dichiarazione dei redditi precompilata 31
4.1.2. Lotta all'evasione fiscale e tecniche di intelligenza artificiale 32
4.1.3. Antiriciclaggio 33
4.2. Previdenza, assistenza sociale e altri benefici economici 34
4.2.1. Erogazione di benefici 34
4.2.2. Dati dei beneficiari di fondi a valere sul Fondo sociale europeo 36
4.2.3. Isee precompilato 36
4.2.4. Reddito e pensione di cittadinanza 37
4.3. La protezione dei dati personali in ambito scolastico e universitario 37
4.4. Trasparenza e pubblicità dell'azione amministrativa 40
4.4.1. Il rispetto della data protection by design *e* by default 40
4.4.2. La pubblicazione di dati personali online *da parte delle pubbliche amministrazioni* 41
4.4.3. L'accesso civico 41
4.5. I trattamenti effettuati presso regioni ed enti locali 44
4.5.1. Tributi locali 44
4.5.2. Rifiuti urbani 45
4.5.3. Mobilità e trasporti 45
4.5.4. Servizi online *e misure di sicurezza* 47
4.6. Il Rpd in ambito pubblico 48
4.7. Ordini professionali 49

Indice

4.8. Digitalizzazione della pubblica amministrazione 49
4.9. La materia anagrafica ed elettorale 55
4.10. Videosorveglianza in ambito pubblico 58

5. La sanità 60

5.1. Il trattamento dei dati personali effettuato nell'ambito dell'emergenza sanitaria 60
5.2. La sanità digitale 63
5.2.1. Il Fascicolo sanitario elettronico (Fse) 63
5.2.2. Il dossier *sanitario* 67
5.2.3. La medicina predittiva 68
5.2.4. Trattamenti di dati personali nell'ambito dei sistemi informativi sanitari centrali 71
5.2.5. Protezione dei dati personali e app *sanitarie* 72
5.3. Trattamenti per finalità di cura e amministrative correlati alla cura 74
5.3.1. Provvedimenti derivanti da data breach 74
5.3.2. Provvedimenti derivanti da reclami e segnalazioni 76
5.4. Trattamenti per finalità ulteriori rispetto a quelle di cura e/o amministrative correlati alla cura 78

6. La ricerca scientifica 80

6.1. Provvedimenti adottati ai sensi dell'art. 110 del Codice 80
6.2. Trattamenti di dati personali per scopi di ricerca medica in ambito Covid-19 83
6.3. Comunicazioni ai sensi dell'art. 2-*ter*, comma 3, del Codice 84

7. La statistica 87

7.1. La statistica ufficiale 87
7.2. Istruttorie relative ai lavori statistici del Psn 89
7.3. *Data breach* nell'ambito della statistica ufficiale 92

8. I trattamenti in ambito giudiziario e da parte di Forze di polizia 93

8.1. Trattamenti in ambito giudiziario 93
8.2. Trattamenti da parte di Forze di polizia 94
8.3. Pareri resi su schemi di decreti in ambito giudiziario o in relazione ad attività di polizia 95
8.4. Il controllo sul Ced del Dipartimento della pubblica sicurezza 96
8.5. Il controllo sul Sistema di informazione Schengen 96
8.5.1. Follow up *della valutazione Schengen dell'Italia* 96
8.5.2. L'attività di controllo e monitoraggio del Garante sul Sistema SIS II 97

9. L'attività giornalistica 98

9.1. Dati statistici ed aspetti procedurali 98
9.2. Trattamento dei dati nell'esercizio dell'attività giornalistica 99
9.2.1. Dati giudiziari 99
9.2.2. Dati relativi a minori 100
9.2.3. Dati di personaggi noti 100
9.2.4. Pubblicazione di fotografie a corredo di articoli giornalistici 100
9.2.5. Notizie di rilevante interesse pubblico e rispetto dell'essenzialità dell'informazione 101

9.3. Attività svolta nei confronti di TikTok 103
9.4. Trattamento dei dati da parte dei motori di ricerca 104

10. Cyberbullismo e *revenge porn* 106

11. *Marketing* e trattamento di dati personali 107

11.1. Il fenomeno del *telemarketing* indesiderato e l'azione di contrasto 107
11.1.1. Il telemarketing *illegale nel settore telefonico* 107
11.1.2. Il telemarketing *illegale nel settore energetico* 109
11.1.3. Il telemarketing *illegale in altri settori commerciali* 109
11.1.4. Ulteriori violazioni nell'ambito del telemarketing *illegale* 110
11.1.5. Utilizzo di call-center *ubicati fuori dall'Unione europea* 111
11.1.6. Scenari evolutivi nel settore del telemarketing *illegale: il codice di condotta* 111
11.1.7. Marketing e *profilazione* 112
11.1.8. Attività svolte nell'ambito della tutela del consumatore nei servizi di comunicazione elettronica 112

12. Servizi di comunicazioni elettroniche e internet 114

12.1. Accesso all'*account* di posta elettronica 114
12.2. Conservazione ed accesso ai dati di traffico telematico e telefonico 115
12.3. *Cookie* e profilazione tramite utilizzo di nuove tecnologie 115
12.4. Raccolta e pubblicazione dati *online* 116
12.5. Violazione dei diritti dell'interessato in rete 117
12.6. Procedure IMI relative a trattamenti transfrontalieri di dati personali effettuati da fornitori di servizi della società dell'informazione 118
12.7. Altre attività di coordinamento a livello europeo 121

13. La protezione dei dati personali nel rapporto di lavoro privato e pubblico 123

13.1. Trattamenti di dati mediante dispositivi tecnologici nel rapporto di lavoro privato 123
13.2. Esercizio dei diritti 126
13.3. Omessa informativa 128
13.4. Trattamenti dei dati biometrici 129
13.5. Trattamento del dato relativo allo stato di gravidanza 130
13.6. Videosorveglianza nel settore privato 130
13.7. La protezione di dati nell'ambito del rapporto di lavoro pubblico. I trattamenti effettuati per finalità di prevenzione dal contagio da Sars-CoV-2 132
13.7.1. La vaccinazione anti Sars-Cov-2 come requisito professionale e le certificazioni verdi per accedere ai luoghi di lavoro 132
13.7.2. Trattamenti di dati personali nell'ambito di una campagna di screening *anti Covid-19: il ruolo del datore di lavoro* 133
13.7.3. Trattamenti di dati personali effettuati in occasione dell'accertamento del requisito vaccinale per i professionisti sanitari 133
13.8. Trattamento di dati nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti (cd. *whistleblowing*) 134
13.9. Trattamento di dati per finalità di gestione del rapporto di lavoro 135
13.9.1. Trattamento di dati nell'ambito di procedure concorsuali 135

Indice

13.9.2. Pubblicazione e condivisione di dati personali nel registro elettronico delle scuole 136
13.9.3. Circolazione di informazioni personali nei contesti lavorativi, anche nei sistemi di protocollazione informatica degli atti 136
13.10. Diffusione *online* di dati personali dei lavoratori 137
13.10.1. Pubblicazione di graduatorie e atti di procedure concorsuali 139
13.10.2. Dati personali di lavoratori in banche dati pubbliche 140

14. Le attività economiche 142
14.1. Trattamento di dati personali in ambito assicurativo 142
14.2. Trattamento di dati personali in ambito bancario-finanziario e sistemi di informazioni creditizie 143
14.3. Imprese 148
14.3.1. Modifiche ai tempi di conservazione dei dati relativi a inadempimenti non regolarizzati 150
14.4. Concessionari di pubblici servizi 150
14.5. Attività di recupero crediti 151
14.6. Procedure IMI relative a trattamenti di dati in ambito economico-produttivo 152

15. Altri trattamenti in ambito privato 155
15.1. Trattamento di dati personali nell'ambito del condominio 155
15.2. Trattamenti di dati da parte di associazioni e fondazioni 156

16. Intelligenza artificiale e diritto alla protezione dei dati personali 159

17. Violazione dei dati personali 163

18. Il trasferimento dei dati personali all'estero 164

19. L'attività ispettiva 166
19.1. L'attività ispettiva dopo l'emergenza pandemica 166
19.2. La collaborazione con la Guardia di finanza 167

20. Il contenzioso giurisdizionale 168
20.1. Considerazioni generali 168
20.2. Le opposizioni ai provvedimenti del Garante e le decisioni giudiziali di maggior rilievo 168
20.3. Il contributo del Garante nei giudizi in materia di protezione dati 174

21. Le relazioni comunitarie e internazionali 176
21.1. La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dei dati 176
21.2. La cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni 189
21.3. La partecipazione dell'Autorità in seno al Consiglio d'Europa, all'OCSE e ad altri gruppi di lavoro internazionali 191
21.4. Le conferenze internazionali ed europee 195
21.5. Le domande pregiudiziali davanti alla Corte di giustizia dell'Unione europea 196
21.6. I progetti per l'applicazione del RGPD finanziati dall'Unione europea 197

Indice

22. Attività di normazione tecnica internazionale e nazionale 199

23. L'attività di comunicazione, informazione e di rapporto con il pubblico 201

23.1. La comunicazione del Garante 201
23.1.1. I 25 anni dell'Autorità 201
23.2. I prodotti informativi 203
23.3. Il sito istituzionale, i prodotti multimediali e le pubblicazioni 204
23.4. Le manifestazioni e convegni 204
23.5. L'attività internazionale 205
23.6. L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi 205

24. Attività di studio e documentazione 208

III – L'UFFICIO DEL GARANTE

25. La gestione amministrativa e dei sistemi informatici 213

25.1. Il bilancio e la gestione economico-finanziaria dell'Autorità 213
25.2. L'attività contrattuale, la logistica e la manutenzione dell'immobile 214
25.3. L'organizzazione dell'Ufficio 216
25.4. "Autorità trasparente" e adempimenti relativi alla disciplina anticorruzione 218
25.5. Il settore informatico e tecnologico 219

IV – I DATI STATISTICI

Elenco delle abbreviazioni e degli acronimi più ricorrenti

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

Gepd	Garante europeo per la protezione dei dati
Gruppo Art. 29	Gruppo dei garanti europei istituto dall'art. 29 della direttiva 95/46/CE
G.U.	Gazzetta ufficiale della Repubblica italiana
GUUE	Gazzetta ufficiale dell'Unione europea
IA	Intelligenza artificiale
IMI	*Internal Market Information System*
Ivass	Istituto per la vigilanza sulle assicurazioni
IWGDPT	*International Working Group on Data Protection in Telecommunications*
l.	legge
lett.	lettera
Mef	Ministero dell'economia e delle finanze
Mise	Ministero per le imprese e il *made in Italy*
n.	numero
p.	pagina
p.a.	pubblica amministrazione/pubbliche amministrazioni
par.	paragrafo
Pec	posta elettronica certificata
Pnrr	Piano nazionale di ripresa e resilienza
provv.	provvedimento del Garante
r.d.	regio decreto
reg.	regolamento
RGPD o Regolamento	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
Rpd	Responsabile della protezione dei dati
Rpo	Registro pubblico delle opposizioni
Rspp	Responsabile del servizio prevenzione e protezione
See	Spazio economico europeo
sez.	Sezione
Spid	Sistema pubblico dell'identità digitale
Ssn	Servizio sanitario nazionale
tab.	tabella
T-PD	Comitato consultivo della Convenzione del Consiglio d'Europa n. 108/1981
t.u.	testo unico
TFUE	Trattato sul funzionamento dell'Unione europea
UE	Unione europea
Url	*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
2022

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

1 Introduzione

Anche nel 2022 il protrarsi dell'emergenza sanitaria dà solo parzialmente conto della attività del Garante, che trova una definizione d'insieme nella sua natura trasversale, costante nei 25 anni intercorsi dalla sua istituzione, al cui ricorrere sono state dedicate importanti iniziative di comunicazione e studio (cfr. cap. 23), volte sia a promuovere la consapevolezza degli obblighi imposti dalla normativa, sia all'approfondimento di complesse tematiche, quali quelle proprie della società dell'informazione.

Le relazioni istituzionali dell'Autorità, in particolare i pareri sugli atti normativi, in attuazione dell'art. 36, par 4, del RGPD, forniscono in questa prospettiva le grandi coordinate delle linee di azione dell'Autorità.

Come rilevato dal Presidente dell'Autorità nell'audizione dinanzi alla XII Commissione affari sociali della Camera dei deputati sul decreto-legge n. 1/2022, recante misure urgenti per fronteggiare l'emergenza Covid-19, (cfr. sez. IV, tabb. 3, 4, 5) i menzionati pareri, lungi dal rappresentare un passaggio burocratico, costituiscono presupposto essenziale per il corretto bilanciamento sotteso alle sempre più numerose norme che prevedono trattamenti di dati personali.

1 Executive Summary

The continuation of the health emergency in 2022 does not account, once again, for the whole gamut of the activities carried out by the Garante. Those activities can only be appreciated comprehensively by having regard to their cross-sectoral nature, which has been a standing feature in the 25 years since the Garante was set up. Indeed, this significant anniversary was celebrated by way of major media events and studies (see Chapter 23) which were meant both to raise awareness of the obligations arising from the law and to dig deeper into complex issues such as those related to the 'information society'.

The Garante's interactions with governmental and parliamentary bodies, in particular the opinions rendered on bills and draft legislation under Article 36(4) GDPR, do provide a bird's view of the main strands of activity from the Authority's perspective. As highlighted by the President of the Garante when he was heard by the XII Committee of the Italian Chamber of Deputies (Social Affairs) regarding decree-law 1/2022 on urgent measures to tackle the Covid-19 emergency (see Section IV, Tables 3 to 5), those opinions are by no means pieces of a bureaucratic puzzle; in fact,

In quel caso è stato richiamato con forza il principio di proporzionalità, in via generale sancito dall'art. 52 CDFUE per le limitazioni dei diritti fondamentali – e declinato in termini di minimizzazione dall'art. 5, par. 1, lett. *c*), del RGPD –, secondo cui come ribadito più volte dalla Corte di giustizia UE "le deroghe e le restrizioni alla tutela dei dati personali" devono intervenire "entro i limiti dello stretto necessario".

La verifica del rispetto dei principi di correttezza del trattamento, di minimizzazione, integrità e riservatezza dei dati è stata costante, segnatamente in materia di sanità.

Per quanto riguarda l'attestazione delle esenzioni all'obbligo di vaccinazione Covid-19 l'Autorità ha rappresentato l'esigenza, condivisa dal Ministero della salute, di introdurre uno strumento digitale analogo alle certificazioni verdi, per evitare che un impedimento alla vaccinazione fosse rivelato dalla presentazione di un documento cartaceo (provv. 27 gennaio 2022, n. 18, doc. web n. 9742129, cfr. par. 5.1).

Assai chiaro, nella prospettiva di accompagnare le trasformazioni sociali e l'innovazione tecnologica con la salvaguardia dei diritti fondamentali dei singoli, è il parere non favorevole (22 agosto 2022, n. 294, doc. web n. 9802729) reso sullo schema di decreto di riforma della disciplina di attuazione del Fse alla luce dello specifico investimento del Pnrr. Al riguardo l'Autorità ha evidenziato, tra l'altro, la necessità di: definire il perimetro di titolarità dei trattamenti e dei limiti di responsabilità dei soggetti coinvolti; delimitare adeguatamente l'accesso al Fse in emergenza per impossibilità dell'interessato o rischio grave ed imminente per la sua salute; specificare le misure volte al rispetto del diritto dell'interessato all'oscuramento dei suoi dati sanitari; accompagnare la riforma del Fse con una preventiva e adeguata

they are a fundamental prerequisite to achieve the appropriate balancing that must underpin the increasing number of laws and regulations where the processing of personal data is envisaged. In the case at issue, the Garante called for respecting the proportionality principle both as set out from a general standpoint in Article 52 of the CFR-EU regarding any limitations on fundamental rights and as mirrored in the data minimisation requirements under Article 5(1)(c) GDPR. Accordingly, and as repeatedly pointed out by the Court of Justice of the EU, 'any derogations from or limitations on the protection of personal data' are only allowed 'insofar as they are strictly necessary.'

The Garante has consistently focused on verifying compliance with lawfulness, minimisation, integrity and confidentiality requirements, especially in the health care sector. Concerning the certifications of exemptions from Covid-19 vaccination obligations, the need to rely on a digital tool as was the case with the 'green certifications' was pointed out and was also supported by the Italian Ministry of Health; this was aimed to avoid disclosure of the reasons preventing vaccination on account of the submission of a paper-based document (see Decision No 18 of 27 January 2022 – Paragraph 5.1).

The Garante rendered an unfavourable opinion (see Decision No 294 of 22 August 2022) on the draft decree reforming implementation of the Electronic Health Record (EHR) in the light of the specific NRRP-related investments – and in so doing, it signalled quite clearly that social transformations and technological evolution must go hand in hand with the protection of the fundamental rights of individuals. In this respect, the Garante emphasized, among other things, the need to determine controllership of the processing and liability

valutazione d'impatto, tenendo conto degli specifici rischi e dei significativi effetti dei trattamenti in parola.
Altro significativo parere non favorevole è stato reso su uno schema di decreto relativo alla realizzazione dell'Ecosistema dati sanitari (Eds) (22 agosto 2022, n. 295, doc. web n. 9802752), osservando tra l'altro che questo comporta una duplicazione dei dati e dei documenti generati per finalità di cura, costituendo una banca dati (*data repository* centrale) che acquisisce ed elabora le informazioni per offrire servizi agli esercenti le professioni sanitarie, al Ministero della salute, alle regioni/province autonome e allo stesso interessato; è stato inoltre richiesto di delimitare adeguatamente i dati trasmessi al sistema, precisare le sfere di competenza dei diversi soggetti in esso coinvolti, chiarire l'ambito di operatività del consenso dell'interessato e le conseguenze della sua eventuale revoca.
L'esigenza di assicurare la tutela dei diritti e delle libertà degli interessati emerge con particolare rilievo anche a fronte dei rischi derivanti dal trattamento su larga scala, con strumenti di intelligenza artificiale, vieppiù quando si tratta di dati sensibili.
In tal senso rileva la valutazione d'impatto sottoposta dall'Agenzia delle entrate in relazione ad un trattamento volto ad analizzare rischi e fenomeni evasivi/elusivi tramite i dati contenuti nell'Archivio dei rapporti finanziari ed il loro incrocio con quelli delle altre banche dati dell'Agenzia, ossia con tutte le tipologie di dati personali che costituiscono l'immenso patrimonio informativo nella sua disponibilità. L'Autorità ha al riguardo evidenziato che tra i principali rischi connessi all'utilizzo di modelli di analisi stocastica con tecniche di *machine learning* vi sono quelli relativi a potenziali opacità nella fase di sviluppo dell'algoritmo, errori e distorsioni di diversa natura (cd. *bias*), che impongono di

of the different entities involved; to adequately restrict access to the EHR in emergency situations, which should be limited to the data subject's incapability or to the risk of severe, impending harm to their health; to set out the measures ensuring compliance with the data subject's right to have their health data redacted; to carry out an adequate DPIA prior to implementing any amendments to the EHR by taking due account of the specific risks and significant effects on the processing at issue.
An unfavourable opinion was also rendered on a draft decree concerning the so-called 'health data eco-system' (see decision no 295 of 22 August 2022); the Garante pointed out, among other things, that such an eco-system would entail duplication of treatment-related data and documents by setting up a centralised data repository to acquire and process information and thereby provide services to health care professionals, the Ministry of Health, Regions and data subjects. The Authority requested additionally that the data transmitted to the system be minimised as appropriate, the respective competences of the entities involved be detailed, and the consequences arising from the data subject's giving or withdrawing their consent be clarified.
The need for ensuring the protection of data subjects' rights and freedoms is especially evident in the face of the risks resulting from large-scale processing activities based on AI tools – the more so if special category (sensitive) data are involved.
From this standpoint, mention should be made of the data protection impact assessment submitted by the Italian Revenue Agency in connection with processing activities that were meant to investigate into the risk and/or the occurrence of tax evasion/dodging. To that end, the information stored in the

commisurare le misure da adottare alle caratteristiche delle banche dati di volta in volta utilizzate ed ai modelli di analisi impiegati (provv. 30 luglio 2022, n. 276, doc. web n. 9808839). È stato pertanto richiesto, tra l'altro, di effettuare specifiche verifiche sulla qualità dei modelli di analisi impiegati; di documentare periodicamente le metriche utilizzate, le attività svolte, eventuali criticità e le misure di conseguenza adottate, coinvolgendo anche il Rpd, ed aggiornando, se necessario, la valutazione di impatto. Il Garante ha altresì segnalato l'esigenza di potenziare l'intervento umano nella formazione dei *dataset* di analisi e di controllo, formare il personale coinvolto al fine di assicurare la comprensione delle capacità e dei limiti del processo algoritmico, nonché di garantire che gli operatori, in qualsiasi situazione particolare, possano se del caso ignorare l'*output* del processo algoritmico, evitando la possibile tendenza a farvi automaticamente affidamento.

Rischi elevati per i diritti e le libertà fondamentali degli interessati sono stati rilevati anche a fronte di trattamenti non massivi, come quelli oggetto della delega dell'interessato ad un terzo per la richiesta di servizi erogati *online* da parte degli aderenti al Sistema di gestione deleghe (Sgd), previsto dall'art. 64-*ter*, comma 7, d.lgs. 7 marzo 2005, n. 82 (Cad) (cfr. par. 4.8).

L'Autorità, nel parere sul relativo d.P.C.M., nonché sul d.m. concernente lo schema di manuale operativo e sulla valutazione d'impatto ha in primo luogo segnalato (provv. 24 febbraio 2022, n. 74, doc. web n. 9752853) l'esigenza di evitare che soggetti che non hanno acquisito i necessari poteri in conformità alle vigenti disposizioni di legge si ritrovino a trattare dati personali del delegante in forza della semplice esibizione di una copia digitale di un documento di identità e di una delega, a tal fine in-

Register of holders of financial positions [Archivio dei rapporti finanziari] would be matched with the information stored in the other databases held by the Agency – i.e. with all the categories of personal data making up the huge information repositories of the Agency. The Garante pointed out in this respect that one of the key risks in using stochastic analysis models based on machine learning consisted in possible flaws affecting development of the relevant algorithms along with biases and errors of various types; accordingly, the measures to be implemented must be adjusted to the features of the databases relied upon from time to time as well as to the analytical models involved (see Decision No 276 of 30 July 2022). For this reason, the Garante requested, among other things, that specific checks be carried out on the quality of such analytical models, and that the parameters relied upon, the activities performed, any criticalities and the measures taken to deal with such criticalities be documented on a regular basis by involving the Agency's DPO and updating the impact assessment as necessary. Additional requirements laid out by the Garante included enhancing the role of human interventions in creating analysis and control datasets, training the staff involved so as to make them fully aware of the potentialities and limitations of algorithmic processes, and ensuring that operators would be enabled, at any specific time, to disregard algorithmic outputs so as to prevent automatic reliance on such outputs.

High risks to the data subjects' rights and fundamental freedoms were also found in connection with processing activities that are not massive in nature, such as those resulting from the data subject's delegating a third party to request online services as delivered by the entities that are part of the so-called Delegation Management System

dividuando puntualmente alcune criticità, non pienamente superate nel d.m. 30 marzo 2022 poi adottato, come rilevato dall'Autorità nel successivo provv. 6 ottobre 2022, n. 330 (doc. web n. 9823221).

La verifica, ad istanza di parte ovvero d'ufficio, della legittimità dei trattamenti di dati su larga scala, ad opera dei *media*, richiede decisioni adeguate alle peculiarità dei diversi casi. In applicazione della direttiva 680/2016 i dati personali sono peraltro protetti anche nei confronti delle autorità di contrasto al crimine, come nel caso in cui è stata ritenuta illegittima la divulgazione dell'immagine in primo piano dell'interessato, in stato di detenzione carceraria già da qualche mese, da parte di una questura nel corso di una conferenza stampa in cui si dava notizia di un ulteriore provvedimento restrittivo nei confronti del medesimo interessato (provv. 24 febbraio 2022, n. 62, doc. web n. 9766469).

In particolare in tema di essenzialità dell'informazione si menziona l'accoglimento di un'istanza che lamentava la pubblicazione integrale, in una rivista di carattere giuridico, di un'ordinanza della Suprema Corte concernente il riconoscimento in Italia di un provvedimento di adozione di un minore da parte di una coppia omosessuale emesso da un giudice statunitense, nonostante sull'ordinanza fosse stata apposta – d'ufficio – l'annotazione (art. 52 del Codice) di omettere le generalità degli interessati in caso di riproduzione o diffusione dell'atto (provv. 28 aprile 2022, n.157, doc. web n. 9779098).

L'esigenza di protezione è particolarmente stringente per prevenire e contrastare il fenomeno della diffusione, con intenti vendicativi e comunque in assenza del consenso della persona interessata, di immagini a contenuto sessualmente esplicito (*revenge porn*) alla luce di specifica normativa, confluita nell'art. 144-

(which was set up by the consolidated law on digital administration, No 82 of 7 March 2005 – see paragraph 4.8 in the Annual Report). The Garante pointed out, in the first place (see the opinion issued both on the draft decree by the Prime Minister's Office and on the Ministerial decree containing the draft operating manual and impact assessment - Decision No 74 of 24 February 2022), that it was necessary to prevent the processing of personal data relating to the individual delegating a third party by entities that are not empowered to do so in accordance with the legislation in force – since their empowerment would only result from their holding a digital copy of that individual's ID along with the delegation instrument. The criticalities highlighted by the Garante in this respect were not addressed in full by the subsequent Ministerial decree of 30 March 2022, which was recalled in the Garante's additional decision on this issue (No 330 of 6 October 2022).

Checking on lawfulness of large-scale processing by media outlets requires making decisions that are adjusted to the peculiarities of the individual cases – whether resulting from complaints or based on own-volition inquiries. It should be recalled that Directive 2016/680 safeguards personal data also when processed by law enforcement authorities. This is the case of a decision finding that disclosure of the close-up picture of an individual was unlawful as that individual was already serving a sentence and a press conference had been convened by the police to inform about the imposition of additional corrective measures on the said convict (see Decision No 62 of 24 February 2022).

Regarding the notion of materiality of the information disclosed, reference can be made to a decision granting a complaint against the publication in a legal journal of the full text of an order by the

bis del Codice. A tal fine è stato inserito nel regolamento del Garante n. 1/2019 un apposito articolo (art. 33-*bis*) dedicato alla disciplina del procedimento da seguire nella gestione delle segnalazioni di *revenge porn*. È stata inoltre prevista l'introduzione di un modello di segnalazione telematica per gli interessati, definendo un percorso differente a seconda che si tratti di utenti dotati di una identità digitale e quindi autenticati, oppure di utenti non autenticati.

Circa il trattamento di dati personali nella rete (v. par. 9.3), particolarmente complessa la vicenda relativa all'invio di pubblicità personalizzata da parte di un noto *social network* sulla base della profilazione degli utenti, senza il loro consenso. In questo caso il Garante è intervenuto direttamente in via d'urgenza in base alla direttiva europea 2002/58, cd. direttiva *e-privacy*, attuata dall'art. 122 del Codice, quindi al di fuori della procedura di cooperazione prevista dal RGPD attraverso il cd. sportello unico, che avrebbe visto l'esercizio dell'iniziativa da parte dell'Autorità di protezione dati irlandese, Paese ove il *social network* ha fissato il proprio stabilimento principale.

Al di fuori dell'ambito di applicazione della direttiva *e-privacy* la regola generale è la cooperazione tra le autorità europee, nei diversi meccanismi previsti dal RGPD, che trova estesa applicazione per i trattamenti collocati nel contesto di attività economiche. Nei casi transfrontalieri di importanza strategica, individuati dal Comitato europeo per la protezione dei dati secondo criteri qualitativi e quantitativi (quali il numero elevato di interessati coinvolti, l'interazione fra protezione dei dati e altri ambiti giuridici), per potenziare la cooperazione vengono creati gruppi di lavoro ristretti di autorità di protezione dei dati sotto la guida dell'autorità capofila.

Non sfocia in provvedimenti del Garante

Italian Court of Cassation. The Court had recognised, by way of that order, a decree for the adoption of a child by a homosexual couple which had been issued by a US judge; however, the order in question bore the notice – pursuant to Section 52 of the Italian Data Protection Code – requiring the data subjects' names to be redacted if the order was reproduced or published (see Decision No 157 of 28 April 2022).

Strong safeguards are especially necessary to prevent and counter the so-called revenge porn, that is, the dissemination of sexually explicit materials for retaliation and anyhow without a person's consent. Specific provisions are now set out in Section 144-a of the Italian DP Code, and an ad-hoc Section (33-a) in the Garante's Rules of Procedure 1/2019 regulates the handling of revenge porn notifications. An online form to report revenge porn situations was made available on the Garante's website and different procedures are envisaged depending on whether the reporting entity is digitally authenticated or not.

As for the processing of personal data on the Internet (see paragraph 9.3), an especially complex case related to the sending of customised ads by a well-known social media platform based on users' profiling without consent. The Garante stepped in directly and urgently in accordance with the e-privacy directive (2002/58), which was transposed by way of Section 122 of the DP Code and does not entail application of the so-called one-stop-shop cooperation procedure under the GDPR – otherwise, the Irish data protection authority would have acted as the lead supervisory authority, since the social platform in question has its main establishment in Ireland.

Apart from the subject matters falling within the scope of the e-privacy directive, the cooperation rules set out in the

te, quando non siano sollevate obiezioni pertinenti e motivate ai sensi dell'art. 60, par. 4 del RGPD, la complessa valutazione degli schemi di decisioni predisposti dalle altre autorità che nei singoli casi rivestano il ruolo di capofila.
Non si concludono con provvedimenti collegiali neppure le segnalazioni e i reclami archiviate dai singoli Dipartimenti, talvolta in relazione ad istanze palesemente infondate, comunque in esito ad uno scrupoloso esame di quanto prospettato, e sempre con trasparente motivazione della decisione – in qualche caso impugnata in giudizio – di non definire il procedimento con una deliberazione del Collegio. Di alcune delle decisioni di maggior rilievo si dà conto nel testo.
Nel settore delle attività economiche, che, per la sua granularità presenta casistiche eterogenee riferite ad una variegata pluralità di titolari e responsabili operanti in diversi Stati membri, si menziona in particolare il caso di un distributore di energia, sanzionato per l'illecito trattamento dei dati dei clienti inerenti all'indennizzo CMOR (corrispettivo di morosità), che nel passaggio del cliente ad un nuovo fornitore consente al venditore uscente di recuperare eventuali crediti non riscossi, tramite un articolato meccanismo di riparto di competenze economiche e di trasmissione di flussi di comunicazione. In questo caso la restituzione al Sistema informativo integrato di informazioni inesatte e non aggiornate sulla morosità aveva effetti pregiudizievoli anche per i clienti finali, impossibilitati a passare ad altro venditore nel libero mercato (provv. 24 novembre 2022, n. 390, doc. web n. 9832979).
Da questi riferimenti è evidente la natura interdisciplinare delle valutazioni dell'Autorità, concernenti da un lato le regole proprie del settore nel quale il trattamento dei dati si inserisce (che ne determinano le finalità e quindi consen-

GDPR by way of different mechanisms are generally applicable; this is especially so with the processing operations by business entities. It should be noted that such cooperation was fostered by the EDPB in respect of strategic cross-border processing cases as identified through both quantitative and qualitative criteria – such as a high number of concerned data subjects or the interplay between data protection and other legal frameworks. In particular, working groups are set up including a small number of concerned supervisory authorities to take care of the interactions with the lead supervisory authority.
It should also be recalled that the complex evaluation of the draft decisions submitted by the lead supervisory authorities in cross-border cases does not result into decisions by the Board of the Garante – except where it entails the raising of relevant and reasoned objections pursuant to Article 60(4) GDPR.
The same applies to all the decisions on complaints or alerts that are dismissed by the individual competent departments at the Garante. In some cases, the complaints prove to be clearly unsubstantiated, but all cases are evaluated thoroughly and clear reasons are provided for the dismissal decisions – a few of which have been challenged in court. The most significant ones among such decisions are summarised in the Annual Report.
The data protection issues arising in connection with processing activities by businesses are highly multifarious on account of the multiplicity of controllers and processors operating from different EU Member States. Reference can be made here to a utility company which was fined because of the unlawful processing of data relating to customers who had defaulted on payments. Whenever such customers shift to a different utility company, the former provider is

tono di delimitarne l'ambito) e dall'altro, molto frequentemente, complessi profili di tecnologia dell'informazione. Ciò anche per quanto riguarda i cd. *data breach*: ricevute le segnalazioni, l'Autorità esamina l'adeguatezza delle misure adottate per porre rimedio alla violazione dei dati personali o per attenuarne i possibili effetti negativi nei confronti degli interessati, e valuta la necessità di comunicare la violazione agli interessati coinvolti, fornendo indicazioni specifiche sulle misure da adottare per proteggersi da eventuali conseguenze pregiudizievoli (cfr. cap. 17).

Nell'insieme, a fronte di trattamenti così strutturati ed elaborati, effettivi poteri di controllo sul rispetto dei diritti del singolo e sul modello di società che in questa prospettiva si può prefigurare richiedono all'Autorità una capacità di analisi adeguata ad esercitare le sue funzioni di garanzia in posizione di reale indipendenza e con concreta autonomia di valutazione.

Parte non secondaria del quadro d'insieme è costituita dalla dimensione sovranazionale che caratterizza questo tipo di relazioni, oggetto delle regole di protezione dati, come indicano, in materia di intelligenza artificiale, tra l'altro, gli approfondimenti cui l'Autorità ha contribuito entro la cerchia della *Global privacy assembly* (GPA) nonché la memoria presentata il 9 marzo 2022 in occasione dell'audizione informale avanti alle Commissioni IX e X riunite della Camera dei deputati a margine della proposta di regolamento (UE) sull'intelligenza artificiale (cfr. doc. web n. 9751565).

Per quanto più direttamente riguarda la dimensione europea, tra i risultati della laboriosa partecipazione alle attività del Comitato (15 riunioni plenarie e 162 riunioni dei sottogruppi) relative all'applicazione del Regolamento e della direttiva *law enforcement,* v. par. 21.1

entitled by law to collect unpaid debt by means of a complex mechanism to allocate debt and communicate the relevant information. In the case at issue, inaccurate as well as outdated information had been entered in the integrated information system regarding defaults, which had also affected end-customers since they had been prevented from shifting to different utility providers on the free market (see Decision No 390 of 24 November 2022).

The foregoing overview points quite clearly to the multidisciplinary nature of the assessment the Garante carries out; indeed, account must be taken on the one hand of sector-specific rules applying to the individual processing – which regulate the purposes of the processing and allow determining the relevant scope – whilst, on the other hand, complex IT issues are very frequently to be tackled. This applies to the so-called data breaches as well. Having received the required notifications, the Garante assesses adequacy of the measures implemented to remedy or mitigate the effects produced by the personal data breach on data subjects along with the need to communicate the breach to the data subjects concerned; additionally, specific indications are provided on the measures to be taken in order to avert prejudicial effects (see Chapter 17).

From a general perspective, the Garante is required to exercise effective oversight on respect for the rights of individuals and the societal model that is taking shape in this context when faced with highly structured and complex processing activities such as those recalled above. This requires the Garante, in turn, to be equipped with analytical capabilities that can allow it to exercise its supervisory powers in a truly independent manner and on the basis of factually autonomous assessment procedures.

A far from ancillary role is played against

si segnalano, a titolo esemplificativo, il parere congiunto del Cepd e del Gepd sulla proposta di regolamento del Parlamento e del Consiglio per prevenire e combattere gli abusi sessuali sui minori, le linee guida 5/2022 sul riconoscimento facciale nel settore delle attività di polizia e giudiziarie e, per quanto più direttamente riguarda lo svolgimento delle funzioni istituzionali, le nuove linee guida sul calcolo delle sanzioni amministrative, sottoposte a consultazione pubblica, che armonizzano la metodologia utilizzata dalle autorità per la protezione dei dati, rinviando al testo per l'attività svolta in ambito OCSE e Consiglio d'Europa.

Il Garante quale interlocutore di soggetti pubblici e privati trova nel dialogo con la magistratura, segnatamente con la giurisdizione ordinaria che conosce delle sue decisioni, il suo punto di riferimento, e anche quando le sentenze non ne confermano gli orientamenti registra comunque attenta considerazione delle valutazioni svolte in relazione ai singoli casi. Particolare rilievo acquista, tra le diverse decisioni del 2022, l'ordinanza con cui la Suprema Corte, riformando senza rinvio la sentenza di primo grado, ha ritenuto legittimo l'ordine impartito dal Garante (provv. 26 ottobre 2017, n. 445, doc. web n. 7323489) ad un motore di ricerca in rete di deindicizzare globalmente, e non solo sulle versioni europee del motore stesso, i risultati reperibili in associazione al nominativo dell'interessato, in quanto "non vi è dubbio che il diritto alla protezione dei propri dati personali e il suo fondamento costituzionale non tollerino limitazioni territoriali all'esplicazione della sfera di protezione, tanto più che nella specie tale diritto si sovrappone e si accompagna ai diritti all'identità, alla riservatezza e alla contestualizzazione delle informazioni" (Cass. civ. 15 novembre 2022, n. 34658). I riferimenti contenuti nella

this background by the supranational dimension of data protection rules. As regards artificial intelligence, reference can be made to the contributions provided by the Garante to the ongoing debate within the Global Privacy Assembly (GPA) as well as to the submission made by its President to the joint Committees IX and X of the Italian Chamber of Deputies concerning the draft EU artificial intelligence Regulation.

As for the European dimension, examples of the substantial contributions given by the Garante to the activities of the European Data Protection Board – which met 15 times in a plenary format and held 162 meetings of expert subgroups – in implementing both the GDPR and the law enforcement directive (see Para. 21.1) include the joint EDPB-EDPS opinion on the draft regulation to prevent and counter sexual abuse on minors, the 5/2022 guidelines on facial recognition in the law enforcement sector, and the recent guidelines on the calculation of administrative fines which are meant to harmonise the approach followed by data protection authorities in this area. Specific information on the activities carried out within other forums such as the OECD and the Council of Europe can be found in the relevant paragraphs of the Annual Report.

The dialogue struck up with the judiciary provides key inputs to the Garante, which is called upon to interact with both public and private entities. The decisions by the Garante may be challenged before judicial authorities, which carefully consider the analysis performed by the Garante in the individual cases even when they do not uphold those decisions. Special importance can be attached as for the case-law of 2022 to an order whereby the Court of Cassation quashed the judgment rendered by the first-instance court and thus found that

menzionata ordinanza ad una decisione del Garante francese ed alle sentenze in argomento della Corte di giustizia, oltre che a precedenti della stessa Suprema Corte, dànno una chiara visione della complessiva dimensione del tema, delle sue implicazioni e delle finalità di protezione perseguite dall'Autorità.

***

Il testo di seguito dà conto analiticamente di ciò che in questa introduzione si è schematizzato, cercando soprattutto di indicare i diversi piani sui quali si svolgono le funzioni istituzionali, nella medesima prospettiva di tutela e garanzia della persona e dei suoi dati nello svolgimento delle sue relazioni. Giova aggiungere che nel meccanismo di protezione dei dati personali, oltre ai Garanti, al Comitato, ed ai giudici che si pronunciano sulla legittimità dei loro atti, hanno un ruolo fondamentale i singoli, il cui esercizio dei diritti, alla base del sistema, rappresenta uno strumento indispensabile per assicurarne la coesione e per affrontare i profondi cambiamenti del contesto nel quale l'Autorità opera.

the Garante could legitimately order a search engine to delist the search results obtained from the data subject's name globally, i.e., not only in the European versions of the search engine. The Court stated that 'it is unquestionable that the right to the protection of one's personal data and the Constitutional foundations of this right do not admit of any geographical limitation on the scope of the protection; this is all the more so if one considers that the right at issue overlaps and is paired with the rights to one's identity and privacy and to contextualised information.' (see decision No 34658 of 15 November 2022). The reference made by the Court to a decision by the French supervisory authority as well as to relevant judgments by the Court of Justice of the EU and to its own case-law does highlight the multifarious implications of the issues at stake but also the protection objectives underpinning the Garante's activity.

***

The Annual Report will provide more substantial elements to the summary overview contained in this Foreword, which is meant above all to point to the different levels at which the Garante operates whilst acting consistently from the same perspective – i.e., protecting and safeguarding individuals and their data in all their interactions. As well as the supervisory authorities, the European Data Protection Board, and the courts gauging the legitimacy of the actions by those authorities, the individual data subjects have a key role to play in the data protection framework. By exercising their rights, they lay the foundations for the whole framework and provide the indispensable cement to make it sound and capable to address the deep-ranging changes of the environment in which the Garante operates.

2 Il quadro normativo in materia di protezione dei dati personali

Nel 2022 sono stati approvati numerosi provvedimenti normativi rilevanti (pur in diversa misura), in termini di protezione dei dati personali. Nell'impossibilità di descriverli tutti, si analizzano di seguito gli atti normativi maggiormente incidenti sulla materia.

2.1. *Le leggi*

Legge di bilancio 2023

La legge 29 dicembre 2022 n. 197, recante il bilancio di previsione dello Stato per l'anno finanziario 2023 e il bilancio pluriennale per il triennio 2023-2025, prevede alcune disposizioni di interesse in materia di protezione dei dati personali tra le quali si segnalano, in particolare, le seguenti:

- il comma 323 dell'art. 1, recante modifiche all'art. 10, d.lgs. 15 settembre 2017, n. 147 (Disposizioni per l'introduzione di una misura nazionale di contrasto alla povertà) relativamente alle misure di semplificazione in materia di Isee e presentazione della Dsu in forma semplificata, con rinvio a successivo decreto del Ministro del lavoro e delle politiche sociali, sentiti l'Inps, l'Agenzia delle entrate e il Garante, per l'individuazione delle modalità operative, delle ulteriori semplificazioni e delle modalità tecniche per consentire al cittadino la gestione della dichiarazione precompilata resa disponibile in via telematica dall'Inps, fermo restando quanto previsto dal d.P.C.M. n. 159/2013 per quanto attiene al trattamento dei dati e alle misure di sicurezza;
- il comma 684 dell'art. 1 nel quale è confluito un emendamento del Governo (n. 123.01.000) in materia di intercettazioni, tracciamento delle comunicazioni e acquisizione dei dati di traffico da parte dei Servizi di informazione per la sicurezza che, oltre a imputare le spese al relativo comparto (anche per evitare la circolazione delle informazioni sulle spese, recanti elementi riservati, al di fuori del circuito *intelligence*), ne modifica anche la disciplina, autonomizzandola da quella delle intercettazioni volte alla prevenzione di gravi reati (art. 226 disp. att. c.p.p.) cui, invece, l'art. 4, d.l. n. 144/2005, convertito, con modificazioni, dalla l. n. 155/2005, nel suo testo previgente, rinviava integralmente. Si segnalano, in particolare, i seguenti aspetti:
  - la soppressione del riferimento – che resta invece per le intercettazioni preventive di polizia – al contenuto dell'obbligo motivazionale del provvedimento autorizzatorio del Procuratore della Repubblica, relativo alla sussistenza di elementi investigativi che giustifichino l'attività di prevenzione e alla ritenuta (da parte dell'Autorità giudiziaria) necessità del compimento dell'atto. La norma proposta prevede ora che le intercettazioni siano autorizzate "quando risultano sussistenti le condizioni" che le giustificano, ossia quando siano ritenute indispensabili per l'espletamento delle attività rimesse alle Agenzie. Si esclude, dunque, la necessità che l'istanza sia sorretta da "elementi investigativi" giustificanti la captazione, alleggerendo l'onere motivazionale della richiesta, sebbene comunque il decreto autorizzatorio debba, in quanto motivato, riferirsi alla ritenuta indispensabilità delle operazioni. Resta fermo

l'onere motivazionale relativo alla sussistenza di ragioni che rendano necessaria la proroga (eventuale) dell'intercettazione;
- per una diversa formulazione della norma rispetto all'attuale, per l'acquisizione dei tabulati e il tracciamento delle comunicazioni non è più previsto il requisito della necessità investigativa né il deposito di elementi a supporto, ma la (sola) mera finalizzazione di tali operazioni all'espletamento delle attività (genericamente indicate) demandate ai Servizi. I tabulati vanno distrutti entro sei mesi (termine prorogabile massimo a 24 su autorizzazione del Procuratore generale, ma senza più il requisito della indispensabilità per la prosecuzione dell'attività di prevenzione);
- l'estensione da 5 (prorogabili a 10) a 30 giorni (addirittura a 6 mesi dietro autorizzazione del Procuratore generale, in presenza di particolari esigenze di natura tecnica e operativa) del termine massimo di differimento previsto per il deposito dei verbali delle operazioni e dei contenuti intercettati;
- l'espressa attribuzione anche al Procuratore generale dell'onere della distruzione dei contenuti e verbali anche da lui detenuti, ad eccezione dei decreti autorizzatori, una volta adempiuti gli obblighi di comunicazione al Copasir;
- la soppressione della possibilità (prima prevista in via generale per tutte le captazioni preventive) di utilizzo ai soli fini investigativi dei risultati delle intercettazioni (e delle altre operazioni descritte), pur restando fermo il dovere degli organismi di comunicare notizie di reato alla polizia giudiziaria, la quale a sua volta è tenuta a riferirne al pubblico ministero.

Legge di delegazione europea

La legge 4 agosto 2022, n. 127, delega il Governo al recepimento delle direttive e all'attuazione di altri atti normativi dell'Unione europea. Tra le norme di interesse si segnalano, in particolare, le seguenti, relative:

a) all'adeguamento della normativa interna al regolamento (UE) 2018/1727, che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (nuovo Eurojust), sostituisce e abroga la decisione 2002/187/GAI del Consiglio, nonché alle disposizioni del regolamento (UE) 2018/1805, relativo al riconoscimento reciproco dei provvedimenti di congelamento e confisca (artt. 11 e 12);

b) all'attuazione della direttiva (UE) 2019/1937, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (art. 13);

c) all'adeguamento della normativa nazionale al regolamento (UE) 2019/816 che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di Paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726) (art. 14);

d) all'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2021/784, relativo al contrasto della diffusione di contenuti terroristici *online* (art. 15).

Sul provvedimento è stato audito al Senato, l'8 marzo 2022, il Presidente dell'Autorità, il quale si è soffermato in particolare sull'analisi degli artt. 13 e 14 recanti le deleghe legislative, rispettivamente, per il recepimento della direttiva sul *whistleblowing* e per l'adeguamento dell'ordinamento interno al regolamento 2019/816 sul sistema ECRIS-TCN.

Si è preliminarmente ricordato come il recepimento della direttiva (UE) 2019/1937 sul *whistleblowing* incida in maniera significativa sul quadro regolatorio vigente in materia, sia sotto il profilo soggettivo che oggettivo, risultando la tutela del segnalante estesa tanto al settore pubblico quanto a quello privato. Si sono poi analizzate le implicazioni della previsione relativa alla "divulgazione pubblica",

ammessa dalla direttiva, a certe condizioni, da parte del segnalante, al contrario di quanto previsto dalla normativa interna. Si è dunque ritenuta opportuna la realizzazione, in fase di esercizio della delega – con l'auspicato coinvolgimento del Garante – di un congruo bilanciamento tra l'esigenza di riservatezza della segnalazione, funzionale alla tutela del segnalante, la necessità di accertamento degli illeciti e il diritto di difesa e al contraddittorio del segnalato.

Con riferimento all'adeguamento dell'ordinamento interno al regolamento 2019/816, sull'istituzione di un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di Paesi terzi e apolidi (ECRIS-TCN), il Presidente dopo aver ricordato il parere 11/2017, reso dal Garante europeo per la protezione dei dati sullo schema di regolamento – che già sottolineava l'opportunità di una generale valutazione della proporzionalità e necessità della costituzione di un sistema informativo centralizzato *ad hoc* – ha rimarcato la necessità – nonostante i ridotti margini di discrezionalità del legislatore interno in ragione della natura regolamentare dell'atto – di assicurare, nella norma di adeguamento, il più congruo bilanciamento tra le esigenze di giustizia e la riservatezza individuale. Ha, peraltro, evidenziato che in tal senso depone anche il criterio direttivo di cui alla lett. *b*) della norma di delega, che sarebbe stato tuttavia più corretto riformulare estendendo la clausola di salvaguardia alla normativa (anche) interna di protezione dei dati.

Nell'ambito dell'audizione, il Presidente ha avuto modo di esprimere rilievi anche su di un emendamento (n. 13.01) presentato in Commissione e non approvato, che al comma 4 dell'art. 13 prevedeva di inserire, tra i principi di delega, l'attribuzione al Garante del ruolo di Istituzione nazionale indipendente per la protezione e promozione dei diritti umani, ai sensi della risoluzione dell'Assemblea generale delle Nazioni Unite 20 dicembre 1993, n. 48/134, al fine di promuovere e tutelare i diritti fondamentali della persona riconosciuti dalla Costituzione e dalle convenzioni internazionali di cui l'Italia è parte. A tal fine, funzioni e poteri del Garante venivano conseguentemente estesi alla materia dei diritti umani complessivamente intesa, con le conseguenti rimodulazioni organizzative della struttura. Nell'esprimere condivisione per la soluzione proposta, il Presidente ha sottolineato come l'Autorità offra, per criteri e procedure di nomina, garanzie ordinamentali di indipendenza certamente adeguati e che, in favore della scelta del Garante, depongono la trasversalità degli ambiti d'intervento e la varietà dei contesti considerati nell'esercizio delle sue funzioni.

Legge concorrenza

La legge annuale per il mercato e la concorrenza, 5 agosto 2022, n. 118, comprende varie disposizioni particolarmente rilevanti sotto il profilo della protezione dei dati personali. Esse sono state oggetto di analisi, da parte del Garante, nell'ambito della memoria inviata alla 10ª Commissione del Senato il 16 febbraio 2022.

La memoria ha analizzato, in primo luogo, la delega al Governo, di cui all'art. 2, comma 1, per la mappatura e la trasparenza dei regimi concessori di beni pubblici, da realizzarsi attraverso la costituzione e il coordinamento di un sistema informativo di rilevazione (e trasmissione telematica) delle concessioni, al fine di promuovere la massima pubblicità e trasparenza, anche in forma sintetica, dei principali dati e delle informazioni relativi a tutti i rapporti concessori. In relazione alla norma, si è sottolineata l'opportunità che sullo schema di decreto legislativo venisse acquisito il parere del Garante, in ragione della rilevanza, quantitativa e qualitativa, del sistema informativo da istituire e delle informazioni soggette alle forme di trasparenza previste.

Gli artt. da 15 a 21 della legge recano, inoltre, disposizioni in materia sanitaria, con particolare riguardo alle modalità di accreditamento, distribuzione e rimborsabilità

dei farmaci equivalenti, alla revisione del sistema di produzione dei medicinali emoderivati da plasma italiano e alla selezione della dirigenza sanitaria. Tra questi ultimi di particolare interesse risultano gli artt.15 e 20 dell'attuale testo, rispetto ai quali si è suggerito l'utilizzo di forme aggregate per la pubblicazione, sul sito internet degli enti, delle aziende e delle strutture pubbliche e private eroganti prestazioni per conto del Ssn, dei dati sugli aspetti qualitativi e quantitativi dei servizi erogati e dell'attività medica svolta. Rispetto, invece, alla previsione della pubblicazione dei *curricula* dei candidati, dei criteri di attribuzione del punteggio e della graduatoria, si è suggerito di introdurre il riferimento ai tempi massimi di pubblicazione per i dati personali dei soggetti non selezionati, da commisurare ad esempio a quelli utili per impugnare la graduatoria finale, nonché all'obbligo di adozione di tecniche per evitare l'indicizzazione dei dati personali nei motori di ricerca generalisti. I rilievi non sono stati, tuttavia, recepiti nel testo finale della legge.

Tra le disposizioni in materia di infrastrutture digitali e servizi di comunicazione elettronica (artt. da 22 a 25) rileva, inoltre, l'art. 24 che, al fine di contrastare il fenomeno delle attivazioni inconsapevoli e fraudolente di servizi di telefonia e di comunicazioni elettroniche, vieta ai soggetti gestori di tali servizi l'attivazione, in assenza del consenso espresso e documentato del consumatore o dell'utente, di servizi in abbonamento da parte degli operatori stessi o di terzi, inclusi i servizi per l'erogazione di contenuti digitali forniti sia attraverso sms e mms, sia tramite connessione dati, con addebito su credito telefonico o documento di fatturazione, offerti sia da terzi, sia direttamente dagli operatori. In tale contesto, si è avuto modo di sottolineare come la modifica, in sostanziale continuità con la norma vigente, potrebbe non essere del tutto sufficiente al contrasto delle condotte elusive, demandando all'operatore solo l'onere di verificare la sussistenza di un consenso "espresso e documentato", senza tuttavia normare le specifiche modalità di documentazione della manifestazione di volontà.

L'articolo 27, inoltre, conferisce delega al Governo per la semplificazione dei controlli sulle attività economiche prevedendo, tra i principi e criteri direttivi, anche l'accesso ai dati e lo scambio delle informazioni da parte dei soggetti che svolgono funzioni di controllo anche attraverso l'interoperabilità delle banche dati (lett. *g*) e, infine, il divieto per le p.a., nell'ambito dei controlli sulle attività economiche, di richiedere la produzione di documenti e informazioni già in loro possesso (lett. *l*). Rispetto a tale previsione, oltre a ribadire la necessità che il trattamento osservi, in fase esecutiva, la disciplina di protezione dei dati personali – osservazione recepita nel testo definitivo della legge – si è auspicata l'acquisizione del parere del Garante sullo schema di decreto legislativo.

Rispetto alla delega per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2019/1020, inoltre, l'art. 30, lett. *e*) della legge prevede il rafforzamento della digitalizzazione delle procedure di controllo, di vigilanza e di raccolta dei dati, anche al fine di favorire l'applicazione dei sistemi di intelligenza artificiale per il tracciamento di prodotti illeciti e per l'analisi dei rischi. Anche sul punto, si è richiamata l'esigenza, non accolta, di conformità alla disciplina di protezione dei dati personali, al fine di orientare più correttamente l'esercizio della delega.

La memoria si è inoltre soffermata sull'art. 32 del d.d.l. – soppresso, poi, nel corso dell'esame – che prevedeva l'istituzione di comitati tecnici per la selezione delle candidature a componenti i collegi delle autorità indipendenti di nomina parlamentare, tra le quali il Garante e, in particolare, di una commissione tecnica, con il compito di verificare la sussistenza, in capo ai candidati, dei requisiti normativamente previsti. Una specifica clausola di salvaguardia (all'ultimo periodo

del comma 1) ribadiva poi l'autonomia delle Camere – e dei rispettivi presidenti – ai fini della disciplina delle procedure di nomina di rispettiva competenza.

In estrema sintesi è stata al riguardo auspicata la riduzione del margine di discrezionalità della commissione anche per ridurre il rischio di contenzioso in ordine alle sue scelte, richiamando la giurisprudenza costituzionale secondo la quale gli spazi della discrezionalità politica trovano i loro confini nei principi di natura giuridica posti dall'ordinamento, tanto a livello costituzionale quanto a livello legislativo; e quando il legislatore predetermina canoni di legalità, ad essi la politica deve attenersi, in ossequio ai fondamentali principi dello stato di diritto. Si è quindi suggerito di individuare nell'autorità giurisdizionale l'organo legittimato alla risoluzione delle controversie in questione, attribuendole (almeno per la parte relativa all'esclusione dei candidati dalla rosa dei soggetti eleggibili proposta all'organo titolare del potere di nomina), alla giurisdizione esterna, non parendo sussistenti anche alla luce della sentenza n. 120/2014 della Corte costituzionale, i presupposti per ascriverle all'autodichia camerale. Si è infine sottolineato come la riforma proposta costituisse lo sviluppo di un processo, già in atto, di progressiva estensione delle garanzie di trasparenza delle procedure di nomina dei componenti le autorità, già innovato dal d.lgs. n. 101/2018 (nella parte in cui novella l'art. 153 del d.lgs. n. 196/2003).

Apprezzamento è stato espresso anche per la previsione del criterio della parità di genere quale vincolo per la scelta, tanto dei componenti la commissione tecnica, quanto dei soggetti eleggibili selezionati all'interno della rosa proposta all'organo politico.

Si è infine ricordato che la disciplina proposta, in via omogenea, per tutte le autorità non avrebbe dovuto attenuare le garanzie già previste singolarmente per ciascuna di esse, salvaguardando, dunque, a riforma avvenuta, la garanzia del voto limitato prevista dall'art. 153, comma 1, d.lgs. n. 196/2003, volta a coinvolgere anche le minoranze nella scelta di un organo, quale il vertice di un'autorità indipendente, che non può appunto, per sua espressa natura, rispondere neppure in fase di costituzione a logiche di tipo maggioritario.

2.2. *I decreti-legge*

Decreto cd. Milleproroghe

Il decreto-legge 30 dicembre 2021, n. 228, convertito, con modificazioni dalla legge 25 febbraio 2022, n. 15, prevede la proroga dell'efficacia di varie disposizioni, tra le quali quelle recanti interventi emergenziali che hanno caratterizzato la fase pandemica.

Tra le disposizioni di interesse, anche introdotte dalla legge di conversione, si segnalano, in particolare, le seguenti:

- l'articolo 3, comma 1, recante modifiche al d.lgs. n. 231/2007 in materia di riciclaggio. In particolare, la prima modifica riguarda le modalità di adempimento degli obblighi di adeguata verifica della clientela da parte degli intermediari e degli altri soggetti obbligati a svolgere tali adempimenti e identifica una nuova fattispecie al ricorrere della quale l'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente (nuovo numero 4-*ter* della lett. *a*), comma 1, art. 19, d.lgs. 21 novembre 2007, n. 231). In particolare, ci si riferisce ai clienti già identificati da un soggetto obbligato, i quali, previa identificazione elettronica basata su credenziali che assicurano i requisiti previsti dall'art. 4 del regolamento delegato (UE) 2018/389 della Commissione (procedura che comporta l'autenticazione forte del cliente), consentono al soggetto tenuto all'obbligo di identificazione di accedere alle informazioni relative agli estremi del conto di pagamento intestato al medesimo

cliente presso il citato soggetto obbligato in uno Stato membro dell'Unione europea. Tale modalità di identificazione e verifica dell'identità può essere utilizzata solo con riferimento a rapporti relativi a servizi di disposizione di ordini di pagamento e a servizi di informazione sui conti e il soggetto tenuto all'obbligo di identificazione deve in ogni caso acquisire il nome e il cognome del cliente. La seconda modifica rafforza la tutela del segnalante di operazioni sospette disciplinata dall'art. 38, d.lgs. n. 231/2007, per cui i soggetti obbligati ad effettuare le segnalazioni e gli organismi di autoregolamentazione adottano tutte le misure idonee ad assicurare la riservatezza dell'identità delle persone che effettuano la segnalazione. Il nuovo comma 3 dell'art. 38, integralmente sostituito per effetto delle modifiche in esame, specifica che in ogni fase del procedimento, l'Autorità giudiziaria è tenuta ad adottare le misure necessarie ad assicurare che siano mantenute riservate, oltre all'identità dei segnalanti già citata dalla norma in vigore, anche l'invio della segnalazione e delle informazioni trasmesse dalle FIU (*Financial Intelligence Unit*), nonché il contenuto delle medesime. In ogni caso, i dati identificativi dei segnalanti non possono essere inseriti nel fascicolo del pubblico ministero né in quello per il dibattimento, né possono essere in altro modo rivelati, salvo che ciò risulti indispensabile ai fini dell'accertamento dei reati per i quali si procede. In tale caso, l'Autorità giudiziaria provvede con decreto motivato, adottando le cautele necessarie ad assicurare la tutela del segnalante e, ove possibile, la riservatezza della segnalazione e delle informazioni trasmesse dalle FIU. Si sanziona, inoltre, con la reclusione da due a sei anni, l'indebita rivelazione dell'identità del segnalante ovvero notizie riguardanti l'invio della segnalazione e delle informazioni trasmesse dalle FIU o il contenuto delle medesime, se le notizie rivelate sono idonee a consentire l'identificazione del segnalante;

- l'articolo 3-*septies*, che proroga al 1° luglio 2022 l'entrata in vigore della disposizione che obbliga, pena sanzione amministrativa, associazioni di protezione ambientale, dei consumatori e degli utenti, onlus, fondazioni, cooperative sociali che svolgono attività a favore degli stranieri, a pubblicare nei propri siti internet o analoghi portali digitali, entro il 30 giugno di ogni anno, le informazioni relative a sovvenzioni, sussidi, vantaggi, contributi o aiuti, in denaro o in natura, non aventi carattere generale e privi di natura corrispettiva, retributiva o risarcitoria, agli stessi effettivamente erogati nell'esercizio finanziario precedente dalle pubbliche amministrazioni.

Decreto cd. aiuti

Il decreto-legge 17 maggio 2022, n. 50, convertito, con modificazioni dalla legge 15 luglio 2022 n. 91, reca, all'art. 38, disposizioni in materia di servizi di cittadinanza digitale, riconducibili al progetto "Poli" - Case dei servizi di cittadinanza digitale, di cui all'art. 1, comma 2, lett. *f*), n. 1, decreto-legge 6 maggio 2021, n. 59. L'articolo prevede che il Mise, in qualità di amministrazione titolare, possa stipulare convenzioni con gli enti locali (in particolare i comuni con meno di 15mila abitanti) per affidare a uno sportello unico la gestione dei servizi suscettibili di essere resi *online*, come il rilascio di certificati, l'effettuazione di pagamenti, iscrizioni a servizi pubblici ma anche la gestione delle informazioni sui servizi stessi.

La norma stabilisce, inoltre, che lo sportello unico sia gestito da Poste italiane, a tal fine autorizzato a procedere all'identificazione degli utenti interessati, all'acquisizione dei relativi dati, anche biometrici e della firma grafometrica, con l'osservanza delle disposizioni di legge o di regolamento in vigore. Sempre nei limiti delle singole convenzioni stipulate dai comuni il personale incaricato potrà accedere alle banche dati delle pubbliche amministrazioni eventualmente necessarie per svolgere le attività richieste, nel rispetto delle previsioni di cui all'art. 2-*ter*, comma 1-*bis*, del Codice.

Il decreto-legge 30 aprile 2022, n. 36, convertito, con modificazioni, dalla legge 29 giugno 2022 n. 79, prevede ulteriori misure urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (Pnrr).

Decreto di attuazione Pnrr

Tra le disposizioni di particolare interesse si segnala l'art. 18, che anticipa al 30 giugno 2022 (rispetto al 1° gennaio 2023) l'entrata in vigore delle sanzioni per mancata accettazione dei pagamenti elettronici e estende l'obbligo di fatturazione elettronica anche ai titolari di partita Iva in regime forfettario, finora esclusi. Il comma 4, infine, prevede che gli intermediari che mettono a disposizione degli esercenti sistemi di pagamento elettronico siano tenuti a trasmettere all'Agenzia delle entrate, oltre alle commissioni addebitate e ai dati identificativi degli strumenti di pagamento, anche gli importi complessivi delle transazioni giornaliere effettuate mediante tali strumenti, sia nel caso in cui il soggetto che effettua il pagamento sia un consumatore finale (come già previsto dalla norma vigente), sia nel caso in cui si tratti di un operatore economico. In tal modo l'Agenzia sarà in grado di incrociare i dati di pagamento digitale effettuati con carta con quelli relativi agli scontrini elettronici emessi dagli esercenti, così da effettuare controlli di congruità tra scontrini emessi e pagamenti ricevuti.

Si sono inoltre apportate alcune novelle all'art. 64 del Cad, imponendo ai gestori dell'identità digitale accreditati, prima del rilascio dell'identità digitale a una persona fisica, la verifica dei dati identificativi dei richiedenti, ivi inclusi l'indirizzo di residenza e, ove disponibili, il domicilio digitale o altro indirizzo di contatto, mediante consultazione gratuita dei dati disponibili presso l'Anagrafe nazionale della popolazione residente, anche tramite la Piattaforma digitale nazionale dati. Tali verifiche sono svolte, anche successivamente al rilascio dell'identità digitale, con cadenza almeno annuale.

Si estende, inoltre, l'applicazione della previsione di cui all'art. 64 all'identificazione elettronica funzionale all'accesso ai servizi erogati dalle pubbliche amministrazioni e dai soggetti privati tramite canali fisici, ammettendo il trattamento di "altri dati, fatti e informazioni funzionali alla fruizione di un servizio attestati da un gestore di attributi qualificati".

2.3. *I decreti legislativi*

Tra i numerosi decreti legislativi adottati nel 2022 e rilevanti, in varia misura, in materia di protezione dei dati personali, si segnalano, in particolare, i seguenti:

Il decreto legislativo 10 ottobre 2022, n. 150, attua la delega legislativa conferita dalla legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari.

Riforma del processo penale

Il decreto, su cui il Garante ha reso parere il 1° settembre 2022 (cfr. par. 3.1.2) prevede una riforma ampia e organica del processo penale, del sistema sanzionatorio, dell'ordinamento penitenziario e di alcune normative complementari, delineando una disciplina organica della giustizia riparativa.

Tra gli obiettivi trasversali perseguiti dal decreto legislativo vi è quello della digitalizzazione della giustizia penale e dello sviluppo del processo penale telematico. In questa prospettiva, le novelle apportate, in particolare al Libro secondo del codice di rito penale, introducono significative innovazioni in tema di formazione, deposito, notificazione e comunicazione degli atti e in materia di registrazioni audiovisive e partecipazione a distanza ad alcuni atti del procedimento o all'udienza.

Un'altra direttrice importante della riforma concerne la giustizia riparativa, la

cui disciplina assegna un ruolo centrale ai doveri di riservatezza del mediatore. La disciplina proposta affida lo svolgimento dei programmi di giustizia riparativa ad appositi Centri coordinati a livello statale dal Ministero della giustizia ma gestiti, a livello territoriale, dagli enti locali, configurandone l'attività come servizio di pubblico interesse. Di qui la legittimazione dei Centri per la giustizia riparativa (art. 42), in qualità di titolari del trattamento, a trattare i dati personali, anche appartenenti alle categorie di cui agli artt. 9 e 10 del RGPD, strettamente necessari all'esercizio delle competenze e al raggiungimento degli scopi sanciti dal decreto, nel rispetto del Regolamento (individuato quale plesso normativo applicabile non potendo i Centri ritenersi "autorità competenti" ai fini di cui al d.lgs. n. 51/2018). La normativa di attuazione sarà definita con regolamento, su cui sarà sentito il Garante (per espressa previsione del decreto).

Per altro verso, il decreto ha introdotto due particolari forme di tutela del diritto all'oblio (così normativamente definito) degli imputati e delle persone sottoposte ad indagini: l'annotazione, rispettivamente preventiva e successiva, di deindicizzazione del provvedimento giurisdizionale rilevante. L'annotazione preventiva rappresenta una cautela (ulteriore rispetto all'oscuramento, in particolare su istanza di parte, delle generalità di cui all'art. 52, comma 1, del Codice) volta a circoscrivere gli effetti della pubblicità del provvedimento giurisdizionale (che, anche se favorevole, può comunque risultare pregiudizievole per la parte), agendo in primo luogo sulla sua reperibilità a partire, anzitutto, dal sito istituzionale dell'autorità emanante.

L'annotazione successiva introduce, invece, un criterio di valutazione peculiare della meritevolezza dell'istanza di *delisting*, fondata sulla prevalenza, rispetto alla indiscriminata reperibilità del provvedimento, del diritto alla riservatezza, alla dignità e alla presunzione d'innocenza (ora peraltro tutelato anche in termini di redazione dei provvedimenti giurisdizionali e comunicazione giudiziaria dal d.lgs. n. 188/2021).

Il testo definitivamente approvato tiene conto delle osservazioni rese dal Garante nel parere 1° settembre 2022, n. 292 (doc. web n. 9802612) di cui il Senato ha chiesto il recepimento.

In particolare è stata accolta l'osservazione relativa:

a) all'integrazione dell'art. 87, comma 1, con la previsione dell'acquisizione del parere del Garante sullo schema di regolamento ministeriale recante la definizione delle regole tecniche riguardanti i depositi, le comunicazioni e le notificazioni telematiche degli atti del procedimento penale;

b) all'acquisizione del parere del Garante relativamente al decreto del Ministro della giustizia da adottarsi per regolare le modalità tecniche di pagamento, anche per via telematica;

c) alla ridefinizione, in relazione all'oblio, del contenuto dell'attestazione preventiva con riferimento all'obbligo di adozione – da parte dei siti che pubblicano il provvedimento – di misure idonee a sottrarlo all'indicizzazione da parte dei motori di ricerca generalisti.

Cybersicurezza

Il decreto legislativo 3 agosto 2022 n. 123, reca l'adeguamento della normativa nazionale alle disposizioni del Titolo III, "Quadro di certificazione della cybersicurezza", del regolamento (UE) 2019/881 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cybersicurezza).

Il decreto legislativo, in particolare, attua la delega prevista dall'art. 18 della legge di delegazione europea 2019-2020 (legge 22 aprile 2021, n. 53) volta all'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) n. 2019/881 del 17

aprile 2019, relativo all'Agenzia dell'Unione europea per la cybersicurezza (*European Union Agency for Network and Information Security* - ENISA) e al quadro europeo della certificazione.

All'interno di tale ambito di intervento, l'art. 1, comma 2 del decreto legislativo:

a) individua l'autorità nazionale di certificazione della cybersicurezza in Italia in base ai compiti ed ai poteri ad essa attribuiti in materia di vigilanza in ambito nazionale e di rilascio dei certificati di cybersicurezza, con riferimento al quadro europeo di certificazione;

b) disciplina le modalità di cooperazione dell'autorità nazionale di certificazione della cybersicurezza con le altre autorità pubbliche nazionali ed europee (competenti in materia di vigilanza del mercato) con l'Organismo di accreditamento nazionale designato in Italia;

c) definisce un sistema sanzionatorio applicabile in caso di violazione delle norme del quadro europeo di certificazione con sanzioni effettive, proporzionate e dissuasive.

Sono escluse dall'ambito di applicazione del decreto le disposizioni specifiche riguardanti le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale, coerentemente con quanto previsto dall'art. 1, par. 2, del RGPD che fa salve le competenze degli Stati membri in questi settori, anche in considerazione del carattere specifico della politica di sicurezza e di difesa di ciascuno Stato membro (cons. 43).

Particolare interesse assume poi l'articolo 2 nel quale viene espressamente previsto che il trattamento dei dati personali derivante dall'applicazione del decreto legislativo sia effettuato in accordo con il Regolamento europeo per la protezione dei dati personali e con il vigente Codice.

L'articolo 4 dello schema di decreto legislativo interviene in merito all'autorità nazionale di certificazione della cybersicurezza, disciplinando le modalità con cui sono definite l'organizzazione e le procedure per lo svolgimento dei compiti ad essa affidati.

Tale autorità è individuata nell'Agenzia per la cybersicurezza nazionale, come già previsto dagli artt. 7, comma 1, lett. *e*), e 16, comma 12, lett. *b*), d.l. n. 82/2021.

2.4. *Le norme regolamentari*

Tra i regolamenti di particolare rilievo per la protezione dei dati e sui quali, peraltro, è stato acquisito il parere del Garante (cfr. par. 3.1.3) si segnalano, segnatamente, i seguenti:

a) decreto del Presidente della Repubblica 27 gennaio 2022, n. 26 recante "Regolamento recante disposizioni in materia di istituzione e funzionamento del registro pubblico dei contraenti che si oppongono all'utilizzo dei propri dati personali e del proprio numero telefonico per vendite o promozioni commerciali, ai sensi dell'art. 1, comma 15, della legge 11 gennaio 2018, n. 5" (parere 13 gennaio 2022, n. 3, doc. web n. 9737240).

Tale regolamento, sostitutivo del previgente decreto del Presidente della Repubblica in materia di Registro pubblico delle opposizioni, assolve al duplice obiettivo di attuare la legge n. 5/2018 e le novelle a quest'ultima apportate dalla legge di conversione del decreto-legge n. 139/2021, in virtù di un emendamento parlamentare (9.70, Riccardi et al., AS 2409).

Proprio la novella legislativa ha consentito di superare lo stallo che aveva caratterizzato l'*iter* di adozione di tale regolamento, sul cui schema il Garante si

è espresso più volte negli ultimi anni, da ultimo nel giugno del 2021 ribadendo il proprio orientamento sull'estendibilità, alle chiamate automatizzate, dell'effetto revocatorio dei consensi precedenti, derivante dall'iscrizione nel Registro pubblico delle opposizioni. Il Garante infatti aveva osservato che la legge n. 5/2018 limitava espressamente lo strumento del registro alle chiamate con operatore, sicché per riferire anche alle chiamate automatizzate la revoca del consenso occorreva una norma di legge.

La fondatezza di tali argomentazioni ha indotto il Governo a promuovere una modifica legislativa.

La novella della legge n. 5/2018, contenuta in un emendamento parlamentare, accolto e introdotto nel decreto-legge n. 139/2021 ha infatti esteso la riferibilità del Registro alla revoca dei consensi prestati alla ricezione di chiamate automatizzate. Questo risultato è stato conseguito senza alterare – come richiesto dall'Autorità – il doppio regime (*opt-out* per le chiamate con operatore e *opt-in* per le chiamate automatizzate) previsto dal Codice, con vincoli unionali e realizzando una maggiore tutela per gli utenti (cfr. par. 3.1.3);

b) decreto 26 settembre 2022, n. 184 del Ministro della cultura, di concerto con il Ministro dell'economia e delle finanze, recante "Criteri e modalità di attribuzione e di utilizzo della Carta elettronica di cui all'art. 1, commi 357 e 358, della legge 30 dicembre 2021, n. 234" (parere 12 maggio 2022 n. 171, doc. web n. 9778334);

c) decreto del Presidente della Repubblica 4 ottobre 2022, n. 191, "Modifiche al decreto del Presidente della Repubblica 31 agosto 1999, n. 394, in attuazione dell'articolo 22 della legge 7 aprile 2017, n. 47, recante misure di protezione dei minori stranieri non accompagnati" (parere 7 luglio 2022, n. 241, doc. web n. 9799609).

3 I rapporti con il Parlamento e le altre Istituzioni

3.1. *L'attività consultiva del Garante*

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

La più frequente consultazione del Garante su atti normativi di rango primario e non, ha così contribuito, in linea generale, all'individuazione di un più corretto bilanciamento sotteso alle varie – e sempre più numerose – norme che prevedono trattamenti di dati personali.

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

Il coinvolgimento del Garante nell'ambito del procedimento legislativo o, comunque, dell'esercizio delle funzioni conoscitive, di indirizzo e controllo delle Camere è risultato, nel 2022, alquanto significativo.

Numerosi sono stati i casi di consultazione del Garante su atti normativi primari, spesso anche in sede di conversione di decreti-legge, soprattutto in relazione alle misure adottate per contrastare l'attuale situazione di crisi internazionale, economica ed energetica. Per tali forme di consultazione dell'Autorità è, infatti, sempre più frequente il ricorso allo strumento, particolarmente duttile, dell'audizione parlamentare, che offre anche la possibilità di un dialogo diretto, mediante il dibattito successivo alla relazione, tra i singoli parlamentari e il Garante. Le audizioni sono state talora richieste anche nell'ambito dell'esame, in fase ascendente, di atti normativi dell'Unione europea.

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

a) audizione dinanzi alla XII Commissione della Camera dei deputati nell'ambito dell'esame del disegno di legge di conversione del decreto-legge n. 1/2022, recante misure urgenti per fronteggiare l'emergenza Covid-19, in particolare nei luoghi di lavoro, nelle scuole e negli istituti della formazione superiore - 10 febbraio 2022 (doc. web n. 9744445);

b) memoria presentata alla 10ª Commissione del Senato nell'ambito dell'esame del disegno di legge annuale per il mercato e la concorrenza 2021 (AS 2469) - 16 febbraio 2022 (doc. web n. 9884498);

c) audizione dinanzi alla 14ª Commissione del Senato, nell'ambito dell'esame del disegno di legge recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea-legge di delegazione europea 2021 - 8 marzo 2022 (doc. web n. 9751458);

d) memoria presentata alle Commissioni riunite IX e X della Camera dei deputati sulla proposta di regolamento (UE) sull'intelligenza artificiale COM 2021(206) - 9 marzo 2022 (doc. web n. 9751565).

Non sono mancate richieste di contributi anche nell'ambito dell'esercizio delle funzioni conoscitive, di indirizzo e controllo delle Camere, che dimostrano una diffusa sensibilità rispetto alla protezione dei dati personali e alle sue istanze.

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

a) audizione dinanzi alla Commissione parlamentare d'inchiesta sulla tutela dei consumatori e degli utenti in materia di *telemarketing* - 16 febbraio 2022 (doc. web n. 9745988);

b) contributo alla Commissione parlamentare d'inchiesta sul femminicidio nonché su ogni forma di violenza di genere, istituita presso il Senato, sulle implicazioni in termini di protezione dati della violenza di genere - 6 aprile 2022;

c) audizione dinanzi alla Commissione straordinaria del Senato per il contrasto dei fenomeni di intolleranza, razzismo, antisemitismo, istigazione all'odio e alla violenza, sul fenomeno dei discorsi d'odio, nell'ambito dell'indagine conoscitiva sulla natura, cause e sviluppi recenti del fenomeno dei discorsi d'odio, con particolare attenzione alla evoluzione della normativa europea in materia - 15 febbraio 2022 (doc. web n. 9746273);

d) audizione dinanzi al Copasir sui profili di protezione dati della desecretazione degli atti - 12 maggio 2022;

e) audizione dinanzi alla Commissione parlamentare d'inchiesta sulla tutela dei consumatori e degli utenti, sulle tematiche inerenti alla profilazione *online* del consumatore - 17 maggio 2022 (doc. web n. 9771375).

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

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

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

a) parere 17 marzo 2022, n. 94 reso al Ministero del lavoro e delle politiche sociali su uno schema di disegno di legge recante disposizioni in materia di lavoro digitale (doc. web n. 9761615);

b) parere 26 maggio 2022, n.189, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2017/745, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/ 2009 e che abroga le direttive 90/385/ CEE e 93/42/CEE (doc. web n. 9782450);

c) parere 26 maggio 2022, n. 190, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2017/746, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione, nonché per l'adeguamento alle disposizioni del regolamento (UE) 2022/112 che modifica il regolamento (UE) 2017/746 (doc. web n. 9789069).

Tali provvedimenti, poi divenuti rispettivamente il decreto legislativo 5 agosto 2022, n. 137 e n. 138, sono stati adottati sulla base della delega contenuta nella legge di delegazione europea 2019-2020, volta all'adeguamento dell'ordinamento interno ad altrettanti regolamenti unionali (2017/745 e 746), rispettivamente in materia di dispositivi medici e dispositivi medici in vitro.

Essi disciplinano contenuti, tempistiche e modalità di registrazione delle informazioni che fabbricanti, distributori ed utilizzatori sono tenuti a comunicare

al Ministero della salute; il riordino del meccanismo di definizione dei tetti di spesa; il sistema sanzionatorio; l'individuazione di modalità di tracciabilità dei dispositivi medici attraverso il riordino e la connessione delle banche dati esistenti in conformità al Sistema unico di identificazione del dispositivo (sistema UDI); l'efficientamento dei procedimenti di acquisto tramite articolazione e rafforzamento delle funzioni di *Health Technology Assessment* (HTA), l'adeguamento delle attività dell'Osservatorio dei prezzi di acquisto dei dispositivi, nonché dei trattamenti di dati personali effettuati, in applicazione dei due regolamenti, alla disciplina di protezione dati dal momento che il regolamento 745 (come il 746) era stato adottato prima dell'entrata in vigore del nuovo quadro giuridico europeo. Essi presentano contenuto essenzialmente analogo nell'impianto complessivo, salvo per la revisione del d.lgs. 24 febbraio 1996 n. 47, emanato in attuazione della direttiva 93/42/CE, nonché del d.lgs. 14 dicembre 1992 n. 507, emanato in attuazione della direttiva 90/385/CEE, relativa ai dispositivi medici impiantabili attivi, da parte del primo decreto;

d) parere 7 luglio 2022, n. 241, reso al Ministero del lavoro e delle politiche sociali su uno schema di articolato volto a novellare il d.lgs. n. 231/2007 in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, volto all'istituzione di una banca dati centralizzata, presso gli organismi di autoregolamentazione (doc. web n. 9799609);

e) parere 1° settembre 2022, n. 292, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo di attuazione della legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari (doc. web n. 9802612).

Il testo, proponendo una riforma ampia e organica del processo penale, del sistema sanzionatorio, dell'ordinamento penitenziario e di alcune normative complementari, presentava diversi profili d'interesse in termini di protezione dati.

In particolare, l'Autorità ha fornito osservazioni sui temi della digitalizzazione della giustizia penale e dello sviluppo del processo penale telematico. Rilevanti anche le norme in materia di giustizia riparativa, la cui disciplina assegna un ruolo centrale ai doveri di riservatezza del mediatore e, infine, le disposizioni in materia di oblio per i soggetti destinatari di provvedimenti di archiviazione e proscioglimento, legittimati ad ottenere – conformemente a una formulazione non chiarissima del criterio di delega – un provvedimento di sottrazione preventiva all'indicizzazione dei dati (ed uno successivo di deindicizzazione dei contenuti) relativi al procedimento.

In tali ambiti il parere ha proposto puntuali osservazioni, segnatamente in ordine:

- all'acquisizione del parere del Garante sugli schemi di provvedimenti attuativi di alcune norme sul processo telematico, al fine di conformarne pienamente il contenuto alla disciplina di protezione dati;
- alle garanzie (anche in termini di sicurezza e affidabilità dei collegamenti telematici) da assicurare per la partecipazione a distanza alle udienze o alla formazione degli atti;
- agli accorgimenti da adottare per l'attuazione, in via telematica, delle notificazioni mediante pubblici annunzi (sottrazione all'indicizzazione e termine massimo di pubblicazione);
- alla corretta definizione del procedimento per la deindicizzazione preventiva dei provvedimenti giudiziari per i destinatari di provvedimenti di archiviazione e proscioglimento;

f) parere 10 novembre 2022, n. 364, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo recante attuazione della delega di cui all'art. 2 della legge 5 agosto 2022 n. 118, per la mappatura e la trasparenza dei regimi concessori di beni pubblici (doc. web n. 9826453).

3.1.3. I pareri sugli atti regolamentari

Nel quadro dell'attività consultiva concernente norme regolamentari suscettibili di incidere sulla protezione dei dati personali, il Garante ha reso numerosi pareri.

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

a) schema di regolamento recante disposizioni per il funzionamento del cd. Registro delle opposizioni, sostitutivo del d.P.R. n. 178/2010 (art. 1, comma 15, l. n. 5/2018 come modificato dal d.l. n. 139/2021, convertito con modificazioni, dalla l. n. 205/2021) (parere 13 gennaio 2022, n. 3, doc. web 9737240) (cfr. par. 2.3);

b) schema di decreto, di natura regolamentare, recante la disciplina dei criteri per l'acquisizione, anche mediante la predisposizione di un apposito sistema telematico, dei dati e delle informazioni rilevanti per individuare i beni ereditari vacanti nel territorio dello Stato (parere 27 gennaio 2022, n. 13, doc. web n. 9862624);

c) schema di decreto del Ministro dell'istruzione recante il regolamento sulle modalità di attuazione e funzionamento dell'Anagrafe nazionale dell'istruzione (Anist) prevista dall'art. 62-*quater* del Cad, istituita presso il Ministero dell'istruzione nell'ambito del proprio sistema informativo (parere 24 marzo 2022, n. 96, doc. web n. 9767057).

Tale provvedimento è stato oggetto di rivisitazioni, sulla base di alcune indicazioni fornite in fase istruttoria dal Garante, ma non del tutto recepite nel testo proposto.

L'Autorità ha pertanto ritenuto opportuno segnalare la necessità di alcune modifiche ed integrazioni, oltre che dell'effettuazione di una valutazione d'impatto.

I rilievi espressi hanno sottolineato l'esigenza di maggiore determinatezza in ordine ad alcuni aspetti del trattamento sotteso al funzionamento della banca dati, con riferimento, in particolare, agli scopi di Anist, ai tipi di dati trattati in relazione a ciascuna finalità perseguita e alle diverse categorie di interessati; ai soggetti legittimati all'accesso all'anagrafe in rapporto alle categorie dei dati accessibili; ai tempi di conservazione dei dati in funzione della loro tipologia e delle finalità perseguite; alla previsione di specifiche misure di sicurezza adeguate al rischio connesso al trattamento;

d) schema di regolamento concernente le modalità di funzionamento, accesso, consultazione del sistema di tracciabilità delle armi e delle munizioni, istituito ai sensi dell'art. 11, d.lgs. 10 agosto 2018, n. 104 (parere 7 aprile 2022, n. 133, doc. web n. 9773995);

e) schema di decreto, di natura regolamentare, del Ministro della cultura, di concerto con il Ministro dell'economia e delle finanze, recante criteri e modalità di attribuzione e di utilizzo della Carta elettronica di cui all'art.1, commi 357 e 358, della legge 30 dicembre 2021, n. 234 (cd. 18*app*) (parere 12 maggio 2022 n. 171, doc. web n. 9778334);

f) schema di decreto del Presidente della Repubblica recante regolamento recante modifiche al d.P.R. 31 agosto 1999, n. 394, in attuazione dell'articolo 22 della legge 7 aprile 2017, n. 47, recante misure di protezione dei minori stranieri non accompagnati (parere 7 luglio 2022, n. 240, doc. web n. 9799592);

g) schema di decreto, di natura regolamentare, del Ministro dello sviluppo economico, recante la definizione dei termini e delle modalità operative di alimentazione del fascicolo informatico d'impresa (parere 21 luglio 2022, n. 251, doc. web n. 9806101);

h) schema di decreto, di natura regolamentare, del Ministero della transizione ecologica sulla disciplina del sistema di tracciabilità dei rifiuti e del registro elettronico nazionale per la tracciabilità dei rifiuti (Rentri) (parere 22 agosto 2022, n. 287, doc. web n. 9809087);

i) schema di decreto, di natura regolamentare, del Ministro delle infrastrutture e della mobilità sostenibili recante la disciplina delle modalità di esercizio dell'attività di scuola nautica (parere 10 novembre 2022, n. 363, doc. web n. 9831428);

j) schema di decreto, di natura regolamentare, del Ministro delle infrastrutture e della mobilità sostenibili, recante le modalità di esercizio delle funzioni di coordinamento spettanti al Comando generale del Corpo delle Capitanerie di porto - Guardia costiera per l'applicazione del regolamento (UE) 2019/1239 (parere 24 novembre 2022, n. 383, doc. web n. 9837004).

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

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

Si segnalano, in tal senso, i seguenti:

1) parere sullo schema di regolamento di esecuzione dell'art. 16 della legge della Provincia autonoma di Trento 30 ottobre 2019, n. 10 (legge provinciale sull'agriturismo 2019) e sullo schema di regolamento di esecuzione dell'art. 23-*bis* della legge provinciale 19 dicembre 2001, n. 10 (legge provinciale sull'agricoltura sociale e sulle strade tematiche 2001) concernente l'esercizio dell'attività di enoturismo (parere 10 febbraio 2022, n. 39, doc. web n. 9750283);

2) parere sullo schema di regolamento concernente il funzionamento del registro di artroprotesi della Provincia autonoma di Trento, in attuazione dell'art. 14, comma 5-*bis* della legge provinciale 23 luglio 2010 n. 16 (legge provinciale sulla tutela della salute) (parere 10 febbraio 2022, n. 38, doc. web 9750238);

3) parere su un emendamento alla proposta di legge della Regione Umbria recante l'istituzione della giornata regionale per la lotta alla droga su base volontaria per assessori e consiglieri regionali e comunali (parere 28 aprile 2022, n. 169, doc. web n. 9775868);

4) parere sulla proposta di modifica dell'art. 27, comma 2-*bis* della legge della Provincia autonoma di Trento 24 ottobre 2006, n. 7 (Disciplina dell'attività di cava) (parere 12 maggio 2022, n. 172, doc. web n. 9780857);

5) parere sulla proposta di legge della Provincia autonoma di Trento concernente il sistema provinciale per la politica attiva del lavoro e la realizzazione di interventi e servizi di pubblica utilità (cd. progettone) (parere 26 maggio 2022, n. 191, doc. web n. 9781139);

6) parere sul disegno di legge, della Regione Veneto, di disciplina del progetto "MoVe In", finalizzato al monitoraggio delle percorrenze reali effettuate dai veicoli soggetti alle limitazioni della circolazione mediante l'installazione di dispositivi telematici (parere 15 dicembre 2022, 413, doc. web n. 9843659).

3.1.5. Provvedimenti decisori di segnalazioni

Nel 2022, inoltre, con un provvedimento decisorio, adottato ai sensi dell'art. 144 del Codice e approvato dal Collegio il 7 aprile 2022, n. 170 (doc. web n. 9773687), l'Autorità ha fornito riscontro alle molteplici segnalazioni pervenute tese a denunciare, in senso generale, l'asserita illiceità del trattamento dei dati funzionale al sistema delle certificazioni verdi (tanto nella versione base, quanto in quella rafforzata).

Il provvedimento ha, in particolare, chiarito il perimetro di valutazione possibile per l'Autorità, circoscritto alla legittimità del trattamento e in tale ambito si sono valutate le eccezioni di merito addotte, ravvisandone l'infondatezza, con conseguente archiviazione del procedimento.

3.2. *Consultazione attraverso la piattaforma IMI*

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

Sono state, in particolare, seguite quattro procedure IMI di assistenza reciproca ex art. 61 del RGPD, fornendo i riscontri richiesti su temi di rilievo dal punto di vista legislativo e istituzionale, riguardanti: il quadro sanzionatorio italiano in materia di protezione dati; l'indipendenza esterna del Garante; l'applicazione delle disposizioni del RGPD al trattamento dei dati personali da parte delle Camere; la designazione dell'Autorità di controllo ai fini del *Data Governance Act* (DGA) - regolamento (UE) 2022/868 del 30 maggio 2022.

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

Anche nel 2022 il Garante ha fornito a richiesta del Governo elementi informativi ai fini della redazione della risposta da rendere ad atti di sindacato ispettivo rilevanti in termini di protezione dei dati personali.

Con particolare riferimento all'interrogazione n. 3-01992 dell'On. Stefania Ascari l'Autorità, con nota 20 giugno 2022, ha fornito elementi relativamente al sistema interministeriale di raccolta dati relativi ai reati previsto dall'art. 5, comma 4 della legge 5 maggio 2022, n. 53, recante disposizioni in materia di statistiche in tema di violenza di genere, richiamando le osservazioni svolte in audizione presso la Commissione parlamentare inquirente sul femminicidio.

L'Autorità ha inteso, in particolare, ribadire l'importanza di garantire una circolazione delle informazioni nella misura effettivamente necessaria, per finalità predeterminate e legittime, sulla base di disposizioni normative idonee e nel rispetto dei principi di cui agli artt. 5 del RGPD e 3 del d.lgs. n. 51/2018.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

L'attività svolta dal Garante

RELAZIONE ANNUALE
2022

II - L'attività svolta dal Garante

4 Il Garante e le amministrazioni pubbliche

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

4.1.1. La dichiarazione dei redditi precompilata

Come negli anni precedenti, anche nel 2022 il Garante è stato chiamato a pronunciarsi in merito alla cd. dichiarazione dei redditi precompilata, sia sulle modalità di accesso alla dichiarazione da parte degli interessati e dei soggetti autorizzati che sulle tipologie di dati destinate a confluirvi.

Modalità di accesso

Con riferimento al primo aspetto, è stato sottoposto all'Autorità lo schema di provvedimento del Direttore dell'Agenzia delle entrate, che, in sintesi, ha introdotto l'ipotesi di accesso alla dichiarazione 730 precompilata in presenza di una procura speciale o generale nonché stabilendo i presupposti e le modalità di conferimento e revoca della procura speciale da parte del contribuente ai sensi dell'art. 63, d.P.R. 29 settembre 1973, n. 600. In particolare, tale ipotesi è stata limitata alle persone fisiche, distinguendo tra le procure con firma autenticata e quelle conferite al coniuge o a parenti e affini entro il quarto grado che non richiedono tale autenticazione. Inoltre, recependo indicazioni fornite dall'Ufficio, è stato previsto che nel caso in cui il rappresentato sia impossibilitato a operare a causa di patologie, il rappresentante possa presentare presso un qualsiasi ufficio territoriale, idonea attestazione sanitaria rilasciata dal medico di medicina generale del rappresentato, sulla base del modello disponibile sul sito internet dell'Agenzia. Nell'esprimere parere favorevole, il Garante ha ingiunto all'Agenzia delle entrate di proseguire le attività di controllo sulla legittimità degli accessi alla dichiarazione precompilata effettuati dai Caf anche nel 2022 su un campione significativo, verificando, nei casi anomali, l'effettiva sussistenza dei presupposti dell'accesso alla dichiarazione precompilata e controllando, in particolare, la legittimità degli accessi in presenza di procure speciali (provv. 12 maggio 2022, n. 173, doc. web n. 9778313).

Spese effettuate presso gli esercenti l'arte ausiliaria di ottico

Per quanto riguarda la raccolta dei dati, sullo schema di decreto del Mef che prevede, nell'ambito della trasmissione al Sistema tessera sanitaria (Sistema TS) dei dati relativi alle spese sanitarie a fini di elaborazione della precompilata, nuove modalità di verifica degli esercenti l'arte ausiliaria di ottico, il Garante si è espresso favorevolmente a condizione che, in relazione agli elenchi di tali esercenti acquisiti dal Ministero della salute fino al 30 settembre 2022 e mantenuti nel Sistema TS, siano indicati i tempi di conservazione dei dati personali, nel rispetto del principio di limitazione della conservazione (provv. 20 ottobre 2022, n. 333, doc. web n. 9825728).

Parere favorevole è stato pronunciato anche sullo schema di decreto del Mef - Ragioniere generale dello Stato che adegua le specifiche tecniche e le modalità operative

relative all'acquisizione dei dati relativi agli esercenti l'arte ausiliaria di ottico, il quale mantiene inalterate le garanzie a tutela degli interessati, già precedentemente vagliate dall'Autorità (provv. 20 ottobre 2022, n. 334, doc. web n. 9825795).

Conseguentemente, è stato dato parere favorevole sullo schema di provvedimento del Direttore dell'Agenzia delle entrate che disciplina le modalità tecniche di utilizzo, ai fini della elaborazione della dichiarazione dei redditi precompilata, dei dati delle spese sanitarie comunicate, a decorrere dall'anno d'imposta 2022, anche con riferimento a quelle effettuate presso gli esercenti l'arte ausiliaria di ottico (provv. 10 novembre 2022, n. 401, doc. web n. 9843685).

Trasmissione al Sistema TS dei dati sui *bonus*

Il Garante è stato chiamato poi a esprimersi sullo schema di decreto del Mef - Ragioniere generale dello Stato che, con riferimento ai flussi al Sistema TS dei dati concernenti le spese sanitarie, a fini di elaborazione della dichiarazione dei redditi precompilata, tiene conto dell'introduzione dei contributi di cui all'art.1-*quater*, d.l. 30 dicembre 2021, n. 228 (il cd. *bonus* psicologo) e all'art. 1, commi 437-439, l. 30 dicembre 2020, n. 178 (il cd. *bonus* vista). È stato reso parere favorevole in quanto sono state individuate misure volte a limitare le tipologie di dati oggetto di trasmissione, nel rispetto dei principi di minimizzazione dei dati e *privacy by design* e *by default*, evidenziando che le informazioni raccolte nell'ambito del Sistema TS non possono essere oggetto di trattamenti diversi da quelli previsti dall'ordinamento (provv. 21 dicembre 2022, n. 443, doc. web n. 9843393).

4.1.2. Lotta all'evasione fiscale e tecniche di intelligenza artificiale

Anche nel 2022 il Garante si è occupato dei trattamenti effettuati dall'Agenzia delle entrate tramite l'utilizzo dei dati presenti nell'archivio dei rapporti finanziari e l'incrocio degli stessi con le altre banche dati di cui dispone, anche previa pseudonimizzazione dei dati personali, avvalendosi delle tecnologie, delle elaborazioni e delle interconnessioni tra essi, allo scopo di individuare criteri di rischio utili per far emergere posizioni da sottoporre a controllo e incentivare l'adempimento spontaneo. L'Agenzia è stata autorizzata ad avviare tali trattamenti, sulla base di quanto rappresentato nella valutazione di impatto sulla protezione dei dati sottoposta all'esame dell'Autorità, che ha ingiunto l'adozione di alcune misure di garanzia necessarie ad assicurare il rispetto dei diritti e delle libertà degli interessati (provv. 30 luglio 2022, n. 276, doc. web n. 9808839).

Con decreto Mef adottato il 28 giugno 2022, attuativo della legge n. 160/2019, anche sulla base delle condizioni formulate al riguardo dal Garante nel parere 22 dicembre 2021, n. 453 (doc. web n. 9738520) – oltre alle specifiche limitazioni all'esercizio dei diritti degli interessati in relazione a tali trattamenti – sono state inoltre stabilite le misure adeguate a tutela dei diritti e delle libertà degli interessati che l'Agenzia è tenuta ad adottare in questo contesto, individuandole nell'ambito di una valutazione di impatto da sottoporre alla consultazione preventiva del Garante.

Nella valutazione di impatto trasmessa dall'Agenzia è stata rappresentata l'intenzione di applicare le metodologie di analisi più appropriate per individuare i criteri di rischio utilizzando, oltre ai classici metodi deterministici, anche metodi basati sulle moderne tecniche di *machine learning*, supervisionate e non, e sulle altre soluzioni di intelligenza artificiale. In particolare, sono state elencate le banche dati che (allo stato) l'Agenzia intende impiegare per la creazione dei *dataset* di analisi e sono stati descritti in astratto i possibili modelli di analisi.

Preliminarmente sono stati rilevati gli elevati rischi che tali trattamenti comportano per i diritti e le libertà degli interessati, essendo relativi a tutte le tipologie di dati personali che costituiscono l'immenso patrimonio informativo nella disponibilità dell'Agenzia delle entrate, fondati sul ricorso a nuove tecnologie.

Su tale base, è stata richiesta l'adozione di adeguate misure e garanzie a tutela degli interessati richiamando anche la recente giurisprudenza del Consiglio di Stato (cfr., in particolare, le sent., VI sez., nn. 2270/2019, 8472/2019, 8473/2019, 8474/2019, 881/2020, e 1206/2021) e il quadro regolatorio in via di formazione nel contesto dell'Unione europea, come pure i principi oggetto di elaborazione in seno al Consiglio d'Europa improntati al *design*, sviluppo e applicazione di sistemi di intelligenza artificiale affidabile (*trustworthy* AI).

Il Garante ha evidenziato innanzitutto che, in ossequio a quanto previsto dagli artt. 5, 25 e 35 del RGPD, le misure da adottare per gestire i rischi presentati dal trattamento devono essere valutate in concreto, vale a dire tenendo in considerazione le caratteristiche delle banche dati di volta in volta utilizzate e i modelli di analisi impiegati. Ciò, tenuto conto che tra i principali rischi connessi all'utilizzo di modelli di analisi stocastica con tecniche di *machine learning*, vi sono quelli relativi a potenziali opacità nella fase di sviluppo dell'algoritmo, errori e distorsioni di diversa natura (cd. *bias*).

Specifica attenzione deve essere dedicata, inoltre, alla trasparenza e alla correttezza nei processi decisionali fondati su trattamenti automatizzati.

In tale prospettiva, è stato rilevato che nell'aggiornamento della valutazione di impatto in esame dovranno essere tenute in considerazione le opinioni degli interessati ed è stata ritenuta necessaria anche la pubblicazione, quantomeno di un estratto, della valutazione di impatto, per contribuire ad assicurare un elevato livello di trasparenza di tutti i contribuenti, incrementando così la loro fiducia nei confronti dell'utilizzo di tecniche di intelligenza artificiale.

Il Garante ha chiesto, inoltre, di potenziare l'intervento umano nella formazione dei *dataset* di analisi e di controllo, richiedendo misure adeguate a formare il personale coinvolto al fine di assicurare la comprensione delle capacità e dei limiti del processo algoritmico e favorirne la corretta interpretazione. Occorre poi garantire la possibilità per gli operatori di decidere, in qualsiasi situazione particolare, di ignorare, se del caso, l'*output* del processo algoritmico, evitando la possibile tendenza a farvi automaticamente affidamento.

È stato, altresì, richiesto di effettuare specifiche verifiche sulla qualità dei modelli di analisi impiegati, poiché le attività di monitoraggio costituiscono un presidio necessario per assicurare il rispetto dei principi del Regolamento in ogni fase dei trattamenti, anche con riferimento alla presenza di *bias* o di discriminazioni.

A tal fine l'Agenzia dovrà documentare adeguatamente, in rapporti periodici, le metriche utilizzate, le attività svolte, le eventuali criticità riscontrate e le misure di conseguenza adottate coinvolgendo anche il Rpd ed aggiornando, se necessario, la valutazione di impatto.

Infine, si è chiesto all'Agenzia di adottare efficaci tecniche di pseudonimizzazione dei dati nell'ambito dei trattamenti in esame, volte a ridurre in modo adeguato i rischi di re-identificazione degli interessati anche nei *dataset* di analisi, il rispetto dei principi di minimizzazione dei dati, di integrità e riservatezza.

4.1.3. Antiriciclaggio

Trattamento dei dati sulla titolarità effettiva

Nell'ambito dell'attuazione della normativa antiriciclaggio, InfoCamere scpa ha sottoposto all'Autorità lo schema di disciplinare tecnico sulla sicurezza del trattamento dei dati sulla titolarità effettiva, predisposto ai sensi dell'art. 11, comma 3, del regolamento 11 marzo 2022, n. 55, concernente la comunicazione, l'accesso e la consultazione dei dati e delle informazioni relativi alla titolarità effettiva, tra l'altro, di imprese dotate di personalità giuridica, di persone giuridiche private, di *trust* produttivi di effetti giuridici.

Il Garante ha espresso parere favorevole, anche in ragione della considerazione prestata alle osservazioni fornite nel corso di interlocuzioni informali al fine di rendere conformi i trattamenti ai principi di integrità, riservatezza e di *privacy by design* e *by default* nonché agli obblighi di sicurezza, riservandosi, tuttavia, di valutare le misure tecniche e organizzative che saranno individuate con i decreti attuativi che il Mise è tenuto ad adottare. Particolare attenzione è stata prestata al profilo della consultazione dei contenuti informativi, soprattutto in caso di esclusione dell'accesso alle informazioni concernenti la titolarità effettiva legata a ipotesi delicate e particolari. Ciò anche alla luce della questione pregiudiziale all'epoca pendente dinanzi alla CGUE concernente, nel contesto della disciplina sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo, proprio l'accesso a tali informazioni (cause riunite C-37/20 e C-601/20, instaurate contro i registri delle imprese del Lussemburgo, su cui successivamente la Corte si è pronunciata con sentenza 22 novembre 2022, dichiarando l'invalidità della norma della direttiva europea che demandava agli Stati membri di provvedere affinché le informazioni sulla titolarità effettiva delle società e delle altre entità giuridiche costituite nel loro territorio fossero accessibili in ogni caso al pubblico) (provv. 6 ottobre 2022, n. 316, doc. web n. 9817361).

Operatori di valuta virtuale

Sempre in materia di antiriciclaggio sono stati sottoposti al vaglio dell'Autorità, da parte dell'Organismo agenti e mediatori (Oam), due schemi di specifiche tecniche, relative, rispettivamente, alla procedura di registrazione degli operatori in valute virtuali alla sezione speciale del registro dei cambiavalute e alla procedura di trasmissione all'Oam per via telematica dei dati relativi alle operazioni effettuate sul territorio della Repubblica italiana dagli operatori in valute virtuali iscritti a tale sezione speciale, ai sensi degli artt. 3, comma 4; 5, comma 2, e 7, comma 2, decreto Mef 13 gennaio 2022 (su cui il Garante già si era espresso con provv. 28 ottobre 2021, n. 380, doc. web n. 9721489), attuativo dell'art. 17-*bis*, d.lgs. 13 agosto 2010, n. 141. Il Garante ha pronunciato parere favorevole, formulando alcune condizioni e osservazioni volte ad assicurare il rispetto dei principi di trasparenza, integrità e riservatezza attraverso l'adozione di adeguate misure tecniche e organizzative (provv. 21 dicembre 2022, n. 449, doc. web n. 9856315).

Registro dei soggetti convenzionati ed agenti prestatori di servizi di pagamento

L'Autorità ha inoltre reso parere favorevole sullo schema di decreto del Ministro dell'economia e delle finanze recante norme in materia di registro dei soggetti convenzionati ed agenti prestatori di servizi di pagamento e gli istituti emittenti moneta elettronica in attuazione dell'art. 45, comma 3, d.lgs. 21 novembre 2007, n. 231, nell'ambito del quale sono state disciplinate le modalità tecniche di alimentazione e consultazione del predetto registro e della relativa sottosezione ad accesso riservato, individuando la titolarità del trattamento dei dati in capo all'Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi (provv. 24 febbraio 2022, n. 77, doc. web n. 9751958). La disciplina dei trattamenti è infatti risultata analoga a quanto previsto nei decreti ministeriali attuativi della normativa in materia di antiriciclaggio sui quali il Garante si era già espresso favorevolmente nel corso degli anni (provv.ti 25 settembre 2014, n. 425, doc. web n. 3487879 e 12 aprile 2018, n. 211, doc. web n. 8576294).

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

4.2.1. Erogazione di benefici

Nel corso del 2022, il Garante si è espresso in diverse occasioni in relazione a trattamenti di dati personali necessari per l'erogazione di benefici economici, o comunque di agevolazioni di varia natura.

Contributo a fondo perduto al sistema del vuoto a rendere

È stato espresso parere favorevole sullo schema di decreto del Ministero della transizione ecologica che disciplina l'erogazione di benefici in favore di imprese, volti a promuovere il sistema del vuoto a rendere per gli imballaggi contenenti liquidi a fini alimentari. Il testo ha tenuto conto delle indicazioni fornite nel corso di interlocuzioni informali, tra cui il rispetto del principio di minimizzazione dei dati nei flussi di informazioni verso Guardia di finanza e Agenzia delle entrate nonché nell'assolvimento degli obblighi di pubblicità e trasparenza mediante il registro nazionale degli aiuti di Stato, con misure tecniche e organizzative e modalità di attuazione analoghe a quelle previste dal decreto relativo all'erogazione del cd. *bonus* idrico (cfr. provv.ti 16 settembre 2021, n. 333, doc. web n. 9713770 e 13 gennaio 2022, n. 4, doc. web n. 9740759).

***Bonus* psicologo**

Il Garante ha rilasciato parere positivo sullo schema di decreto del Ministro della salute concernente un contributo per sostenere le spese relative a sessioni di psicoterapia, ai sensi dell'art. 1-*quater*, d.l. 30 dicembre 2021, n. 228. Il Ministero aveva recepito le indicazioni fornite dall'Autorità nel corso di colloqui informali, volte a delimitare i dati personali oggetto dei trattamenti (in particolare le informazioni da fornire in sede di presentazione della domanda di accesso al beneficio, nonché i flussi di dati personali, con particolare riguardo a quelli dei professionisti che accettano il contributo a fronte dell'erogazione della prestazione) e definire puntualmente i ruoli e i compiti di tutti i soggetti coinvolti nel trattamento, oltre che ad attribuire al Ministero della salute, con il coinvolgimento delle regioni e delle province autonome e dell'Inps, il compito di effettuare la valutazione d'impatto sulla protezione dei dati, prima dell'avvio del trattamento, ai sensi dell'art. 35, par. 10, del RGPD (provv. 19 maggio 2022, n. 188, doc. web n. 9774696).

***Bonus* vista**

Il Ministero della salute ha, inoltre, sottoposto all'Autorità lo schema di decreto ministeriale che disciplina l'erogazione, ai sensi dell'art. 1, commi 437-439, l. 30 dicembre 2020, n. 178, in favore dei membri di nuclei familiari, di benefici per l'acquisto di occhiali da vista o di lenti a contatto correttive. Le misure tengono anche conto delle indicazioni fornite dall'Autorità nel corso di interlocuzioni informali tra l'altro circa: la puntuale individuazione dei dati personali trattati in relazione alle varie fasi in cui si articola il trattamento e ai flussi informativi instaurati, anche nel momento della verifica dei requisiti, nonché l'esclusione del trattamento dei dati relativi alla salute; le garanzie di trasparenza per consentire ai richiedenti di essere informati correttamente al momento della presentazione della domanda; la possibilità per gli interessati di effettuare l'autenticazione informatica anche mediante Cns nonché l'individuazione dei tempi di conservazione. Il Garante ha espresso parere favorevole, a condizione che fosse demandata a un provvedimento del Direttore dell'Agenzia delle entrate, sentita l'Autorità, la definizione delle modalità e dei termini della comunicazione all'Agenzia delle entrate dei dati relativi ai rimborsi erogati, ai fini di elaborazione della dichiarazione dei redditi precompilata (provv. 6 ottobre 2022, n. 319, doc. web n. 9817038).

***Bonus* patente autotrasporto**

Il Ministero delle infrastrutture e della mobilità sostenibili ha sottoposto all'Autorità lo schema di decreto, da adottarsi di concerto con il Ministro dell'economia e delle finanze, relativo al riconoscimento del contributo previsto dall'art. 1, commi 5-*bis* e 5-*ter*, d.l. 10 settembre 2021, n. 121, convertito, con modificazioni, dalla l. 9 novembre 2021, n. 156 (cd. buono patente autotrasporto). Lo schema di decreto ha disciplinato il trattamento sulla base delle misure già individuate nei decreti relativi al riconoscimento dei cd. buono veicoli sicuri e buono dispositivi antiabbandono (sui quali il Garante si era già espresso favorevolmente con i provv.ti 22 luglio 2021, n. 274, doc. web n. 9689706 e 15 gennaio 2020, n. 2, doc. web n. 9264222) prevedendo il riutilizzo della medesima piattaforma web. In particolare, a valle delle

indicazioni fornite dagli Uffici, è stato precisato il ruolo assunto dal Ministero e da Sogei spa nell'ambito delle operazioni di trattamento necessarie alla cancellazione dei soggetti accreditati, in caso di usi difformi del beneficio (provv. 26 maggio 2022, n. 194, doc. web n. 9784610).

Il Ministero della cultura ha sottoposto all'Autorità lo schema di decreto, da adottarsi di concerto con il Mef, modificativo del decreto interministeriale 10 febbraio 2021, n. 73, recante disposizioni attuative per la Carta della cultura prevista dall'art. 6, l. 13 febbraio 2020, n. 15, ossia una carta elettronica di importo nominale pari a euro 100, utilizzabile dal titolare per l'acquisto di libri, prodotti e servizi culturali, attribuibile a residenti nel territorio nazionale ed appartenenti a nuclei familiari economicamente svantaggiati. L'Autorità ha reso parere favorevole, considerato che lo schema esaminato ha tenuto conto di alcune indicazioni fornite dall'Ufficio, volte ad assicurare la conformità del trattamento alla normativa in materia di protezione dei dati personali attraverso, in particolare, una corretta definizione dei ruoli assunti dai soggetti coinvolti nell'ambito dell'erogazione del beneficio, l'esatta individuazione delle categorie di dati trattati (riferibili anche all'indicatore Isee) e delle informazioni da rendere agli interessati, nonché un'adeguata valutazione dei rischi per gli interessati (provv. 21 dicembre 2022, n. 444, doc. web n. 9847326).

4.2.2. Dati dei beneficiari di fondi a valere sul Fondo sociale europeo

Nel 2021 l'Autorità aveva chiesto al Garante europeo per la protezione dei dati valutazioni sulla conformità alla normativa europea di settore delle richieste, rivolte dalla Commissione europea all'Inps e al Ministero del lavoro e delle politiche sociali, volte ad acquisire preventivamente, per lo svolgimento degli *audit* previsti dalla disciplina di settore (spec. reg. (UE) 1303/2013), tutti i dati in chiaro sottostanti le spese certificate e relative ai beneficiari di sussidi a valere sul Fondo sociale europeo. Nel corso dell'istruttoria il Garante europeo ha chiamato in causa direttamente la Commissione europea, la quale ha precisato che nell'ambito degli *audit* è necessario trattare i soli dati pertinenti alla base di tutti i pagamenti, ossia quelli che consentirebbero all'autorità preposta di effettuare controlli di plausibilità e di valutare adeguatamente le aree di rischio dell'operazione, che, in una prima fase, possono essere anche non identificativi degli interessati. Il *set* di dati da utilizzare deve, infatti, essere definito in stretta relazione con le finalità di *audit*, tenendo in debita considerazione i principi di adeguatezza e pertinenza dei dati e limitato a quanto necessario per effettuare controlli efficaci e proporzionati sulla spesa certificata.

L'Autorità ha preso atto delle garanzie così individuate, sottolineando l'importanza che i trattamenti di dati personali in parola siano costantemente effettuati nel pieno rispetto dei principi in materia di protezione dei dati personali, sotto il controllo delle autorità di controllo nazionali, ma, soprattutto, del Garante europeo, quale autorità chiamata a vigilare sul rispetto della relativa disciplina da parte di istituzioni e organi dell'Unione europea (nota 31 maggio 2022).

4.2.3. Isee precompilato

In tema di Isee precompilato, di cui all'art. 10, comma 2, d.lgs. 15 settembre 2017, n. 147, il Garante ha espresso parere favorevole sullo schema di decreto del Ministero del lavoro e delle politiche sociali modificativo del decreto 9 agosto 2019 recante individuazione delle modalità tecniche per consentire al cittadino di accedere alla dichiarazione Isee precompilata resa disponibile in via telematica dall'Inps. Tali modifiche si sono rese necessarie per introdurre un meccanismo semplificato per consentire a ciascun componente maggiorenne del nucleo familiare del dichiarante di

autorizzare, attraverso un accesso mediante Spid, Cie o Cns al sistema informativo dell'Isee, la precompilazione di tutti i dati che lo riguardano, anche patrimoniali, in possesso dell'Agenzia delle entrate (provv. 28 aprile 2022, n. 144, doc. web n. 9775708).

Conseguentemente, è stato esaminato dal Garante lo schema di provvedimento congiunto del Direttore generale dell'Inps e del Direttore dell'Agenzia delle entrate, modificativo del precedente provvedimento 20 dicembre 2019, che vi dà attuazione. Il Garante ha espresso parere favorevole, anche in considerazione del fatto che l'Inps, rispetto al sistema introdotto nel 2019 relativo alle modalità di accesso alla Dsu precompilata, ha tra l'altro rappresentato l'assenza di anomalie tali da giustificare una revisione degli scenari di rischio legati all'impiego della Dsu precompilata, evidenziando che, nell'arco del biennio precedente, non sono state rilevate segnalazioni di criticità (provv. 26 maggio 2022, n. 192, doc. web n. 9776692).

4.2.4. Reddito e pensione di cittadinanza

In tema di reddito e pensione di cittadinanza, il Garante ha fornito parere favorevole sullo schema di modulo per la domanda del beneficio, che modifica quello adottato dall'Inps nel 2019 ai sensi dell'art. 5, comma 1, d.l. 28 gennaio 2019, n. 4, anche al fine di dare seguito ad alcune novità introdotte dalla normativa di settore, con specifico riferimento alle modalità di funzionamento del reddito di cittadinanza, ai requisiti che deve possedere il richiedente, alla scala di equivalenza e all'assegno unico previsto dall'art. 7, comma 2, d.lgs. 21 dicembre 2021, n. 230 (provv. 28 aprile 2022, n. 145, doc. web n. 9775818).

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

Anche nel 2022 sono state forniti al Ministero dell'istruzione, alle università e alle istituzioni scolastiche chiarimenti e indicazioni sulla corretta applicazione della disciplina in materia di protezione dei dati personali.

Io studio - Carta dello studente

Con provvedimento 12 maggio 2022, n. 185 (doc. web n. 9782000), sono stati autorizzati i trattamenti dei dati descritti nella valutazione d'impatto sulla protezione dei dati (artt. 36, par. 5 e 58, par. 3, lett. *c*), del RGPD) relativa all'iniziativa Io Studio - Carta dello studente trasmessa dal Ministero dell'istruzione, ai sensi dell'art. 11, d.m. del Ministero dell'istruzione 30 settembre 2021. La valutazione di impatto, che individua il Ministero dell'istruzione quale titolare del trattamento e le società che curano la spedizione della carta agli istituti scolastici e che gestiscono l'applicazione web del portale dello studente quali responsabili, ha tenuto conto delle indicazioni fornite dal Garante ai competenti uffici del Ministero nel corso di interlocuzioni informali con particolare riferimento: all'indicazione dei dati personali degli studenti che il Ministero acquisisce dall'Anagrafe nazionale dello studente in relazione alle singole finalità di volta in volta perseguite e di quelli che esso trasmette al fornitore incaricato della stampa e della spedizione della Carta; alla determinazione dei tempi di conservazione dei dati trattati; alla sicurezza e robustezza degli strumenti di autenticazione informatica e delle misure di conservazione delle credenziali; al richiamo alle misure per garantire la qualità dei dati dell'Anagrafe nazionale degli studenti; all'individuazione delle specifiche misure tecniche e organizzative previste a tutela dei diritti e delle libertà degli interessati in relazione ai trattamenti effettuati.

Anagrafe nazionale dell'istruzione superiore

Un parere favorevole sottoposto a condizioni è stato espresso sullo schema di decreto predisposto dal Ministro dell'università e della ricerca, concernente l'Anagrafe nazionale dell'istruzione superiore (Anis) e relativi allegati (provv. 21

luglio 2022, n. 267, doc. web n. 9806759) allo scopo di completare il quadro giuridico di riferimento delineato dal decreto 19 gennaio 2022, n. 114, adottato in via di prima attuazione dell'art. 62-*quinquies* del Cad (v. parere 2 dicembre 2021, n. 428, doc. web n. 9731869).

Il Garante nel parere ha posto come specifica condizione che: siano definiti in modo puntuale i dati personali oggetto di trattamento e che, con particolare riguardo a quelli indicati all'art. 6 dello schema (Isee, condizione occupazionale, altri dati), siano trattati solo quelli "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità" perseguite; siano chiarite le specifiche modalità di alimentazione dell'Anagrafe (mera consultazione o acquisizione dei dati), precisando quali dati siano attinti dall'Anagrafe nazionale dello Studente (Ans) e quali da altre banche dati stabilendone, in ogni caso, presupposti, modalità e garanzie a tutela degli interessati, anche in termini di qualità delle informazioni trattate; sia chiarito il ruolo rivestito dal Ministero e dalle istituzioni della formazione superiore con riguardo ai trattamenti effettuati tramite Anis, con particolare riferimento all'erogazione dei servizi di certificazione; siano individuati in modo specifico i soggetti o le categorie di soggetti che possono accedere all'Anis, specificando, altresì, le rispettive finalità istituzionali perseguite; siano stabiliti tempi di conservazione dei dati personali proporzionati all'obiettivo perseguito in relazione a ciascuna tipologia di dati.

Trattamenti di dati personali nel contesto dell'emergenza da Covid-19

In merito al settore scolastico e universitario e alla prosecuzione delle attività didattiche e formative nel contesto dell'emergenza epidemiologica da Covid-19, si è provveduto alla elaborazione di nuove FAQ riguardanti i profili in materia di protezione dei dati personali derivanti dall'applicazione del d.l. n. 1/2022, con particolare riferimento alla gestione dei nuovi casi di positività in ambito scolastico.

È stato in primo luogo chiarito che le scuole secondarie di I e II grado e gli istituti di istruzione e formazione professionale, in qualità di titolari del trattamento, nell'ipotesi in cui in una classe si siano verificati due casi positivi, possono trattare i dati forniti dagli alunni per lo svolgimento in presenza dell'attività didattica (conclusione del ciclo vaccinale primario e guarigione da meno di centoventi giorni, effettuazione della dose di richiamo) assicurando che le verifiche dei suddetti requisiti siano effettuate quotidianamente nei confronti dei soli studenti che fruiscano della didattica in presenza e per il periodo di dieci giorni previsto dalla legge; esclusivamente per assicurare lo svolgimento della didattica in presenza nei suddetti casi, con esclusione di ogni altra finalità; secondo modalità che assicurino la sicurezza e l'integrità dei dati; senza acquisizione preventiva della relativa documentazione (certificato vaccinale o di guarigione, *green pass*) che deve essere esclusivamente esibita dall'alunno all'atto del controllo; nel caso di esibizione del *green pass*, utilizzando esclusivamente l'*app* di verifica C-19 (modalità rafforzata); da personale autorizzato e istruito. Il titolare deve astenersi dal raccogliere il certificato vaccinale o di guarigione, o *green pass* nonché dal diffondere l'elenco degli alunni che svolgono la didattica in presenza o da remoto (cfr. FAQ - Trattamento dati nel contesto scolastico nell'ambito dell'emergenza sanitaria, in part. FAQ n. 14, doc. web n. 9337010).

È stato inoltre evidenziato che, in base al quadro normativo di riferimento, l'esecuzione gratuita di test antigenici rapidi è prevista per gli alunni delle scuole secondarie di primo e secondo grado, sottoposti ad autosorveglianza, dietro prescrizione del medico di medicina generale o del pediatra di libera scelta, nonché, per i soggetti che non possono ricevere o completare la vaccinazione anti Sars-CoV-2, sulla base di idonea certificazione medica. In tali casi, le strutture abilitate a eseguire i test possono trattare i dati personali necessari a comprovare la sussistenza

dei requisiti di legge contenuti nella documentazione fornita dagli interessati, senza richiedere ulteriori informazioni (es. stato vaccinale) (cfr. FAQ n. 15).

Nel corso dell'anno di riferimento, sono stati definiti reclami e segnalazioni aventi ad oggetto la pubblicazione, su siti web di istituti scolastici e sul registro elettronico, di dati personali, anche relativi alla salute degli alunni ovvero la comunicazione a terzi dei predetti dati, in assenza di una base giuridica idonea.

Trattamenti di dati anche relativi alla salute, di alunni e studenti

In un caso una scuola aveva inviato il calendario delle riunioni del Gruppo di lavoro operativo per l'inclusione scolastica (di seguito Glo) – recanti l'elenco di tutti gli alunni interessati distinti per classe – oltre che ai soggetti tenuti ad esserne informati, a tutti i genitori invitati a partecipare alle riunioni del Glo. Tali comunicazioni recavano inoltre, in chiaro, l'indirizzo di posta elettronica dei destinatari delle comunicazioni.

Il Garante ha chiarito che la convocazione di una riunione del Glo per l'inclusione scolastica, prevista dalla normativa di settore in materia di disabilità, recante in chiaro il nominativo dell'alunno, rappresenta di per sé una informazione relativa allo stato di salute dell'alunno interessato, da fornire solo ai genitori dello studente, ai docenti della classe di appartenenza e ai soggetti coinvolti nell'intervento terapeutico e formativo (cfr. art. 9, comma 10, d.lgs. 13 aprile 2017, n. 66); trattandosi, quindi, di una comunicazione di dati personali in violazione degli artt. 5, 6, 9 del RGPD e 2-*ter* e 2-*sexies* del Codice è stata comminata all'istituto scolastico una sanzione amministrativa pecuniaria (provv. 28 aprile 2022, n. 148, doc. web n. 9777156).

Similmente un istituto scolastico aveva pubblicato, nell'area del registro elettronico riservata alle comunicazioni, una circolare contenente gli elenchi, divisi per classe, degli alunni, "richiedenti la frequenza delle lezioni in presenza o tramite DDI", recanti, in corrispondenza del nominativo di taluni alunni, il riferimento "alle categorie Bes, Dsa o Alunno h". L'istituto non aveva, inoltre, fornito riscontro all'istanza di esercizio dei diritti ai sensi degli artt. da 15 a 22 del RGPD, presentata dai reclamanti.

Il Garante ha ricordato che tali sigle forniscono informazioni sullo stato di salute degli interessati e che in questo modo sono state comunicate a tutti i genitori degli alunni della singola classe di riferimento in violazione degli artt. 5, 6, 9 del RGPD e 2-*ter* e 2-*sexies* del Codice. Per questo, e per il mancato riscontro all'istanza di esercizio dei diritti ricevuta ai sensi dell'art. 83 del RGPD, è stata comminata una sanzione amministrativa (provv. 15 dicembre 2022, n. 421, doc. web n. 9852255).

In un altro caso uno studente aveva lamentato, con reclamo al Garante, di aver ricevuto una contestazione disciplinare basata sul contenuto delle dichiarazioni da lui rese nel corso di un'assemblea degli studenti, svoltasi mediante piattaforma zoom.

Nell'istruttoria è emerso che nei locali del conservatorio era stata rinvenuta una chiavetta Usb contenente la registrazione dell'assemblea e che il conservatorio l'aveva depositata al protocollo riservato e incaricato un perito di trascriverne i contenuti, successivamente utilizzati per il procedimento nei confronti del reclamante.

L'Autorità, nel richiamare i principi di liceità, correttezza, trasparenza e di limitazione della finalità, ha chiarito che il conservatorio avrebbe dovuto astenersi dal trattare i dati personali contenuti nel dispositivo Usb e, in assenza di elementi volti a identificare il proprietario del dispositivo, avrebbe dovuto consegnarlo alle autorità competenti, astenendosi dall'acquisirlo e dal trattare i dati personali in esso contenuti in assenza di idoneo presupposto di liceità, e quindi in violazione degli artt. 5 e 6 del RGPD e 2-*ter* del Codice.

L'incarico al perito in assenza di una previa regolamentazione del rapporto ai sensi dell'art. 28 del RGPD e dei presupposti per considerarlo autorizzato ai sensi dell'art. 29 del RGPD ha dato luogo a una comunicazione a terzi di dati personali in violazione degli artt. 5 e 6 del RGPD e 2-*ter*, commi 1 e 4, lett. *a*), del Codice.

È stato inoltre ravvisato che la designazione del Rpd sia avvenuta in violazione dell'art. 38, par. 6, del RGPD, trattandosi di un soggetto che, in ragione del ruolo rivestito all'interno della struttura dell'istituto, si trovava in posizione di conflitto d'interessi (cfr. par. 4.6).

In relazione ai predetti elementi e tenuto conto della particolare delicatezza dei dati personali illecitamente trattati riguardanti le opinioni espresse da studenti nel contesto di un'assemblea è stata comminata al conservatorio una sanzione amministrativa pecuniaria (provv. 10 novembre 2022, n. 367, doc. web n. 9835095).

4.4. *Trasparenza e pubblicità dell'azione amministrativa*

Le numerose questioni riguardanti il tema della protezione dei dati personali con riferimento alle esigenze di trasparenza e di pubblicità dell'azione amministrativa, per chiarezza espositiva, sono suddivise in relazione ai principi di *data protection by design* e *by default*, alla pubblicazione di dati personali *online* e all'accesso civico a informazioni e documenti detenuti dalla p.a. (art. 5, d.lgs. n. 33/2013).

4.4.1. Il rispetto della data protection by design *e* by default

Registrazione delle riunioni di organi collegiali

Nel periodo di riferimento l'Autorità ha ribadito che è in primo luogo il titolare del trattamento a dover mettere in atto misure tecniche e organizzative adeguate, per attuare i principi di protezione dei dati fin dalla progettazione (*data protection by design*) e garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento (*data protection by default*), in conformità a quanto richiesto dall'art. 25, parr. 1 e 2, del RGPD.

Al riguardo, si segnalano i quesiti posti dal Consiglio di Stato sul regime applicabile alla registrazione delle riunioni dell'organo collegiale dell'Agcom, volti a conoscere in particolare quali fossero "le condizioni da osservare per garantire la riservatezza e il corretto svolgimento dei lavori dell'Organo consiliare allorquando essi si svolgano con la partecipazione da remoto di alcuni o di tutti i relativi componenti" e se fosse "possibile, o meno, autorizzare il Commissario che ne faccia richiesta alla registrazione dei lavori stessi, da remoto ovvero in presenza, precisando altresì, in caso di risposta affermativa, con quali cautele e mezzi di realizzazione". In tale contesto, è stato rappresentato che Agcom – nella sfera di autonomia organizzativa riconosciuta dall'art. 1, comma 9, l. n. 249/1997 – può trattare lecitamente i dati personali nell'ambito della videoripresa delle sedute del Consiglio in base al proprio regolamento interno concernente l'organizzazione e il funzionamento dell'Agcom (delibera 27/4/2012, n. 223/12/CONS, come modificata dalla delibera 22/7/2021, n. 238/21/CONS). Quanto all'eventuale registrazione dei lavori delle sedute del Consiglio di Agcom è stato evidenziato che per un'autorità pubblica il consenso dei partecipanti non può costituire un valido presupposto per il trattamento dei dati personali (cons. n. 43 del RGPD), sicché la possibilità o meno di autorizzare eventuali registrazioni va disciplinata nell'ambito dell'autonomia organizzativa propria di Agcom, anche tramite il regolamento di cui all'art. 1, comma 9, l. n. 249/1997. Spetta quindi al regolamento interno disciplinare: l'eventuale possibilità di registrazione e i soggetti a ciò legittimati, precisandone condizioni e limiti; le modalità di trattamento; le finalità (determinate, esplicite e legittime) della raccolta/registrazione dei dati; i tempi di conservazione; l'impegno a che i dati siano "successivamente trattati in modo che non sia incompatibile con [le] finalità [determinate]" (art. 5, par. 1, lett. *b*) e *c*), del RGPD) (provv. 27 gennaio 2022, n. 4, doc. web n. 9745318).

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

Si continuano a registrare casi di pubblicazione *online* da parte delle p.a. di dati sulla salute in violazione dell'art. 2-*septies*, comma 8, del Codice e dell'art. 9, parr. 1, 2 e 4, del RGPD.

Registro degli accessi civici

Nello specifico, è stata sanzionata un'azienda sanitaria per la diffusione sul proprio sito web dei dati personali di numerosi soggetti che avevano formulato richieste di accesso civico e documentale all'asl inseriti nel registro degli accessi pubblicato *online*. In particolare, si trattava di informazioni quali il nominativo del soggetto interessato nonché i relativi dati sulla salute, considerando che la tipologia di atti richiesti alla asl, nella maggior parte degli accessi, riguardava documentazione sanitaria (fra cui cartelle cliniche, accertamenti di invalidità, test, relazioni tecniche, ecc.) (provv. 26 maggio 2022, n. 199, doc. web n. 9784482).

Illegittima diffusione di dati personali

Diverse sanzioni o ammonimenti sono stati adottati nei confronti di enti pubblici per aver diffuso *online* dati personali in assenza di un'idonea base normativa in violazione dell'art. 2-*ter*, commi 1 e 3, del Codice e dell'art. 6, par. 1, lett. *c*) ed *e*); par. 2 e par. 3, lett. *b*), del RGPD; nonché del principio di minimizzazione di cui all'art. 5, par. 1, lett. *c*), del RGPD. Ciò con particolare riferimento alla pubblicazione di dati e informazioni personali su siti web istituzionali di una regione e di due comuni riferiti a:

Benefici economici a persone in stato di disagio

- beneficiari di contributi economici riservati a "soggetti particolarmente danneggiati a seguito dell'epidemia da Covid-19", che hanno avuto una riduzione dell'"ammontare del fatturato e dei corrispettivi […]", idonei pertanto a rivelare una situazione di disagio economico-sociale (anche temporanea) degli interessati, nonché soggetti che non sono stati ammessi ad alcun beneficio economico in violazione anche della disciplina statale in materia di trasparenza contenuta nell'art. 26, comma 4, d.lgs. n. 33/2013 (provv. 26 maggio 2022, n. 197, doc. web n. 9789564);

Delibere di costituzione in giudizio del comune

- reclamanti e loro familiari come i figli minori (compresa la circostanza dell'esistenza di un procedimento giudiziario attivato nei confronti del comune), nelle delibere di giunta comunale di costituzione in giudizio dell'ente in un procedimento giudiziario con nomina del relativo rappresentante legale (provv. ti 9 giugno 2022, n. 62, doc. web n. 9789037 e n. 63, doc. web n. 9789488). Il Garante ha chiarito che vanno indicate le sole informazioni necessarie a identificare la causa, per cui sarebbe sufficiente inserire in chiaro anche solo il numero del ruolo generale o alcuni dati della causa non riferibili a persone fisiche. Nel caso in esame, il nome dei reclamanti e relativi familiari potevano essere tranquillamente omessi o oscurati in sede di pubblicazione dell'atto, senza compromettere il rispetto del principio di pubblicità o trasparenza dell'azione amministrativa (cfr. provv. 28 aprile 2022, n. 40, doc. web n. doc. web n. 9777127, cit. *infra* par. 13.10).

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 ai Responsabili della prevenzione della corruzione (Rpct) e ai Difensori civici ai sensi dell'art. 5, commi 7 e 8, d.lgs. n. 33/2013.

Casi di esclusione

In evidenza diversi interventi in ordine alla sussistenza di casi di esclusione ai sensi dell'art. 5-*bis*, comma 3, d.lgs. n. 33/2013, con particolare riferimento a richieste di accesso civico aventi a oggetto:

Dati sulla salute

- la copia di registri di corsia di un ospedale (registro giornaliero delle attività di reparto/corsia e registro giornaliero pazienti in reparto/corsia) contenente dati quali nome e cognome del paziente, specialistica medica relativa al ricovero, reparto,

data di dimissione, numero di giorni di degenza. È stato al riguardo ribadito che i dati erano riconducibili alla definizione di dati sulla salute, attenendo alla «prestazione di servizi di assistenza sanitaria» e rivelando «informazioni relative [allo] stato di salute» dei soggetti interessati (art. 4, par. 1, n. 15, del RGPD). Pertanto, trattandosi di un'"eccezione assoluta", l'amministrazione è tenuta a rifiutare l'accesso "senza necessità di dover svolgere ulteriori valutazioni in ordine alla sussistenza di un eventuale pregiudizio concreto agli interessi dei soggetti interessati" (provv. 18 novembre 2022, n. 381, doc. web n. 9832560);

- l'intero *database* utilizzato per uno studio clinico, contenente dati e informazioni dei pazienti partecipanti, conservati in forma pseudonima, fra cui gli identificatori diretti e quasi identificatori, quali: codice identificativo del paziente e del centro arruolante; età al ricovero; etnia; peso; altezza; abitudini al fumo; data del ricovero; data del tampone; data di uscita dallo studio. L'Autorità ha evidenziato che anche il dato pseudonimo – risultante da un procedimento di pseudonimizzazione come definita dall'art. 4, par. 1, n. 5, del RGPD – è un dato personale, in quanto riferito a persona fisica, identificabile, sicché le informazioni erano riconducibili alla definizione di «dati sulla salute», attenendo alla «prestazione di servizi di assistenza sanitaria» e rivelando «informazioni relative [allo] stato di salute» dei soggetti che avevano partecipato allo studio clinico (art. 4, par. 1, n. 15, del RGPD) (provv. 31 ottobre 2022, n. 358, doc. web n. 9830919);

- la copia degli elenchi, in possesso dell'Inps, dei soggetti sottoposti a visita per il riconoscimento della cecità civile, con indicazione dei relativi nominativi e indirizzi. Nel caso di specie, si trattava di soggetti che avevano chiesto all'ente il riconoscimento della cecità civile sottoponendosi ad apposita visita medica e pertanto di «qualificazioni sanitarie che determinano il riconoscimento dello *status* di soggetto invalido civile» (art. 4, par. 1, n. 15; cons. 35, RGPD) (provv. 22 aprile 2022, n. 137, doc. web n. 9774019);

- la documentazione inerente alle pratiche di risarcimento per lesioni subite da persone fisiche a seguito di sinistri verificatisi nel territorio comunale elencati in due determinazioni dirigenziali che rientravano nella definizione di dati relativi alla salute (provv. 15 febbraio 2022, n. 56, doc. web n. 9750482).

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

In altri casi, il Garante ha fornito parere su richieste di accesso civico generalizzato, esprimendosi sulla sussistenza del limite derivante dalla protezione dei dati personali di cui all'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013.

Dati detenuti dal centro antiviolenza sulle donne

Ciò con particolare riferimento a:

- dati e documenti detenuti da un comune riguardanti l'attività svolta da un centro antiviolenza donne negli ultimi cinque anni, con particolare riferimento ad attività di rendicontazione, agli avvocati e responsabili legali coinvolti, nonché all'attività giudiziaria (provv. 24 ottobre 2022, n. 357, doc. web n. 9829003). In tale fattispecie è stato evidenziato in particolare che i «centri antiviolenza operano in collaborazione con la rete dei servizi sociali e sanitari territoriali e con le forze dell'ordine, al fine di garantire la massima sicurezza e protezione alle donne che subiscono violenza, sole o con figli minori, e un percorso di presa in carico integrata e globale» (art. 12, comma 1, l.r. Puglia 4 luglio 2014, n. 29; cfr. anche art. 3, comma 2, lett. *a*), e 11 della medesima legge, nonché art. 80, comma 9 del reg. Regione Puglia 18 gennaio 2007, n. 4). Pertanto i limiti all'accesso civico riguardavano anche questioni inerenti alla tutela degli interessi pubblici legati alla tutela della «sicurezza e ordine pubblico» nonché «alla conduzione di indagini su reati e loro perseguimento» (cfr. art. 5-*bis*, comma 1, lett. *a*) ed *f*), d.lgs. n. 33/2013). Limitatamente ai profili in materia di protezione dei dati personali è stata in ogni caso invitata l'amministrazione a fornire riscontro tenendo conto della natura particolarmente delicata dei dati e delle

informazioni riferite al centro antiviolenza e alla necessità di tutelare la riservatezza e l'anonimato di persone e attività del centro stesso;

- tutte le *e-mail* scambiate tra una società e l'amministrazione comunale, o anche solo all'interno all'amministrazione, riferite a «comune, sindaco, assessori, distretti e altri soggetti» relative all'evento "Carnevale dei bambini 2022" organizzato dalla predetta società (provv. 28 aprile 2022, n. 158, doc. web n. 9776425). In tale caso, in relazione all'accesso civico generalizzato alla "corrispondenza *e-mail* (anche interna)" di sindaco, assessori e altri soggetti, è stato evidenziato come l'art. 5-*bis*, comma 2, lett. *b*), d.lgs. n. 33/2013 va inquadrato nell'ambito delle garanzie di cui all'art. 15 della Costituzione che tutelano "la libertà e la segretezza" delle comunicazioni interpersonali scambiate anche tramite *e-mail* (cfr., altresì gli artt. 616 ss. c.p. sul segreto della corrispondenza anche se "informatica o telematica" e le linee guida Anac recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5, comma 2, d.lgs. n. 33/2013, determinazione 28 dicembre 2016, n. 1309);

Corrispondenza ed *e-mail*

- *curricula* e allegati comprendenti i titoli dei soggetti controinteressati (contenenti dati anagrafici, di residenza, *e-mail* e numeri di telefono professionale e personale, nazionalità, codice fiscale e stato civile, notizie di carattere professionale e privato ivi compresa una dettagliata descrizione di tutte le esperienze professionali effettuate con dettagli sull'inquadramento e funzioni assunte) (provv. 7 gennaio 2022, n. 2, doc. web n. 9742743);

Dati dei lavoratori

- nominativi di tutti i dipendenti di una direzione provinciale di un'amministrazione centrale dello Stato a cui era stata rinviata, per motivi di servizio, la fruizione dei giorni di ferie maturati rispettivamente nel corso degli anni 2019 e 2020, ivi compreso il numero di giorni di ferie rinviati, nonché la copia di tutti i provvedimenti amministrativi che avevano disposto il predetto rinvio (provv. 15 luglio 2022, n. 249, doc. web n. 9809119);

- dati relativi alla valutazione del personale, fra cui schede di rendicontazione e di autovalutazione dei dirigenti e del segretario generale (provv. 14 novembre 2022, n. 380, doc. web n. 9831454);

- tutti i titoli di studio, laurea e *master* conseguiti dal soggetto controinteressato, con descrizione di tutti i corsi effettuati presso l'università destinataria dell'istanza di accesso civico, con indicazione dei relativi anni accademici, il titolo delle tesi e delle relazioni presentate, nonché le votazioni finali ottenute (provv. 4 febbraio 2022, n. 37, doc. web n. 9746944);

Titoli di studio

- copia dei pagamenti dei tributi Ici, Imu e Tarsu di tutti i componenti di un consiglio comunale e del sindaco, riferiti agli ultimi cinque anni, comprensivi di dati catastali (subalterno e particella) degli immobili in possesso e/o in comunione. In tal caso, è stato evidenziato che i dati e le informazioni personali contenuti nella documentazione richiesta erano di diversa natura e specie (oltre ai dati identificativi e anagrafici, anche quelli di residenza e dei beni immobili in possesso e in comunione con indicazione dei contributi versati), con possibilità di ricostruire tra l'altro la situazione economica e di vita dell'amministratore comunale, il tenore di vita o la situazione patrimoniale. Nelle valutazioni effettuate è stato anche considerato che per la dimensione del comune coinvolto (poco più di 3.400 abitanti), fermo restando gli obblighi di pubblicazione sul sito web istituzionale per finalità di trasparenza previsti dall'art. 14, comma 1, lett. *a*) - *e*), d.lgs. n. 33/2013 per i titolari di incarichi politici, non trovavano applicazione gli obblighi di pubblicità relativi alle dichiarazioni reddituali e patrimoniali degli amministratori locali, previsti dalla lett. *f*) del medesimo articolo per gli altri enti locali (cfr. par. 2.1. della determinazione Anac 8 marzo 2017, n. 241) (provv. 4 marzo 2022, n. 80, doc. web n. 9753567);

Pagamento tributi

Assegnazione di un nuovo numero civico

- informazioni personali riferite a tre soggetti identificati e inerenti all'esistenza o meno nei loro confronti di attività di riscossione coattiva di somme asseritamente non versate al comune e concernenti la tassa sui rifiuti (Tari) (provv. 7 luglio 2022, n. 246, doc. web n. 9799635);

- copia integrale di tutta la documentazione funzionale all'attribuzione di un nuovo numero civico, riferita a un'abitazione, contenente dati e informazioni personali di diversa natura e specie (quali dati anagrafici, recapiti telefoni, peraltro non necessariamente attuali, dei soggetti controinteressati; ma anche notizie private relative alla proprietà posseduta, alle caratteristiche del fabbricato e al sopralluogo a suo tempo effettuato) (provv. 27 gennaio 2022, n. 31, doc. web n. 9745282);

Ispezioni di allevamenti avicoli

- documentazione contenente dati e informazioni personali riguardanti allevamenti e stabilimenti avicoli (autorizzazioni e verbali di ispezioni) (provv. 3 ottobre 2022, n. 314, doc. web n. 9831369);

Elenco dei recapiti dei responsabili unici del procedimento

- *file* integrale comprendente i recapiti dei responsabili unici del procedimento (quali *e-mail*/Pec) iscritti al SIMOG/BDCP/AUSA detenuti da Anac negli ultimi tre anni. Al riguardo, è stato evidenziato che un eventuale accoglimento dell'istanza di accesso civico generalizzato all'elevato numero di recapiti (*e-mail*/Pec) di tutti i Rup avrebbe l'effetto di modificare il regime di conoscibilità dei predetti dati personali, che verrebbero raccolti un unico *file*/*database* a disposizione del soggetto istante (o di terzi a cui potrebbero essere comunicati), accrescendone la vulnerabilità o possibili usi distorsivi da parte di terzi (ad es., per l'invio di comunicazioni indesiderate) e per finalità allo stato non conosciute (né conoscibili), senza tenere in considerazione le ragionevoli aspettative degli interessati riguardo al trattamento dei propri dati personali al momento in cui questi sono stati resi disponibili dalle stazioni appaltanti o comunicati ad Anac, in violazione dei principi di protezione dei dati, fra cui quello di «minimizzazione» e di «limitazione della finalità» (cfr. art. 5, par. 1, lett. *b*) e *c*), del RGPD; v. linee guida Anac in materia di accesso civico, par. 8.1) (provv. 15 dicembre 2022, n. 437, doc. web n. 9843353).

Carenze istruttorie

Si segnalano, infine, diversi casi in cui il Garante ha rappresentato che il mancato invio della documentazione istruttoria da parte del Rpct e la carente indicazione dei motivi per i quali si riteneva sussistere il limite alla protezione dei dati personali (utilizzando mere formule di stile) ha impedito a questa Autorità di esprimersi nel merito delle questioni sottoposte dal Rpct, per cui ci si è limitati a fornire indicazioni di carattere generale (provv.ti 27 maggio 2022, n. 206, doc. web n. 9819719; 10 giugno 2022, nn. 222, doc. web n. 9819702 e 223, doc. web n. 9821576) o a rinviare a precedenti orientamenti del Garante sulle specifiche materie (sui procedimenti disciplinari: provv.ti 1° aprile 2022, n. 110, doc. web n. 9767096; 7 aprile 2022, n. 131, doc. web n. 9774842; sull'accesso ai titoli dei dirigenti: provv. 1° giugno 2022, n. 208, doc. web n. 9789100; sulle dichiarazioni rese ai sensi degli artt. 46 e 47, d.P.R. n. 445/2000: provv. 12 maggio 2022, n. 184, doc. web n. 9781347; sulle procedure edilizie: provv.ti 14 marzo 2022 nn. 92, doc. web n. 9761449 e 93, doc. web n. 9761464).

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

4.5.1. Tributi locali

È pervenuto un quesito, da parte del Rpd di un comune, circa la legittimità della comunicazione, da parte dell'ente locale ad una società, dell'elenco dei contribuenti Tari (nome, cognome, codice fiscale, partita iva), nonché degli importi relativi ad ogni singolo utente e le indicazioni sull'avvenuto pagamento del tributo. Scopo di

tale comunicazione è la restituzione, da parte della società, dell'importo (versato dagli utenti a titolo di Tari), spendibile tramite una carta di credito valida presso gli operatori convenzionati e alle condizioni definite dalla stessa società. Al riguardo, alla luce dei limiti entro i quali è consentito trattare dati personali ad un soggetto pubblico (cfr. art. 6, par. 1, lett. *c*), ed *e*), par. 3, del RGPD e art. 2-*ter* del Codice) e considerato che l'iniziativa prospettata nel sopracitato quesito non rappresenta un servizio istituzionale dell'ente locale, ma piuttosto un'operazione finanziaria che, anche se presentata come vantaggiosa per i contribuenti e per il territorio, avrebbe esposto i cittadini a un sistema finanziario diretto a orientare le scelte di acquisto, l'Autorità ha ritenuto che la comunicazione, da parte degli enti locali, degli elenchi richiesti dalla società risulta priva di alcuna condizione di liceità (nota 31 maggio 2022).

4.5.2. Rifiuti urbani

Continuano a pervenire reclami e quesiti riguardanti la gestione dei rifiuti urbani da parte degli enti locali o gestori pubblici da loro delegati, con particolare riferimento alla compatibilità con la protezione dei dati personali delle regole riguardanti le modalità di conferimento dei rifiuti.

Al riguardo, si è chiarito che la gestione dei rifiuti urbani rientra tra i compiti di interesse pubblico affidati agli enti locali (art. 6, par.1, lett. *e*), del RGPD), che può essere svolto anche da un soggetto terzo, cd. gestore del pubblico servizio, in nome e per conto dell'ente, il quale è comunque tenuto, a rispettare la disciplina applicabile (artt. 4, par. 1, punto 8) e 28 del RGPD). Nel difficile bilanciamento tra la protezione dei dati personali e le esigenze ambientali la normativa consente comunque agli organi addetti al controllo "di procedere a ispezioni di cose e luoghi diversi dalla privata dimora per accertare le violazioni di rispettiva competenza" (art. 13, l. 24 novembre 1981, n. 689). Si è ribadito, in ogni caso, l'invito ai cittadini, laddove lo ritengano opportuno, ad adottare autonomamente alcune misure poste a garanzia della propria riservatezza (quali, ad es., l'oscuramento dei dati personali nei rifiuti cartacei) (note 18 febbraio e 15 marzo 2022).

Diffusione di video su *social network*

A seguito di una segnalazione è emerso che una società, gestore del servizio di raccolta dei rifiuti urbani per un comune, aveva installato alcune videocamere allo scopo di individuare e sanzionare comportamenti illegali, diffondendo poi nel proprio profilo Facebook alcune immagini riprese dai sistemi di videosorveglianza installati sul territorio comunale, dalle quali risultavano identificabili alcuni interessati.

La raccolta delle immagini è risultata rivolta all'acquisizione dei mezzi di prova per l'accertamento e la contestazione degli illeciti amministrativi, ma la pubblicazione su Facebook è stata considerata incompatibile con le finalità in base alle quali i dati sono stati precedentemente raccolti e trattati, con conseguente violazione del principio di limitazione della finalità di cui all'art. 5 par. 1, lett. *b*), del RGPD. Per tale ragione, sono stati sanzionati la società (provv. 28 aprile 2022, n. 163, doc. web n. 9777996) e il comune, titolare del trattamento (provv. 28 aprile 2022 n. 162, doc. web n. 9777974).

4.5.3. Mobilità e trasporti

Piattaforma unica nazionale dei Cude

L'Autorità ha espresso parere su un documento del Ministero delle infrastrutture e della mobilità sostenibile contenente la proposta di semplificazione delle modalità operative per l'istituzione della Piattaforma unica nazionale informatica per il rilascio del contrassegno unificato disabili europeo (Cude).

Con provvedimento 15 aprile 2021, n. 143 (doc. web n. 9590407), il Garante aveva già espresso parere favorevole sullo schema di decreto che definiva le procedure

per l'istituzione della predetta Piattaforma, riservandosi di adottare gli ulteriori atti e valutazioni di competenza, incluse eventuali specifiche misure di garanzia, ai sensi dell'art. 9, par. 4, del RGPD e dell'art. 2-*septies*, comma 4, lett. *a*), del Codice. La proposta di semplificazione presentata ha specificato i dati trattati e i soggetti abilitati ad accedere alla Piattaforma ovvero il titolare del contrassegno, il personale autorizzato del comune e il personale autorizzato ad effettuare i controlli previsti dal codice della strada. Inoltre, la Piattaforma, oltre a non prevedere la raccolta di dati riferibili al titolare/beneficiario del contrassegno, in un'ottica di minimizzazione, non acquisisce neppure il codice alfanumerico identificativo del Cude. La soluzione tecnica proposta ha tenuto conto di alcune indicazioni fornite dall'Ufficio, riguardanti, tra l'altro, il ruolo assunto dai vari soggetti coinvolti nel trattamento dei dati personali (Ministero delle infrastrutture e mobilità sostenibile, comuni, enti aggregatori), le funzionalità della Piattaforma, i profili di autorizzazione, le modalità per rendere l'informativa agli interessati e quelle per l'esercizio dei diritti, i tempi di conservazione dei dati, le procedure di autenticazione degli utenti. La consultazione delle informazioni della Piattaforma da parte degli operatori autorizzati dei comuni e dei cd. enti aggregatori, nonché dei soggetti deputati ad effettuare i controlli previsti dal codice della strada, è consentita solo per i rispettivi compiti e gli accessi e le operazioni effettuate sono tracciati (provv. 28 aprile 2022, n. 143, doc. web n. 9774890, *Newsletter* 30 maggio 2022, n. 490, doc. web n. 9774926).

Utilizzo della Pec per la notifica delle sanzioni relative al codice della strada

Continuano a prevenire diversi reclami e segnalazioni aventi ad oggetto la notifica di sanzioni, per violazione del codice della strada, attraverso la Pec inerente all'attività lavorativa e professionale degli interessati (es. studi professionali).

Al riguardo, la circolare 17 novembre 2021 n. 300/STRAD/1/10060.U/2021 del Ministero dell'interno non ha sciolto del tutto i dubbi circa la compatibilità della notifica via Pec delle contravvenzioni per violazione del codice della strada nelle ipotesi in cui l'indirizzo non risulti direttamente e agevolmente riferibile ad uno studio professionale.

Sul punto, si è chiarito che laddove l'indirizzo Pec cui è stato notificato il verbale di contravvenzione al codice della strada non sia direttamente e agevolmente riferibile ad uno studio professionale, non sussiste il rischio automatico di una comunicazione dei dati personali dell'interessato (il singolo professionista) a terzi (collaboratori, segretari, associati, ecc.), atteso che a tale indirizzo Pec potrebbero accedere soggetti diversi dal professionista intestatario solo su espressa autorizzazione di quest'ultimo (note 21 e 31 marzo, 20 aprile e 27 luglio 2022).

Linee guida taxi

L'Autorità di regolazione dei trasporti ha sottoposto all'attenzione del Garante lo schema di linee guida in materia di adeguamento del servizio taxi per regioni ed enti locali. Nell'ambito delle interlocuzioni formali con gli uffici, è stata sottolineata l'importanza di garantire l'anonimizzazione dei dati (in linea con quanto previsto dal cons. 26 del RGPD e alla luce dei principi fissati dal Gruppo Art. 29 nel parere 5/2014 sulle tecniche di anonimizzazione adottato il 10 aprile 2014) in una fase antecedente alla comunicazione degli stessi ai comuni da parte dei titolari di licenza e/o delle cooperative, per assicurare la riservatezza dei dati personali dei soggetti coinvolti (utenti finali del servizio e titolari di licenza). In subordine, è stata evidenziata la necessità di individuare un'idonea base giuridica del trattamento (art. 6, parr. 1, lett. *c*) ed *e*); 3, del RGPD e art. 2-*ter* del Codice), una corretta individuazione dei ruoli (e delle conseguenti responsabilità) ricoperti da regioni, enti locali e cooperative radio taxi, nonché le misure atte a garantire il rispetto dei principi di cui all'art. 5 del RGPD (nota 7 marzo 2022).

4.5.4. Servizi online *e misure di sicurezza*

Il Garante ha adottato un provvedimento sanzionatorio nei confronti di una società consortile per azioni, con prevalente capitale pubblico, costituita per la gestione di un servizio idrico integrato, per non aver protetto adeguatamente i dati dei clienti registrati sull'area riservata del proprio sito web. All'esito dell'istruttoria è stato accertato che l'accesso al sito web dell'azienda su cui transitavano numerosi dati personali degli utenti (quali credenziali di autenticazione, nomi, cognomi, codici fiscali/numeri di telefono e dati di fatturazione), avveniva tramite il protocollo di rete http, non crittografato e non sicuro ovvero in maniera non conforme ai principi di integrità, riservatezza e protezione dei dati fin dalla progettazione, in violazione degli artt. 5, par. 1, lett. *f*), 25, par. 1, e 32, del RGPD. Nel motivare la decisione, l'Autorità ha evidenziato in particolare che per esigenze di sicurezza l'interazione degli utenti con un sito web ai fini della trasmissione di dati personali deve essere sempre protetta con protocolli crittografici (come quello https) (provv. 6 ottobre 2022, n. 328, doc. web n. 9817058; cfr. *Newsletter* 24 ottobre 2022, n. 496, doc. web n. 9817079).

Portale *online* di un'azienda del servizio idrico integrato

A seguito di una comunicazione di *data breach* e diverse segnalazioni si è appreso che la piattaforma utilizzata dal corpo di Polizia locale di un comune per la gestione delle contravvenzioni al codice della strada, contenente i dati personali dei cittadini destinatari di contravvenzioni, è stata oggetto di un accesso abusivo da parte di soggetti non autorizzati.

Servizio *online* per la gestione delle contravvenzioni

Dall'istruttoria è emerso che il comune, titolare del trattamento, aveva stipulato con una società un contratto per la fornitura delle licenze del *software* utilizzato per la gestione delle contravvenzioni, provvedendo a regolarne i rapporti ai sensi dell'art. 28 del RGPD. Nel contratto con la società, tra l'altro, il comune aveva esplicitamente previsto a carico della stessa società di utilizzare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adatto al rischio inclusa una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative. Sono state così superate le criticità rilevate nei confronti del comune, ma non quelle nei confronti della società, tenuta a verificare costantemente l'efficacia delle misure poste a presidio della piattaforma fornita per la gestione delle contravvenzioni. Infatti il responsabile del trattamento in base alle specifiche competenze tecniche deve collaborare, anche manifestando un'autonomia propositiva, nell'adozione di misure adeguate e nella verifica sistematica dell'efficacia delle stesse, soprattutto nel caso in cui fornisca servizi a una pluralità di titolari del trattamento che coinvolgono un numero elevato di interessati (provv. 24 marzo 2022, n. 107, doc. web n. 9767635).

Cittadinanza digitale

L'Autorità ha altresì avviato una serie di istruttorie – sia d'ufficio che a seguito di segnalazioni ricevute – relative ad iniziative poste in essere da enti locali, volte ad incentivare in vari settori (ambiente, fiscalità, cultura, mobilità, ecc.) comportamenti "virtuosi" degli interessati, attraverso soluzioni basate su logiche di tipo premiale che fanno ricorso a meccanismi di *scoring*.

I predetti progetti, inquadrabili nell'ambito dei percorsi di cittadinanza digitale, si sostanziano in meccanismi finalizzati a determinare una sorta di premialità in capo al cittadino, in esito alla partecipazione a indagini che comportano una raccolta massiva di dati. Tali istruttorie, attualmente in corso, sono dirette ad acquisire ogni più utile elemento valutativo relativo a trattamenti che spesso comportano la profilazione degli interessati – inclusi soggetti vulnerabili – e dai quali possono derivare conseguenze giuridiche negative sui diritti e le libertà degli stessi.

4.6. *Il Rpd in ambito pubblico*

Una società che gestisce il servizio di raccolta dei rifiuti urbani per conto di un comune è stata sanzionata, tra l'altro (cfr. par. 4.10), per non aver designato il Rpd. Ciò in ragione della natura sostanzialmente pubblica dell'attività svolta – la quale implica il trattamento di dati personali di migliaia di cittadini nell'ambito della raccolta, trasporto e smaltimento rifiuti anche ai fini dell'accertamento e contestazione degli illeciti amministrativi derivanti dalla violazione delle norme regolamentari comunali – e tenuto anche conto che il ricorso ad un sistema di videosorveglianza comporta un monitoraggio regolare e sistematico degli interessati su larga scala (provv. 28 aprile 2022, n. 163, doc. web n. 9777996).

Un provvedimento correttivo è stato adottato nei confronti di un comune che aveva comunicato, quali dati di contatto del Rpd (una persona giuridica esterna) i propri recapiti istituzionali, anziché i dati di contatto specifici del Rpd medesimo, che pertanto risultava privo di un canale di comunicazione *ad hoc*, in contrasto con la posizione di autonomia che il Regolamento assegna al Rpd. Con il provvedimento, oltre a comminare una sanzione amministrativa, è stato ingiunto al comune di comunicare all'Autorità, ai sensi dell'art, 37, par. 7, del RGPD, gli specifici dati di contatto del Rpd designato (provv. 7 aprile 2022, n. 119, doc. web n. 9773950).

Sempre in tema di dati di contatto, è stata accertata la violazione dell'art. 37, par. 7, del RGPD da parte di un altro comune che non aveva proceduto tempestivamente né alla comunicazione all'Autorità (che deve essere effettuata mediante l'apposita procedura *online* v. https://servizi.gpdp.it/comunicazionerpd/s/) né alla pubblicazione sul proprio sito web delle informazioni di contatto riferite al Rpd di nuova designazione (provv. 15 dicembre 2022, n. 423, doc. web n. 9852800).

Un altro comune è stato sanzionato per essere stato privo di Rpd nel periodo compreso tra le dimissioni del primo Rpd e la designazione del successivo (provv. 10 novembre 2022, n. 365, doc. web n. 9834477).

Conflitto di interessi

In relazione ad un reclamo, è stato accertato che un comune aveva designato in passato, quale Rpd, il responsabile dell'area affari generali, quindi un soggetto che ricopriva una posizione apicale nell'organizzazione dell'ente, titolato ad assumere decisioni di impatto anche in materia di protezione dei dati personali, in violazione dell'art. 38, par. 6, del RGPD, integrando così un conflitto d'interessi. Altre infrazioni hanno riguardato, in violazione dell'art. 37, par. 7, del RGPD, la tardiva comunicazione dei dati di contatto del Rpd, nonché l'omessa comprova dell'idonea pubblicazione di tali dati di contatto: a tale ultimo riguardo, è stato ritenuto che la mera pubblicazione dell'atto di designazione del Rpd, indistintamente con tutti gli altri atti e provvedimenti amministrativi pubblicati dal comune, non può soddisfare l'obbligo di pubblicità previsto dal Regolamento, poiché gli interessati non sono messi in condizione di reperire facilmente e direttamente i dati di contatto del Rpd (provv. 12 maggio 2022, n. 174, doc. web n. 9781242).

Il tema del conflitto di interessi del Rpd, quale violazione dell'art. 38, par. 6, del RGPD, è stato oggetto di censura anche in un altro caso, ove un comune aveva affidato al proprio Rpd, un avvocato, il compito di difendere l'ente in alcuni giudizi civili originati da ricorsi in cui venivano sollevate eccezioni anche in merito al rispetto della normativa in materia di protezione dei dati personali. Infatti ove il Rpd medesimo avesse rilevato violazioni della normativa in materia di protezione dei dati, non avrebbe potuto portare le stesse all'attenzione del titolare del trattamento senza, al contempo, pregiudicare la posizione processuale dell'ente e il suo stesso interesse, in quanto legale, a ottenere una pronuncia favorevole. Peraltro, il reclamante, in

conseguenza del mandato ricevuto dal Rpd, non aveva potuto più rivolgersi allo stesso, confidando nella sua imparzialità nell'espletamento dei propri compiti, essendo stata svuotata, di fatto, la previsione di cui all'art. 38, par. 4, del RGPD, secondo cui gli interessati possono contattare il Rpd per tutte le questioni relative al trattamento dei loro dati personali e per l'esercizio dei loro diritti quali, ad esempio, quelli di accesso, cancellazione o limitazione (provv. 9 giugno 2022, n. 214, doc. web n. 9794895).

Anche un conservatorio è stato destinatario di un provvedimento sanzionatorio per violazione dell'art. 38, par. 6, del RGPD, avendo designato il proprio direttore, per un certo periodo, quale Rpd (provv. 10 novembre 2022, n. 367, doc. web n. 9835095).

4.7. *Ordini professionali*

L'Autorità si è occupata di alcuni ordini professionali con riguardo a diversi profili di protezione dei dati.

In un caso, un ordine provinciale dei medici chirurghi e degli odontoiatri, nel quadro della disciplina sulle modalità di accertamento dell'adempimento del requisito vaccinale da parte dei professionisti sanitari (d.l. 1° aprile 2021, n. 44), nel comunicare a taluni enti l'intervenuta sospensione del professionista reclamante, aveva inoltrato agli stessi anche una nota dell'azienda sanitaria datrice di lavoro dell'interessato contenente dati personali afferenti unicamente al rapporto di lavoro. Il Garante ha ritenuto tale comunicazione, in quanto non prevista dalla predetta normativa emergenziale, priva di base giuridica ed effettuata in violazione degli artt. 5, par. 1, lett. *a*), e 6 del RGPD, nonché 2-*ter* del Codice, nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139 (provv. 24 novembre 2022, n. 385, doc. web n. 9839018).

Un diverso ordine provinciale dei medici chirurghi e degli odontoiatri aveva, invece, rilasciato, in persona del proprio presidente e nel contesto di trasmissioni televisive, alcune dichiarazioni relative alle iniziative assunte nei confronti di un medico, espressosi in senso critico in merito a taluni obblighi di vaccinazione previsti dalla legge. L'ordine aveva inoltre dato conto di tali iniziative sul proprio sito web comunicando altresì che il professionista sarebbe stato convocato a breve per acquisire informazioni. Trattandosi di iniziative solo prodromiche all'eventuale avvio di un procedimento disciplinare e poiché il professionista non era stato destinatario di alcun provvedimento disciplinare da annotare sull'albo professionale (cfr. art. 61, comma 2, del Codice), il Garante ha dichiarato l'illiceità del trattamento, ritenendo la diffusione dei dati personali del reclamante non conforme al principio di liceità, correttezza e trasparenza, priva di una base giuridica ed in violazione degli artt. 5, par. 1, lett. *a*), e 6 del RGPD, nonché 2-*ter* del Codice (nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139). In ragione delle peculiari circostanze, l'Autorità ha, tuttavia, ritenuto sufficiente ammonire il titolare del trattamento (provv. 15 dicembre 2022, n. 418, doc. web n. 9855545).

4.8. *Digitalizzazione della pubblica amministrazione*

Nel corso del 2022 il processo di digitalizzazione della p.a. ha subito una forte accelerazione, soprattutto per effetto della necessità di dare attuazione al Pnrr. In questo contesto, il Garante ha esercitato la sua funzione consultiva sugli schemi

Spid per minori

di atti promossi dalle amministrazioni centrali in materia di erogazione dei servizi *online* ai cittadini. Inoltre, ha preso parte ad una azione di *enforcement* coordinata a livello europeo in merito all'utilizzo di servizi *cloud* in ambito pubblico (cfr. par. 21.4).

L'AgID ha chiesto al Garante di pronunciarsi sullo schema di linee guida operative per la fruizione dei servizi Spid da parte dei minori, che definiscono le modalità di rilascio dell'identità digitale al minore e le modalità di fruizione dei servizi *online* mediante tale identità.

Nel rendere un articolato parere, il Garante ha anzitutto premesso che i casi nei quali l'identità digitale Spid dei minori potrebbe essere utilizzata sono i medesimi nei quali potrebbe essere usata la Carta di identità digitale (Cie) della quale la maggiore parte dei minori è già verosimilmente in possesso, rendendo difficile ritenere, almeno in via generalizzata, proporzionati i trattamenti di dati personali connessi al rilascio e all'utilizzo delle identità digitali. Ciò, peraltro, tenendo conto che non è dato rinvenire nell'ordinamento un significativo numero di casi nei quali ai minori sia richiesto di identificarsi direttamente e non per il tramite degli esercenti la potestà genitoriale (cfr. artt. 316 e ss. c.c.). Si aggiunga che, in tal modo, nei processi di identificazione e autenticazione informatica degli utenti, viene affidata agli *identity provider* (IdP) la gestione del complesso meccanismo che regola le autorizzazioni dei genitori all'utilizzo dei servizi offerti dai fornitori dei servizi e i consensi da essi forniti al trattamento dei dati dei minori (peraltro suscettibili di consentire la profilazione del comportamento degli utenti), con un inevitabile incremento dei rischi per i diritti e le libertà degli interessati.

Nel parere condizionato il Garante ha prioritariamente rappresentato la necessità di escludere dall'applicazione delle linee guida i minori infraquattordicenni, il cui grado di maturità e consapevolezza, con caratteristiche a loro volta molto differenti nella fascia di età, non è paragonabile a quello dei minori ultraquattordicenni, specie rispetto alle insidie del mondo digitale; né vengono indicati e circoscritti gli eventuali servizi per i quali tale identità dovrebbe essere spendibile autonomamente dai minori nell'ambiente digitale. Peraltro, l'impersonificazione da parte dei genitori con l'utilizzo di credenziali di autenticazione non direttamente a loro attribuite, connaturata in questo modello, renderebbe impossibile la corretta imputazione delle operazioni al soggetto che le ha effettuate, con ricadute negative in termini di correttezza e sicurezza del trattamento (criticità peraltro aggravata in caso di servizi rivolti esclusivamente a minori, quali quelli indicati dal cons. 38 del RGPD), oltre che in violazione anche del principio di *accountability* da parte degli IdP. Ad ogni modo, il Garante, consapevole del ruolo strategico che l'identità digitale assume nel percorso di digitalizzazione del Paese e, in particolare, del mondo della scuola ha ritenuto compatibile con la normativa in materia di protezione dei dati personali, limitatamente al settore della scuola e in presenza di determinate garanzie, l'introduzione, per un periodo sperimentale, fino al 30 giugno 2023, di Spid per i minori infraquattordicenni per l'utilizzo di servizi *online* esclusivamente forniti dalle scuole a cui gli stessi possono autonomamente accedere (quale il registro elettronico), escludendo in ogni caso la fascia d'età 0-4 anni, e avendo cura di non precludere tale accesso agli studenti che non siano ancora in possesso di Spid, eventualmente anche consentendo loro l'utilizzo delle credenziali già in uso.

Al fine di valutare l'adeguatezza delle garanzie adottate ed eventualmente valutare l'introduzione di ulteriori cautele, l'AgID dovrà trasmettere un'apposita relazione all'Autorità entro il 30 aprile 2023, tenendo anche conto delle eventuali risultanze fornite dal Ministero dell'istruzione (provv. 2 febbraio 2022, n. 36, doc. web n. 9744322).

L'AgID ha sottoposto all'Autorità, ai fini dell'acquisizione del relativo parere, lo schema di linee guida recanti le regole tecniche dei gestori di attributi qualificati (ivi compresi i dati relativi al possesso di abilitazioni o autorizzazioni richieste dalla legge ovvero stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche) trattati in sede di verifica dell'identità digitale, ai sensi dell'art. 64, d.lgs. 7 marzo 2005, n. 82, e del d.P.C.M. 24 ottobre 2014.

Gestori di attributi qualificati

Il Garante, nell'esprimere parere favorevole in ragione della conformità del testo alle indicazioni fornite nel corso di riunioni informali, ha posto alcune condizioni, volte ad assicurare il rispetto dei principi di liceità, correttezza, minimizzazione dei dati e *privacy by design* e *by default* con specifico riferimento alla possibilità di consentire l'autenticazione ai servizi offerti anche mediante Cns; all'esclusione, dal novero degli attributi qualificati (e quindi, dal trattamento ivi disciplinato) delle categorie particolari di dati personali e dei dati personali relativi a condanne penali e reati (artt. 9 e 10 del RGPD), in ragione della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per gli interessati, stante l'assenza di misure appropriate e specifiche a tutela dei diritti fondamentali degli interessati; alla messa a disposizione, da parte delle *Attribute Authorities* in favore dei fornitori di servizi e per impostazione predefinita, dei soli dati personali necessari per ogni specifica finalità del trattamento, tenendo conto dell'effettivo contenuto informativo da fornire (provv. 16 giugno 2022, n. 230, doc. web n. 9790035).

Altro parere richiesto dall'AgID ha riguardato lo schema di regole tecniche per la gestione delle sessioni di autenticazione e *single sign-on* con riferimento al Punto di accesso telematico (Pat) di cui all'art. 64-*bis*, d.lgs. 7 marzo 2005, n. 82 (la cui adozione è prevista dalle linee guida sul punto di accesso telematico ai servizi della p.a., emanate con determinazione AgID 8 novembre 2021, n. 598, su cui il Garante si è espresso con provv. 1° novembre 2021, n. 394, doc. web n. 9714315), che individua le modalità operative con cui il Pat assicura l'identificazione e l'autenticazione degli utenti finali dei servizi in rete resi disponibili dal Pat (dipendente dallo stato delle identità rilasciate agli stessi utenti in Spid) e la realizzazione del meccanismo di *single sign-on* tra il Pat e i servizi in rete resi disponibili dai soggetti erogatori per dare inizio a specifici flussi o azioni dispositive integrate nell'esperienza dell'utente all'interno del Pat. Pur tenendo conto di alcune indicazioni fornite dall'Autorità, lo schema ha mantenuto profili di criticità rispetto ai quali il parere contiene condizioni ed osservazioni. Preliminarmente, e come già rilevato nel parere reso sulle citate linee guida sul Pat, considerato che sono effettuati trattamenti su larga scala, con dati personali appartenenti anche a categorie particolari o relativi a condanne penali e reati, potenzialmente relativi all'intera popolazione italiana, il Garante ha evidenziato che l'introduzione di nuove modalità di gestione delle sessioni di autenticazione, anche di lunga durata, e dei meccanismi di *single sign-on* per l'accesso ai servizi erogati mediante il Pat deve essere accompagnata da una rigorosa valutazione d'impatto sulla protezione dei dati personali predisposta dal gestore del Pat e successivamente esaminata dall'Autorità. Ha inoltre ritenuto che adeguate garanzie devono essere individuate anche a valle delle autonome valutazioni d'impatto che ciascun IdP Spid dovrà svolgere.

Gestione delle sessioni di autenticazione e *single sign-on*

Con specifico riguardo alla durata delle sessioni di autenticazione – lo schema prevede l'utilizzo di *Access Token* con *time-to-live* pari al massimo a 12 ore e *Refresh Token* con *time-to-live* pari al massimo a 270 giorni – il parere ha tra l'altro osservato che occorre valutarne attentamente la compatibilità con gli obblighi di sicurezza gravanti sugli IdP, in relazione ai rischi di accesso non autorizzato ai dati personali e, più in generale, di compromissione dell'integrità, della disponibilità e della resilienza

dei sistemi e dei servizi di trattamento, per l'assenza di un limite alla validità temporale della sessione di autenticazione. Si rende pertanto necessaria, prima di determinare i periodi temporali di validità dei predetti *Token* un'adeguata valutazione – che sarà acquisita dall'Autorità – dei rischi connessi al complesso dei trattamenti posti in essere dal gestore del Pat, dagli IdP e, in caso di utilizzo dei meccanismi di *single sign-on*, dai soggetti erogatori. Altre condizioni e osservazioni sono state previste in relazione ad altri profili, quali il *single sign-on* con i servizi dei soggetti erogatori e la tracciatura delle transazioni (provv. 21 luglio 2022, n. 271, doc. web n. 9808982).

CieId

Il Garante è stato chiamato a pronunciarsi, ai sensi dell'articolo 66 del Cad, sullo schema di decreto del Ministro dell'interno, di concerto con i Ministri dell'economia e delle finanze e per l'innovazione tecnologica e la transizione digitale, concernente le modalità di impiego della carta d'identità elettronica (Cie). Tale schema contiene, in particolare, disposizioni concernenti la gestione dell'identità digitale rilasciata al cittadino associata alla Cie medesima (CieId) – analogamente a quanto consentito con l'identità digitale Spid (cfr. art. 64, comma 2-*quater*, del Cad) – per l'accesso ai servizi erogati in rete dalle p.a. e dai privati (i cd. fornitori di servizi), con tre diversi livelli di sicurezza di autenticazione informatica.

Lo schema recepisce le indicazioni fornite dall'Ufficio, volte ad applicare al sistema CieId le misure già previste per il sistema Spid, quali in particolare quelle concernenti: l'individuazione dei dati personali raccolti al momento dell'attivazione delle credenziali, nonché la fonte di provenienza e la previsione di flussi, verso i fornitori dei servizi e nel processo di autenticazione informatica, che limitino la richiesta dei dati al minimo necessario per l'erogazione di ciascun servizio in rete; l'individuazione delle finalità per le quali viene assicurata l'integrazione con l'Anpr; la definizione delle misure a garanzia della gestione, conservazione, limitazione della finalità e accessibilità dei registri degli accessi; la previsione di compiti di monitoraggio in capo al Ministero dell'interno nonché degli obblighi di notifica al Garante delle violazioni dei dati personali; la puntuale definizione dei ruoli e dei compiti di tutti i soggetti a vario titolo coinvolti nei trattamenti; l'effettuazione della valutazione di impatto sulla protezione dei dati, ai sensi dell'art. 35 del RGPD, da parte del Ministero dell'interno, quale titolare del trattamento.

Considerato che lo schema consente al cittadino maggiorenne, di conferire o negare il consenso alla donazione di organi in caso di morte anche attraverso il portale dell'identità del cittadino, il parere favorevole ha posto la condizione che, prima dell'avvio del trattamento, il Ministero dell'interno acquisisca apposita conferma dal Ministero della salute per assicurare il pieno coordinamento con la normativa in materia di prelievi e di trapianti di organi e di tessuti. Inoltre, con riferimento al trattamento dell'IdAnpr riferito a ciascun cittadino (associato alla CieId in fase di attivazione delle credenziali di autenticazione informatica), l'Autorità si è riservata di effettuare specifiche valutazioni all'esito dell'esame degli schemi di provvedimenti attuativi dell'art. 62, comma 6-*bis*, del Cad, mentre, i servizi messi a disposizione dal Ministero per l'utilizzo del NIS – in relazione ai quali le modalità e i requisiti di accesso saranno disciplinati da un separato atto del Ministero dell'interno, sentito il Garante – potranno essere attivati solamente in presenza di apposita e idonea base giuridica che funga da presupposto e determini le finalità, le tipologie di dati personali oggetto di trattamento e le operazioni eseguibili (provv. 7 luglio 2022, n. 247, doc. web n. 9803398).

Sistema di gestione deleghe

Tramite il Sistema di gestione deleghe (Sgd), previsto dall'articolo 64-*ter*, comma 7, d.lgs. 7 marzo 2005, n. 82 (Cad), un soggetto può delegarne un altro, in possesso dell'identità digitale di cui all'art. 64 del Cad, a richiedere, in nome e per suo conto, l'erogazione dei servizi *online*, individuati nella delega, offerti dai fornitori di servizi

aderenti al Sgd; anche a tutori, curatori e amministratori di sostegno, nonché a soggetti esercenti la responsabilità genitoriale, viene consentito di esercitare, tramite il Sgd, i poteri loro attribuiti. In relazione al Sgd il Garante è stato chiamato a esprimersi sia sullo schema di decreto del Ministro per l'innovazione tecnologica e la transizione digitale che sullo schema di manuale operativo e sulla valutazione d'impatto (su questi ultimi due congiuntamente).

Il parere sullo schema di decreto è stato molto articolato. Anzitutto è stato rilevato che l'introduzione del Sgd, come configurato in tale schema, ha per effetto quello di sovrascrivere e travolgere il sistema normativo vigente in materia considerandolo assorbito in quello tecnologico. Ciò, sul versante della protezione dei dati personali, si traduce in un *vulnus* insanabile per effetto del quale anche soggetti privi dei necessari poteri – per non averli mai acquisiti in conformità alle vigenti disposizioni di legge – si ritroverebbero a poter trattare dati personali del delegante in forza della semplice esibizione di una copia digitale di un documento di identità e di una delega. Inoltre, diversamente da quanto previsto dal richiamato art. 64-*ter* del Cad, il ruolo di titolare del trattamento viene riconosciuto all'Istituto Poligrafico e Zecca dello Stato anziché alla struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale. Ciò posto, il sistema delle deleghe così configurato comporta rischi elevati per i diritti e le libertà fondamentali degli interessati, poiché espone il delegante, in caso di utilizzi impropri, a possibili trattamenti illeciti o non autorizzati mediante lo strumento della delega, in relazione alla consultazione di dati personali (anche sanitari o bancari) ovvero ad operazioni con significativi effetti sulla sfera giuridica (ad es., azioni di carattere dispositivo, anche patrimoniali, o la richiesta di benefici o agevolazioni di vario genere), favorendo altresì la possibilità di comportamenti fraudolenti a danno della finanza pubblica.

In ragione di ciò, il parere ha prescritto, tra le altre cose, di espungere la possibilità di conferire la delega semplice a professionisti iscritti a ordini, albi o collegi e alle persone giuridiche dotate di specifiche autorizzazioni previste dalla legge nell'ambito dell'attività svolta professionalmente o istituzionalmente, in considerazione del fatto che, nello schema, non sono state rinvenute misure adeguate ad affrontare i rilevanti rischi connessi. Inoltre l'Autorità ha chiesto che fossero individuate adeguate misure volte ad assicurare la delimitazione dell'operatività della delega in conformità ai poteri attribuiti a tutori, curatori e amministratori di sostegno, nonché a mitigare i rischi di accessi abusivi o non autorizzati ai servizi in caso di revoca della tutela, della curatela o dell'amministrazione di sostegno (ovvero di rimozione o sostituzione dei predetti soggetti), di eventuale decadenza o sospensione della responsabilità genitoriale (provv. 24 febbraio 2022, n. 74, doc. web n. 9752853).

A seguito del predetto parere, è stato adottato il decreto 30 marzo 2022, che, tuttavia, mantiene talune criticità rilevate dal Garante, e le soluzioni individuate in relazione ad alcune di esse non risultano adeguate a superare i rilievi mossi sul piano della conformità alla disciplina in materia di protezione dei dati personali. Tali criticità si riflettono anche sul manuale operativo e sulla valutazione d'impatto successivamente sottoposti all'esame dell'Autorità e sui quali è stato conseguentemente espresso parere negativo. Inoltre, con tale ultimo provvedimento, il Garante ha avvertito il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri che i trattamenti di dati personali nell'ambito del Sgd, come configurati nel decreto e negli atti conseguenti, potrebbero violare i principi di liceità, correttezza e trasparenza, di minimizzazione, di integrità e riservatezza, di *accountability* e di *privacy by design* e *by default*, nonché gli obblighi di sicurezza, in considerazione dei rischi derivanti da possibili accessi non autorizzati, non adeguatamente valutati e gestiti (provv. 6 ottobre 2022, n. 330, doc. web n. 9823221).

Piattaforma dei benefici economici erogati da soggetti pubblici

Il Ministro per l'innovazione tecnologica e la transizione digitale ha sottoposto all'Autorità uno schema di decreto che disciplina un complesso di trattamenti attraverso cui assicurare l'erogazione con modalità uniformi di benefici economici – destinati a specifici acquisti da effettuare attraverso terminali di pagamento fisici o virtuali ed erogati dalle p.a. che aderiscono al progetto – con l'obiettivo di digitalizzare i pagamenti e consentire un più efficiente controllo della spesa pubblica, semplificando l'accesso alle diverse iniziative da parte dei cittadini. Il Garante ha osservato preliminarmente che i trattamenti effettuati tramite la predetta piattaforma presentano rischi elevati per i diritti e le libertà degli interessati derivanti dalla raccolta massiva e generalizzata di informazioni di dettaglio, riferibili agli strumenti di pagamento (numero di carta di credito, ecc.) e ai conti correnti (Iban) in uso agli utenti fruitori (spesso soggetti vulnerabili), nonché ad ogni aspetto della vita quotidiana dell'intera popolazione sulla base degli acquisti effettuati, nonché derivanti da accesi non autorizzati e utilizzi impropri. Il parere ha posto una serie di condizioni e osservazioni concernenti, in particolare: la trasmissione al gestore, da parte degli esercenti dei soli dati relativi alle transazioni di cui l'utente intende avvalersi per l'erogazione dei benefici economici connessi a iniziative a cui lo stesso ha aderito, introducendo misure volte a escludere la trasmissione delle informazioni relative a transazioni che non risultino utili a tal fine; la raccolta dei dati relativi al codice categoria dei beni acquistati; le verifiche sulla titolarità dei conti correnti e sull'intestazione degli strumenti di pagamento, tenendo in considerazione anche i casi in cui gli utenti potrebbero operare sulla piattaforma in favore di terzi beneficiari; l'utilizzo di Spid, Cie, *app* IO, e tessera sanitaria quali strumenti di acquisto; la tutela delle informazioni relative agli strumenti di pagamento e alle transazioni commerciali per assicurare che siano trattate solo per le finalità di erogazione dei benefici e non siano oggetto di utilizzi impropri o accessi non autorizzati (provv. 28 luglio 2022, n. 286, doc. web n. 9809029).

Siti web delle p.a.

Il Garante ha espresso parere favorevole sullo schema di linee guida di *design* per i siti internet e i servizi digitali della p.a., predisposto dall'AgID, ai sensi degli artt. 53, comma 1-*ter*, e 71, d.lgs. 7 marzo 2005, n. 82. Il Garante ha tuttavia ritenuto necessarie alcune integrazioni al testo, con particolare riguardo alla necessità di effettuare una valutazione d'impatto sulla protezione dei dati in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche; di fornire agli interessati informazioni concise, trasparenti, intelligibili; di impiegare eventuali *cookie* o altri strumenti di tracciamento in maniera trasparente, solo nei casi in cui ciò si renda necessario, nel rispetto delle indicazioni fornite dal Garante con le linee guida *cookie* e altri strumenti di tracciamento (cfr. provv. 10 giugno 2021, n. 231, doc. web n. 9677876), assicurando, in ogni caso, la piena fruibilità del sito o del servizio digitale anche quando l'utente non intende prestare il proprio consenso all'archiviazione di informazioni sul proprio dispositivo o all'accesso alle informazioni ivi archiviate; di rispettare le regole per il trasferimento dei dati personali nei Paesi terzi ove sono stabiliti eventuali fornitori di servizi di *hosting* o *cloud computing* (provv. 24 febbraio 2022, n. 76, doc. web n. 9753209).

Censimento linguistico

La Provincia di Bolzano ha richiesto il parere dell'Autorità in merito allo schema di regolamento d'esecuzione in materia di censimento linguistico, attuativo dell'art. 18, comma 2, d.P.R. 26 luglio 1976, n. 752 (su cui l'Autorità aveva espresso il proprio parere con provv. 29 ottobre 2020, n. 199, doc. web n. 9487448) che ha introdotto la possibilità di effettuare la rilevazione dei dati anche in via telematica. Fino ad oggi, infatti, il censimento si è svolto esclusivamente in modalità cartacea.

Lo schema ha individuato una procedura per garantire, anche in caso di rileva-

zione telematica, l'anonimizzazione del dato relativo all'appartenenza/aggregazione al gruppo linguistico dell'interessato, in modo tale da impedirne la re-identificazione. In particolare, anche tenendo conto delle indicazioni fornite dall'Ufficio, è stato previsto che il trattamento dei dati personali per le finalità statistiche proprie del censimento linguistico venga suddiviso in due fasi, ognuna riconducibile a un distinto e autonomo titolare del trattamento (ossia i comuni – in qualità di titolari del trattamento relativo ai dati personali necessari all'identificazione dei soggetti interessati – e l'Astat, ufficio di statistica della Provincia di Bolzano – titolare del trattamento dei dati relativi all'espressione dell'appartenenza o dell'aggregazione dei soggetti interessati a uno dei tre gruppi linguistici), con distinti sistemi informatici, per separare il dato relativo all'appartenenza o all'aggregazione al gruppo linguistico da ogni riferimento relativo all'identità dei soggetti interessati. L'Autorità ha espresso parere favorevole sullo schema, riservandosi di esaminare la valutazione d'impatto che sarà trasmessa, allo scopo di verificare l'adeguatezza delle misure in concreto adottate in ogni fase del trattamento per garantire, in particolare, l'anonimizzazione dei dati relativi all'appartenenza/aggregazione al gruppo linguistico e la non re-identificazione degli interessati (provv. 6 ottobre 2022, n. 318, doc. web n. 9825838).

Cloud in ambito pubblico

È stata altresì avviata la prima azione coordinata nell'ambito del *Cooperation Enforcement Framework* (CEF) – promossa dal Cepd, a cui hanno partecipato le autorità di protezione dati europee, tra cui il Garante – che ha riguardato l'utilizzo dei servizi *cloud* da parte dei soggetti pubblici. L'indagine è stata complessivamente svolta mediante la somministrazione di un apposito questionario nei confronti di circa 100 soggetti operanti nel settore pubblico in tutta Europa, attivi in vari settori, incluse le Istituzioni europee, le centrali di committenza e i fornitori di servizi Ict della pubblica amministrazione centrale e locale.

All'esito di questa attività di raccolta di informazioni e di analisi (che l'Autorità ha svolto anche mediante accertamenti di carattere ispettivo) è in via di elaborazione, in seno al Comitato, un *report* finale (che sarà pubblicato sul sito del Comitato stesso), cui saranno allegati i *report* nazionali elaborati da ciascuna autorità (compreso il Garante) sulla base di un modello comune, nella consapevolezza della necessità di procedere con azioni coordinate e condivise.

4.9. *La materia anagrafica ed elettorale*

Codice identificativo univoco in Anpr (Id-Anpr)

Il Ministero dell'interno ha chiesto il parere dell'Autorità sullo schema di decreto recante modalità di attribuzione da parte di Anpr di un codice identificativo univoco per garantire la circolarità dei dati anagrafici e l'interoperabilità con le altre banche dati delle p.a. e dei gestori di servizi pubblici di cui all'art. 2, comma 2, lett. *a*) e *b*), del Cad, da adottarsi ai sensi dell'art. 62, comma 6-*bis*, d.lgs. 7 marzo 2005, n. 82. Nell'ambito dello schema, sono state disciplinate le modalità per l'adeguamento e l'evoluzione delle caratteristiche tecniche della piattaforma di funzionamento dell'Anpr per l'attribuzione a ciascun cittadino del codice identificativo univoco (Id-Anpr), previsto dall'art. 62, comma 3, ultimo periodo, del Cad, al fine di garantire l'interoperabilità della stessa con le altre banche dati delle p.a. e dei gestori di pubblici servizi. Lo schema esaminato ha sostanzialmente tenuto conto delle indicazioni fornite dall'Ufficio e non ha presentato, nel suo complesso, rilevanti criticità. Nel parere, tuttavia, è stato chiesto di inserire, in particolare, un riferimento esplicito all'interoperabilità di Anpr con le altre banche dati pubbliche (provv. 15 dicembre 2022, n. 414, doc. web n. 9852231).

Anpr e Archivio nazionale informatizzato dei registri dello stato civile

Il Ministero dell'interno ha altresì richiesto il parere del Garante sullo schema di decreto ai sensi dell'art. 62, comma 6-*bis*, d.lgs. 7 marzo 2005, n. 82, recante modalità di aggiornamento della piattaforma di funzionamento dell'Anpr per l'erogazione dei servizi resi disponibili ai comuni per l'utilizzo dell'Archivio nazionale informatizzato dei registri dello stato civile. Lo schema è risultato complessivamente conforme alla normativa in materia di protezione dei dati personali. Tuttavia, anche sulla scorta dei precedenti su cui si è già espresso il Garante (cfr. provv. 14 ottobre 2021, n. 367, doc. web n. 9717543), sono state formulate alcune condizioni concernenti, in particolare, l'utilizzo dell'identità Spid ad uso professionale, i tempi di conservazione dei *log* di accesso dei cittadini all'Archivio e le misure volte a garantire il rispetto del principio di esattezza dei dati, di cui all'art. 5, par. 1, lett. *d*), del RGPD. Inoltre, considerato che il trattamento in esame presenta un rischio elevato per i diritti e le libertà degli interessati, è stata evidenziata la necessità di effettuare la valutazione d'impatto prima di procedere al trattamento (provv. 15 settembre 2022, n. 298, doc. web n. 9815094).

Anpr e liste elettorali

Il Ministero dell'interno ha richiesto il parere del Garante sullo schema di decreto, da adottarsi di concerto con il Ministro per l'innovazione tecnologica e la transizione digitale e il Ministro per la p.a., ai sensi dell'art. 62, comma 6-*bis*, d.lgs. 7 marzo 2005, n. 82, concernente le modalità di integrazione nell'Anpr delle liste elettorali e dei dati relativi all'iscrizione nelle liste di sezione di cui al d.P.R. 20 marzo 1967, n. 223 (recante il t.u. delle leggi per la disciplina dell'elettorato attivo e per la tenuta e la revisione delle liste elettorali). Lo schema di decreto ha anche definito i servizi resi disponibili agli uffici elettorali dei comuni per la tenuta e l'aggiornamento delle liste elettorali, che restano disciplinate dal predetto d.P.R. In tale contesto, è stato rilevato che tali trattamenti presentano un rischio elevato per i diritti e le libertà degli interessati, poiché riguardano diverse categorie di dati personali, ivi inclusi quelli relativi a condanne penali e reati (art. 10 del RGPD) – tale dovendo considerarsi anche la mera informazione sulla non inclusione di un cittadino nelle liste elettorali, nelle fattispecie contemplate dall'art. 2, d.P.R. n. 223/1967 – riferibili ad un numero di interessati elevato rispetto alla popolazione di riferimento, sull'intero territorio nazionale. Essendo state recepite solo in parte le indicazioni fornite dall'Ufficio, l'Autorità ha ravvisato la necessità di ulteriori modifiche, anche relative ai profili della sicurezza, al fine di rendere conformi i trattamenti alla normativa in materia di protezione dei dati personali (provv. 21 luglio 2022, n. 252, doc. web n. 9805346).

Piattaforma *referendum*

Il Ministero per l'innovazione tecnologica e la transizione digitale ha chiesto il parere del Garante sullo schema di decreto, da adottarsi di concerto con il Ministro della giustizia, ai sensi dell'art. 1, comma 343, l. 30 dicembre 2020, n. 178, che disciplina la piattaforma per la raccolta *online* delle firme per i *referendum* previsti dagli artt. 75 e 138 della Costituzione, nonché per i progetti di legge previsti dall'art. 71, secondo comma, della Costituzione. In tale contesto, sono state evidenziate notevoli criticità, tra cui, in primo luogo, l'assenza di un'adeguata valutazione degli specifici rischi per i diritti e le libertà costituzionali degli interessati, atteso che la titolarità della piattaforma sarebbe stata affidata in gestione ad un soggetto terzo, ancora da individuare, cui sarebbe stato rimesso l'intero sviluppo tecnologico dell'infrastruttura stessa. Inoltre, è stato rimarcato che i dati dei sottoscrittori di una proposta referendaria o di progetto di legge rivelano – ancor più del dato relativo alla partecipazione alla consultazione referendaria – le opinioni o la posizione politica del sottoscrittore (v. art. 9, par. 1, del RGPD). Di conseguenza, sono state poste una serie di condizioni e osservazioni per rendere la piattaforma coerente con il sistema di garanzie posto a presidio dei diritti di partecipazione alla vita democratica (provv. 24 marzo 2022, n. 106, doc. web n. 9760791).

Il Garante ha espresso parere favorevole in ordine allo schema di decreto del Mef, di concerto con i Ministeri della salute e dell'interno, attuativo dell'art. 12, d.l. n. 34/2020, in base al quale le strutture sanitarie e i sanitari competenti inviano al Sistema TS del Mef i dati dell'avviso di decesso, del certificato necroscopico e dell'attestazione di nascita, di cui agli artt. 72, comma 3; 74, comma 2, e 30, comma 1, d.P.R. n. 396/2000, nonché della denuncia della causa di morte di cui all'art. 1, d.P.R. 10 settembre 1990, n. 285, con esonero dall'invio ai comuni di ulteriore attestazione cartacea. Il Sistema TS rende immediatamente disponibili, senza registrarli, i dati sopra indicati all'Anpr, per le finalità di cui all'art. 62, comma 6, lett. *c*), del Cad nonché all'Istat. Sono state recepite nello schema di decreto alcune delle indicazioni fornite dall'Ufficio in particolare quelle relative alla necessità di un coordinamento delle disposizioni dello schema di decreto con il citato art. 12, d.l. n. 34/2020 e con le altre disposizioni normative vigenti; la necessità di rivedere alcuni flussi documentali non indicati nel medesimo art. 12 (Inps e asl) – tra l'altro quelli dai quali sarebbero derivati effetti giuridici, inizialmente previsti verso l'Inps – per anticipare, a scopi meramente cautelativi, la sospensione dell'erogazione di prestazioni pensionistiche o di altro tipo, evitando indebiti – nonché verso le asl – prima della formazione degli atti dello stato civile, i quali presentavano criticità, anche in termini di esattezza e qualità dei dati; la necessità di limitare la funzione di "interrogazione e ricerca", il rispetto delle garanzie previste dall'ordinamento a tutela della volontà della madre di non essere nominata nella dichiarazione di nascita, previste dall'art. 30, d.P.R. n. 396/2000, e del conseguente limite all'accesso a tali informazioni da parte del figlio biologico (art. 28, l. n. 184/1983 e art. 93 del Codice), nonché le misure per assicurare, anche nei confronti dell'Istat, le garanzie a tutela della riservatezza della donna nel caso del cd. parto in anonimato. Da un punto di vista delle misure tecniche, la necessità di precisare, con maggior dettaglio, il sistema di reportistica per il monitoraggio dei servizi del Sistema TS, di prevedere, quale misura tecnico organizzativa, anche il *disaster recovery* dei sistemi, di adottare in tutti i casi procedure di autenticazione informatica a due o più fattori. Ciononostante, considerata la sussistenza di alcuni limitati profili di criticità, il parere è stato condizionato all'adozione di ulteriori modifiche, in particolare, l'eliminazione dal testo del riferimento alla "conservazione o memorizzazione" di tali informazioni, esclusa dall'art. 12, d.l. n. 34/2020, nonché la necessità di ancorare il perimetro soggettivo e temporale del servizio di interrogazione e ricerca alle condizioni e ai termini previsti dalla legge per la trasmissione dei documenti oggetto del decreto (provv. 26 maggio 2022, n. 193, doc. web n. 9780893).

Anpr e Sistema TS. Trasmissione informazioni su nascite e decessi

Nel corso del 2022, il Ministero dell'interno ha richiesto al Garante il parere su uno schema di decreto direttoriale con il quale è stato approvato il documento tecnico volto a consentire che i cittadini residenti all'estero iscritti nell'Anagrafe degli italiani residenti all'estero (Aire) possano richiedere l'emissione della Cie, non solo presso i consolati di competenza, ma, in analogia con i residenti in Italia, anche tramite i comuni. Considerato che la procedura disciplinata dallo schema di decreto si basava sull'infrastruttura Cie già esistente e che le misure tecniche e organizzative presentate erano già state validamente utilizzate per il rilascio ordinario della Cie, non è stato ritenuto necessario indicare ulteriori misure. Tuttavia, continuando ad indicare le figure genitoriali esclusivamente come padre e madre, e non anche come genitori, lo schema di decreto evidenziava il mancato adeguamento a quanto previsto nei pareri del Garante 31 ottobre 2018, n. 476, doc. web n. 9058965 e 25 marzo 2021, n. 160, doc. web n. 9677947. Il parere favorevole, è stato pertanto rilasciato a condizione che nel testo del documento allegato allo schema di decreto, in aggiunta e non in sostituzione alla locuzione già presente di padre e madre, fosse

Modifiche alle modalità emissione Cie

indicata quella di genitore, nella seguente forma: padre/genitore e madre/genitore (provv. 16 giugno 2022, n. 229, doc. web n. 9790002).

4.10. *Videosorveglianza in ambito pubblico*

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

Fototrappole

Un reclamante lamentava che un comune – al solo fine di testare il funzionamento di alcune cd. fototrappole per il contrasto del fenomeno dell'illecito abbandono dei rifiuti – avesse trattato i dati personali dei soggetti ripresi da queste ultime, in assenza di alcun atto organizzativo in relazione all'impiego dei predetti dispositivi e di alcuna preventiva determinazione in materia di protezione dei dati personali, omettendo di assicurare che le misure a tutela della protezione dei dati personali fossero integrate nel trattamento fin dalla sua progettazione e per impostazione predefinita durante l'intero ciclo di vita dei dati. Il comune non aveva neppure fornito agli interessati l'informativa sul trattamento dei dati personali. Il Garante ha, pertanto, ritenuto che il complessivo trattamento fosse avvenuto in violazione degli artt. 5, par. 1, lett. *a*), e par. 2 (in combinato disposto con l'art. 24), 12, par. 1, 13 e 25 del RGPD (provv. 7 aprile 2022, n. 119, doc. web n. 9773950) e applicato una sanzione pecuniaria.

In un caso simile è emerso che, prima di iniziare il trattamento, l'ente non aveva né fornito un'adeguata informativa agli interessati, né stipulato per iscritto un accordo sulla protezione dei dati con la società che, in qualità di responsabile del trattamento, gestiva il servizio di raccolta dei rifiuti (in violazione dell'art. 28 del RGPD), né redatto una valutazione di impatto sulla protezione dei dati (in violazione dell'art. 35 del RGPD). Il Garante, oltre a comminare una sanzione amministrativa pecuniaria, ha prescritto al comune di fornire un'idonea informativa agli interessati e di redigere la predetta valutazione d'impatto (provv. 28 aprile 2022, n. 162, doc. web n. 9777974). Con separato ma connesso provvedimento, è stata sanzionata anche la società gestrice del servizio di raccolta dei rifiuti, per aver pubblicato nel proprio profilo Facebook video e immagini, ottenuti mediante i dispositivi video in questione, che ritraevano persone identificabili. La diffusione di tali dati da parte della società è stata ritenuta incompatibile con la finalità originaria per la quale gli stessi erano stati raccolti (ovvero l'accertamento di illeciti amministrativi in materia ambientale), priva di una base giuridica, e, pertanto, non conforme ai principi di limitazione della finalità e liceità, correttezza e trasparenza, con conseguente violazione degli artt. 5, par. 1, lett. *a*) e *b*), 5, e 6 del RGPD, nonché 2-*ter* del Codice (nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139). È stata, altresì, accertata la mancata stipula per iscritto di un accordo sulla protezione dei dati sia con il titolare del trattamento, ovvero il comune, sia con l'azienda fornitrice, che agiva in qualità di sub-responsabile del trattamento, sebbene in assenza di autorizzazione da parte del titolare, in violazione dell'art. 28 del RGPD (provv. 28 aprile 2022, n. 163, doc. web n. 9777996) (cfr. par. 4.6).

In un altro caso, sempre relativo all'impiego di cd. fototrappole per il contrasto del fenomeno dell'illecito abbandono dei rifiuti, un comune aveva fornito agli interessati un'inidonea informativa sul trattamento dei dati personali "di primo livello" e aveva

del tutto omesso di fornire agli stessi un'informativa completa "di secondo livello" agendo in maniera non conforme al principio di liceità, correttezza e trasparenza. Inoltre, contravvenendo a quanto richiesto dai principi di responsabilizzazione e limitazione della conservazione, il comune non aveva fissato i tempi massimi di conservazione delle immagini per ciascuna finalità di trattamento perseguita. Il Garante ha conseguentemente accertato la violazione degli artt. 5, par. 1, lett. *a*) ed *e*), e par. 2 (in combinato disposto con l'art. 24), 12 e 13 del RGPD (provv. 9 giugno 2022, n. 214, doc. web n. 9794895).

Il Garante ha poi adottato un provvedimento prescrittivo e sanzionatorio nei confronti di un comune, che aveva utilizzato una telecamera di videosorveglianza, installata sulla pubblica via per la tutela della cd. sicurezza urbana (cfr. art. 5, comma 2, lett. *a*), d.l. 20 febbraio 2017, n. 14), per una finalità – ovvero la contestazione di una violazione amministrativa della normativa emergenziale in materia di contenimento della diffusione del virus Sars-CoV-2 – che non poteva ritenersi compatibile con quella originaria, risultando il trattamento non conforme al principio di limitazione della finalità e in assenza di una base giuridica. È, inoltre, emerso che il comune non aveva redatto il registro delle attività di trattamento e aveva fornito agli interessati un'inadeguata informativa di primo livello, aveva omesso di fornire agli stessi un'informativa completa, di secondo livello, né aveva fissato tempi certi di conservazione delle immagini. Il comune aveva, altresì, subordinato l'esercizio del diritto di accesso alle immagini di videosorveglianza al pagamento di cospicua somma. Il Garante ha pertanto comminato al comune una sanzione amministrativa pecuniaria e prescritto di fornire gratuitamente riscontro all'istanza di accesso dell'interessato (provv. 20 ottobre 2022, n. 341, doc. web n. 9831369).

5 La sanità

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

Nel 2022 è cessato lo stato di emergenza, ma le disposizioni introdotte per disciplinare il trattamento dei dati in tale ambito sono rimaste in vigore sino al 31 dicembre 2022 (cfr. art. 10, d.l. 24 marzo 2022, n. 24).

In tale contesto, il Garante ha espresso numerosi pareri sulle disposizioni normative che hanno introdotto strumenti e prescrizioni volte a contenere il diffondersi del Covid-19, verificando la presenza di misure di garanzia appropriate e specifiche per proteggere i diritti fondamentali e gli interessi delle persone fisiche.

Certificazioni concernenti l'esenzione dalla vaccinazione anti Covid-19

Un particolare ambito di intervento ha riguardato le certificazioni mediche che attestano una condizione temporanea o definitiva di esenzione alla vaccinazione anti Covid-19, con riferimento alle quali l'Autorità, nell'immediatezza della relativa previsione normativa, ha evidenziato al Ministero della salute che, alla luce dei principi di correttezza del trattamento, di minimizzazione e di integrità e riservatezza dei dati, era necessario introdurre uno strumento digitale analogo alle certificazioni verdi che attestasse la predetta esenzione, in quanto la presentazione di un documento cartaceo avrebbe inevitabilmente rivelato a terzi la sussistenza di una condizione di salute dell'interessato che gli impediva, in via temporanea o definitiva, di sottoporsi alla predetta vaccinazione (cfr. provv.ti 11 ottobre 2021, n. 363, doc. web n. 9707431 e 13 dicembre 2021, n. 430, doc. web n. 9727220).

Con parere 27 gennaio 2022, n. 18, sullo schema di d.P.C.M. adottato di concerto con il Ministro della salute, il Ministro per l'innovazione tecnologica e la transizione digitale e il Mef, ai sensi dall'art. 9-*bis*, comma 3, d.l. 22 aprile 2021, n. 52, l'Autorità ha preso atto che lo schema di decreto sottoposto alla sua attenzione era stato elaborato tenendo conto delle predette sollecitazioni e indicazioni (doc. web n. 9742129).

In particolare, l'Autorità ha rilevato che, come dalla stessa suggerito, nella facciata delle certificazioni di esenzione – che include il QR *code* – sono riportati i medesimi dati presenti nelle certificazioni verdi Covid-19 (nome e cognome, data di nascita e identificativo univoco) e che gli ulteriori dati di dettaglio sono riportati nelle facciate interne della stessa, al fine di garantire che il soggetto deputato al controllo della certificazione digitale di esenzione non venga a conoscenza della condizione di salute alla base della quale è stata emessa la certificazione di esenzione. Come richiesto dall'Autorità inoltre è stato previsto per la facciata esterna delle certificazioni di esenzione lo stesso *layout* grafico di quella delle certificazioni verdi Covid-19, al fine di assicurare che il verificatore non possa distinguere se si tratta di certificazione di esenzione o di certificazione verde per avvenuta vaccinazione o guarigione o esito negativo di test anti Covid-19.

Verifica del rispetto dell'obbligo vaccinale

Ulteriore parere in tema di certificazioni verdi è stato espresso con riferimento ai trattamenti di dati personali finalizzati alla verifica del rispetto dell'obbligo vaccinale ai fini dell'irrogazione delle previste sanzioni amministrative pecuniarie. Con parere 18 febbraio 2022, n. 57, il Garante ha preso atto che il Ministero della salute nel disciplinare i suddetti trattamenti ha accolto le osservazioni formulate dall'Autorità nell'ambito dell'istruttoria, introducendo specifiche misure di garanzia

idonee a tutelare i diritti fondamentali e gli interessi delle persone fisiche (doc. web n. 9746905).

In particolare, in tale parere l'Autorità ha ritenuto che le criticità evidenziate il 10 febbraio 2022 dal Presidente in audizione alla Camera (Commissione XII Affari sociali, cfr. par. 3.1.1), nell'ambito dell'esame del disegno di legge di conversione in legge del d.l. n. 1/2022, sono state superate (doc. web n. 9744445). In tale contesto, il Presidente ha infatti evidenziato la necessità di garantire idonee misure a protezione dei diritti fondamentali degli interessati come quella di assicurare che l'Agenzia delle entrate-Riscossione (AdER) non conosca le ragioni dell'esenzione alla vaccinazione, ritenendo "opportuno escludere espressamente che l'attestazione dell'asl all'AdER contenga informazioni idonee a rivelare lo stato di salute dell'interessato e, in senso più ampio, dati ulteriori rispetto alla sola insussistenza dell'obbligo vaccinale o all'impossibilità di adempiervi". Con specifico riferimento al ruolo dell'AdER nel predetto procedimento sanzionatorio, il Presidente, pur riconoscendo "le peculiarità del procedimento sanzionatorio in questione che – derogando alla legge n. 689, sottende una significativa concentrazione delle sue varie fasi", ha ricordato che non si può legittimare "l'attribuzione ad AdER di competenze ulteriori rispetto a quelle, di natura essenzialmente riscossiva, da esercitarsi a partire dalla notifica dell'avviso di addebito".

È stato infatti accolto l'invito a prevedere che le asl, competenti per territorio, adottino misure tecniche e organizzative idonee ad assicurare l'integrità e la riservatezza dei dati contenuti nelle comunicazioni che il destinatario dell'avvio del procedimento sanzionatorio, deve effettuare per documentare l'eventuale certificazione relativa al differimento o all'esenzione dall'obbligo vaccinale, ovvero altra ragione di assoluta e oggettiva impossibilità.

È stato accolto anche l'invito dell'Ufficio a prevedere che i destinatari dell'avvio del procedimento sanzionatorio diano notizia all'AdER della sola avvenuta presentazione della predetta comunicazione all'asl competente con modalità idonee ad assicurare il rispetto del principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. *c*), del RGPD.

Sono state altresì previste misure adeguate ad assicurare che la comunicazione telematica tra l'asl e l'AdER circa l'eventuale attestazione relativa all'insussistenza dell'obbligo vaccinale o all'impossibilità di adempiervi avvenga nel rispetto del principio di integrità e riservatezza (art. 5, par. 1, lett. *f*), del RGPD).

Analogamente, è stato previsto che la comunicazione trasmessa al Ministero dall'AdER indichi esclusivamente l'insussistenza dell'obbligo vaccinale o l'impossibilità di adempiervi, senza contenere informazioni idonee a rivelare lo stato di salute dell'interessato.

App Immuni

Con riferimento all'*app* Immuni, è stato reso parere sullo schema di decreto del Ministro della salute relativo all'organizzazione e al funzionamento del servizio telefonico di supporto per gli utenti dell'*app*, alla luce della cessazione dello stato di emergenza sanitaria. In tale parere il Garante ha preso atto delle misure tecniche e organizzative introdotte anche a seguito delle interlocuzioni informali tra gli uffici che hanno portato all'individuazione di precisi termini di conservazione dei diversi dati trattati, a garantire la trasparenza delle informazioni da fornire agli interessati, nonché all'individuazione delle modalità di comunicazione dei referti dei test Covid-19 all'interessato in conformità alla specifica disciplina di settore (provv. 28 aprile 2022, n. 142, doc. web n. 9775888).

Con il provvedimento 24 novembre 2022, n. 386, di autorizzazione ai sensi dell'art. 36 del RGPD, l'Autorità ha preso atto della necessità di adeguare la valutazione d'impatto all'evoluzione della disciplina legata alla gestione della

5

pandemia da Covid-19 e alle connesse misure per mitigare i rischi per i diritti e le libertà degli interessati connessi a tali trattamenti di dati personali svolti per l'esecuzione di compiti di interesse pubblico (doc. web n. 9837022).

Sempre in tema di Covid-19 esaminando i numerosissimi reclami e segnalazioni relativi al trattamento dei dati personali nel contesto emergenziale, l'Ufficio ha evidenziato che gli interventi emergenziali 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 RGPD per il perseguimento di motivi di interesse pubblico nel settore della sanità pubblica (cfr. art. 9, par. 2, lett. *i*), del RGPD), e che resta ovviamente fermo che il trattamento dei dati personali connesso alla gestione della predetta emergenza sanitaria deve svolgersi nel rispetto della disciplina vigente in materia di protezione dei dati personali e, in particolare, dei principi e dei limiti applicabili al trattamento, di cui all'art. 5 del RGPD.

Tra i provvedimenti adottati dal Garante a seguito delle attività istruttorie avviate d'ufficio o a seguito di reclami o di segnalazioni merita evidenziare i seguenti.

Con provvedimento 27 gennaio 2022, n. 34 (doc. web n. 9746448) è stata sanzionata un'azienda sanitaria che aveva previsto la possibilità di prenotare prestazioni sanitarie legate al Covid-19 sul sito internet istituzionale non garantendo un protocollo di comunicazione sicura tra la stessa e gli utenti (http in luogo di https). Inoltre i dati degli utenti che accedevano al servizio erano indicizzati e liberamente rintracciabili in rete con l'ausilio di comuni motori di ricerca a causa dell'assenza di un sistema di autenticazione informatica che avrebbe dovuto limitare l'accesso ai soli soggetti autorizzati.

A seguito di una segnalazione il Garante ha adottato un provvedimento sanzionatorio nei confronti di un policlinico romano che consentiva l'accesso agli ambulatori solo a coloro che fossero in possesso di una certificazione verde (provv. 20 ottobre 2022, n. 356, doc. web n. 9827446). Nel ricostruire i vari interventi normativi sul tema e i relativi pareri rilasciati dall'Autorità, è stato rappresentato che la limitazione delle libertà personali effettuata attraverso il trattamento di dati sulla salute degli interessati e realizzata mediante la previsione di subordinare l'accesso a luoghi e a servizi al possesso di una certificazione attestante l'avvenuta vaccinazione o guarigione da Covid-19, o l'esito negativo di un test antigenico o molecolare, è ammissibile solo se prevista da una norma di legge statale (artt. 6, par. 2, e 9 del RGPD e artt. 2-*ter* e 2-*sexies* del Codice, cons. n. 48 del RGPD e del Consiglio sull'EU *digital* Covid certificate adottato il 14 giugno 2021; cfr. anche Corte cost., sent. n. 271/2005 sulla riserva di legge statale sulla protezione dati; Corte cost., sent. n. 37/2021).

In un altro caso il Garante ha sanzionato una società che aveva sviluppato un sistema informativo che consentiva di prenotare l'esecuzione di tamponi Covid-19 in farmacia fornendo solo il codice fiscale (provv. 20 ottobre 2022, n. 342, doc. web n. 9832507). Il Garante ha ricordato che l'uso del codice fiscale, quale unico elemento di accesso ai sistemi di prenotazione del vaccino, rende il sistema vulnerabile nei confronti di attacchi informatici volti a effettuare prenotazioni fraudolente in modo massivo, mentre inserire in fase di prenotazione un dato ulteriore rispetto al codice fiscale, quale il numero della tessera sanitaria, appare ampiamente bilanciato rispetto ai rischi di una non corretta identificazione dello stesso e di prenotazione di una dose vaccinale che non sarà poi utilizzata, trattandosi comunque di una informazione già in possesso dell'interessato proprio perché apposta sul documento (tessera sanitaria) che attesta il codice fiscale e che deve essere in ogni caso in possesso dell'interessato all'atto della somministrazione del vaccino (cfr. provv. 13 maggio 2021, n. 187, doc. web n. 9674151). Ulteriori profili di illiceità sono stati rinvenuti nell'informativa da rendere agli interessati e nella designazione del responsabile del trattamento.

5.2. *La sanità digitale*

Nei molteplici interventi relativi ai trattamenti di dati personali effettuati attraverso gli strumenti di sanità digitale è stato costantemente ribadito che non vi sono ostacoli da parte dell'Autorità all'introduzione di strumenti volti ad agevolare uno sviluppo equilibrato e sostenibile dei servizi sanitari offerti ai cittadini che tenga conto della tutela dei diritti fondamentali dell'individuo e della protezione dei dati personali, alla luce del progresso sociale e degli sviluppi scientifici e tecnologici.

5.2.1. Il Fascicolo sanitario elettronico (Fse)

L'ultimo triennio è stato caratterizzato da numerosi interventi normativi volti ad accelerare lo sviluppo degli strumenti di sanità digitale nel nostro Paese, a cui è stato dato ulteriore impulso con l'attuazione della Missione 6 (salute) del Pnrr e del connesso investimento sul potenziamento del Fse. Si sono in particolare susseguite innovazioni della disciplina del Fse, la cui attuazione è stata demandata a decreti ministeriali sui quali deve essere richiesto il parere del Garante (cfr. d.l. n. 179/2012, d.l. n. 34/2020 e art. 2-*sexies*, comma 1-*bis*, del Codice).

Il primo intervento sulle disposizioni di attuazione della nuova disciplina sul Fse si è avuto con parere 7 aprile 2022, n. 136 (doc. web n. 9773977) sullo schema di decreto del Ministro della salute e del Ministro delegato per l'innovazione tecnologica e la transizione digitale di concerto con il Mef riguardante l'integrazione dei dati essenziali che compongono i documenti del Fse. Il Garante ha preso atto che il Ministero della salute ha accolto le osservazioni formulate in ordine alla necessità che, nell'ampliare il novero dei dati presenti nei documenti accessibili attraverso il Fse, siano indicati solo atti di cui è certa la natura e l'origine con esclusione delle autocertificazioni, in quanto la disciplina di settore prevede la non sostituibilità dei certificati medici e sanitari (art. 49, d.P.R. n. 445/ 2000).

In tale provvedimento il Garante ha inoltre preso atto dell'intenzione del Ministero della salute di procedere in più fasi alla riforma delle disposizioni attuative del Fse anche alla luce del Pnrr, nelle more dell'adozione del decreto di cui all'art. 12, comma 7, d.l. 18 ottobre 2012, n. 179 che riguarderà i contenuti del Fascicolo, i limiti di responsabilità e i compiti dei soggetti che concorrono alla sua implementazione, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali, le modalità e i livelli diversificati di accesso al Fse, nonché la definizione e le relative modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dello stesso. La riforma della disciplina sulla protezione dei dati personali determinata dalla piena applicazione del RGPD e gli interventi normativi che, nel tempo, hanno modificato le disposizioni di rango primario in tema di Fse, rendono necessaria infatti un'opera di rimeditazione normativa del d.P.C.M. n. 178/2015 (recante l'attuale disciplina attuativa del Fse), che risulta ancorato ad una impostazione del Fascicolo in parte normativamente superata.

Nel predetto parere l'Autorità ha inoltre evidenziato la necessità di tenere conto dei nuovi istituti giuridici introdotti dal RGPD (es. valutazione di impatto), definendo con chiarezza il perimetro dei nuovi trattamenti di dati introdotti dai numerosi interventi normativi successivi all'adozione del menzionato d.P.C.M. n. 178/2015 e quindi in esso non contemplati (es. flussi di dati dal Sistema TS). È stato perciò ritenuto necessario che nel decreto previsto dall'art. 12, comma 7, d.l. n. 179/2012, relativo ai contenuti del Fascicolo, sia indicata chiaramente la titolarità dei trattamenti, con particolare riferimento a: il profilo sanitario sintetico, le prescrizioni farmaceutiche e specialistiche, il *dossier* farmaceutico,

5

il consenso/diniego alla donazione degli organi e dei tessuti, le prenotazioni di prestazioni sanitarie, il taccuino personale e le esenzioni. In questo modo sarà possibile precisare le responsabilità in ordine al rispetto dei principi generali e degli adempimenti in materia di protezione dei dati personali, con particolare riguardo a quelli di esattezza, aggiornamento e sicurezza, specificare ove risiedano i dati stessi e i documenti accessibili, il taccuino personale, il profilo sanitario sintetico e il *dossier* farmaceutico nonché garantire l'esercizio dei diritti da parte degli interessati.

L'Autorità ha richiamato infine l'attenzione su quanto già rilevato nell'ottobre del 2020 in merito all'alimentazione automatica del Fse – a partire dal 19 maggio 2020 – con tutti i dati delle prestazioni sanitarie effettuate in epoca antecedente a tale data, che sarebbe stata possibile solo qualora fossero rispettate, contestualmente, le seguenti due condizioni: avere provveduto a un'idonea campagna nazionale e regionale di informazione sulle novità in materia e avere riconosciuto agli interessati, dal momento in cui sono stati informati, un termine non inferiore a 30 giorni per manifestare la propria eventuale opposizione (cfr. comunicato stampa 20 gennaio 2021, doc. web n. 9516732).

Successivamente, un parere non favorevole è stato reso sullo schema di decreto di riforma della disciplina di attuazione del Fse alla luce dello specifico investimento del Pnrr (parere 22 agosto 2022, n. 294, doc. web n. 9802729).

In tale parere il Garante, ribadita la necessità di un coordinamento normativo degli strumenti di sanità digitale in fase di definizione ed effettuato un *focus* sulla natura giuridica, ancora non definita, del Fse, ha posto l'accento sulla imprescindibile definizione del perimetro di titolarità dei trattamenti e dei limiti di responsabilità dei soggetti coinvolti, auspicata nel richiamato parere del 7 aprile 2022, ma non realizzata nello schema in parola.

L'Autorità ha infatti rilevato che lo schema di decreto trasmesso non disciplina tutti gli elementi richiesti dalla normativa di settore, nonché dagli artt. 6, par. 3 e 9 del RGPD e dall'art. 2-*sexies* del Codice e, tra l'altro, che l'ambito di applicazione dello schema di decreto risulta non compiutamente definito e in contraddizione con altre disposizioni vigenti (d.P.C.M. n. 178/2015, art. 12, commi 7, 15-*bis*, 15-*ter* e 15-*septies*, d.l. n. 179/2012, art. 7, d.l. n. 34/2020, art. 2-*sexies*, comma 1-*bis*, del Codice).

Specifiche criticità sono state rilevate anche perché sono state tenute in considerazione solo in parte le osservazioni già formulate dal Garante nel 2017 con riferimento ai dati relativi alle esenzioni e alle prescrizioni specialistiche (parere 26 luglio 2017, n. 339, doc. web n. 6930323).

In particolare è stato ribadito che l'accesso al Fse in emergenza (per impossibilità fisica, incapacità di agire o incapacità di intendere o di volere o rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato), nel caso in cui l'interessato non abbia prestato il consenso al Fse deve essere limitato al Profilo sanitario sintetico (Pss), salvo che il Ministero della salute, sulla base di documentata valutazione tecnico-scientifica, dia conto al Garante, dell'esigenza di accedere all'intero Fse in quanto l'accesso al solo Pss non sia ritenuto sufficiente per apprestare le cure in emergenza. Fermo restando comunque, anche in tale ipotesi, che il personale medico, in emergenza, potrà accedere, con un criterio di gradualità, prima al Pss e, solo qualora non vi trovasse le informazioni necessarie, all'intero Fse, prevedendo, in ogni caso, nell'eventualità di emergenze sanitarie o di igiene pubblica, l'accesso a dati non direttamente identificativi del Fse da parte del Ministero della salute, degli uffici delle regioni e delle province autonome competenti in materia di prevenzione sanitaria.

Il Garante ha poi chiesto che siano indicati puntualmente i diritti esercitabili da parte dell'interessato in relazione alle diverse finalità perseguibili attraverso il Fse e alla pluralità dei soggetti deputati a raggiungerle, avendo cura di specificare le misure adottate per garantire l'esercizio del diritto di oscuramento previsto dalla normativa di settore, l'oscuramento di *default* dei dati soggetti a maggior tutela e quelle per assicurare il diritto dell'interessato di prendere visione degli accessi al suo Fse (con riferimento alla tipologia di accessi registrati dalla regione di assistenza dell'interessato e di cui lo stesso può avere visione, alle operazioni registrate, al soggetto che ha effettuato l'accesso e alla finalità dallo stesso perseguita).

Con riferimento al Pss, è stato chiesto che sia definito l'ambito di responsabilità del medico di medicina generale e dell'azienda sanitaria, con particolare riferimento alle modalità di conservazione e alle misure di sicurezza dei dati trattati anche in relazione alle distinte versioni di tale documento che possono essere redatte nel tempo. Analogamente, per i trattamenti effettuati attraverso il taccuino personale, l'Autorità ha chiesto che siano definiti i ruoli del trattamento, con particolare riferimento alla titolarità dello stesso, anche in considerazione alle operazioni di conservazione, cancellazione e trasferimento dei dati tra regioni previste nello schema di decreto.

L'Autorità ha richiesto che, con riferimento al *dossier* farmaceutico, sia definita la titolarità dei trattamenti e sia indicato ove risiedono i dati e i soggetti che possono accedervi e per quali finalità e che sia integrato il modello di informativa con tutti gli elementi richiesti dagli artt. 13 e 14 del RGPD, in relazione ai molteplici trattamenti effettuati attraverso il Fse, superando le inesattezze e le incongruenze ivi contenute rispetto a quanto previsto nella normativa primaria.

Quanto al consenso dell'interessato, è stato richiesto che siano previste distinte e autonome espressioni di volontà in relazione alle diverse finalità del trattamento, perseguite da ciascuna categoria di soggetti in conformità alla normativa primaria e avendo cura di indicare, per ognuna di esse, le conseguenze della revoca, le modalità di espressione (anche in relazione ai minori e ai soggetti sottoposti a tutela) e di alimentazione dell'anagrafe dei consensi, nonché le misure adottate per assicurare l'espressione di un consenso libero, specifico, informato, esplicito e sempre revocabile.

Ulteriori rilievi sono stati espressi con riferimento all'istituto della delega dell'interessato richiedendo una configurazione dei sistemi che assicuri che l'utenza del soggetto delegato sia collegata già ad un profilo di autorizzazione che consenta di accedere al Fascicolo del/dei delegante/i, adottando idonee misure per registrare gli accessi anche da parte del soggetto delegato, nonché determinando l'ambito di operatività della delega, il periodo di validità della stessa, il numero massimo di deleghe attribuibili ad un medesimo soggetto e quello che ogni assistito può effettuare per l'accesso al proprio Fse.

L'Autorità ha poi rappresentato la necessità di definire la titolarità per i trattamenti aventi finalità di diagnosi, cura e riabilitazione e per quelli aventi finalità di prevenzione, indicando i compiti attribuiti ai soggetti che intervengono a vario titolo, le connesse responsabilità, le modalità e i livelli diversificati di accesso. Analoghe considerazioni sono state espresse con riferimento ai trattamenti effettuati dal Ministero della salute per le varie finalità allo stesso attribuite, con riferimento ai quali è stato chiesto di indicare le misure adottate per scongiurare il rischio di re-identificazione dell'interessato e per assicurare che il trattamento avvenga esclusivamente ad opera di personale tenuto al segreto professionale.

Un ultimo importante rilievo dell'Autorità ha riguardato la necessità che la riforma del Fse sia accompagnata da una preventiva e adeguata valutazione d'impatto, da effettuare tenendo conto degli specifici rischi e dei significativi effetti che i trattamenti disciplinati dallo schema di decreto trasmesso possono avere sulla

5

sfera giuridica degli interessati in relazione all'insieme dei trattamenti che saranno posti in essere nell'ambito del nuovo sistema Fse da una pluralità di titolari che presentano rischi analoghi.

In pari data è stato espresso un ulteriore parere non favorevole al Ministero della salute su uno schema di decreto trasmesso insieme a quello sul Fse relativo alla realizzazione dell'Ecosistema dati sanitari (Eds) (parere 22 agosto 2022, n. 295, doc. web n. 9802752), evidenziando che l'Eds comporta una duplicazione dei dati e dei documenti generati per finalità di cura, costituendo una banca dati (*data repository* centrale) che acquisisce, memorizza e gestisce i dati, poi elaborati per offrire servizi agli esercenti le professioni sanitarie, al Ministero della salute, alle regioni/province autonome e allo stesso interessato.

Anche in tale parere sono state rilevate numerose criticità tra le quali la necessità che sia determinato in modo tassativo il contenuto dell'Eds, indicando quali siano i "dati trasmessi dalle strutture sanitarie e socio-sanitarie, dagli enti del Ssn e da quelli resi disponibili tramite il Sistema TS" che alimentano l'Eds, al fine di "garantire il coordinamento informatico e assicurare servizi omogenei sul territorio nazionale per il perseguimento delle finalità del Fse", assicurando che la raccolta riguardi soltanto i dati generati successivamente all'adozione dello schema di decreto di cui all'art. 12, comma 15-*quater*, d.l. n. 179/2012.

L'Autorità ha poi chiesto che siano indicati, in conformità all'art. 12, comma 15-*quater*, d.l. n. 179/2012, i soggetti tenuti all'alimentazione dell'Eds e le modalità di realizzazione di tale alimentazione. È stata poi evidenziata la necessità che siano indicati gli specifici diritti esercitabili da parte dell'interessato sui dati raccolti e generati dall'Eds in relazione ai diversi servizi erogati dall'Ecosistema e descritte le specifiche misure adottate per assicurare il rispetto dell'esercizio del diritto di oscuramento.

È stato altresì rilevato che devono essere indicati l'ambito di operatività del consenso dell'interessato e le conseguenze di un'eventuale revoca dello stesso con specifico riferimento alla raccolta, all'elaborazione dei dati e all'erogazione dei servizi da parte dell'Eds, nonché alle tipologie di servizi resi dall'Eds.

Le criticità evidenziate dal Garante hanno riguardato anche la titolarità dei trattamenti, con riferimento alla quale è stato richiesto che siano descritti i ruoli del trattamento nelle fasi di raccolta ed elaborazione dei dati trasmessi dalle strutture sanitarie e socio-sanitarie, dagli enti del Ssn e di quelli resi disponibili tramite il Sistema TS, nonché con riferimento alla richiesta dei servizi erogati dall'Eds.

In merito alla valutazione di impatto e alle misure di sicurezza relative all'Eds, l'Autorità ha infine richiesto che sia riformulata la valutazione trasmessa in versione bozza, in modo da rispettare le specifiche osservazioni formulate nel predetto parere ed in quello reso in pari data sullo schema di decreto sul Fse in considerazione dei significativi effetti che i trattamenti disciplinati dallo schema di decreto in esame possono avere sulla sfera giuridica degli interessati.

Referti HIV sul Fse

Nel 2022 l'Autorità ha ricevuto numerose segnalazioni in merito alla possibilità per l'interessato di ricevere i risultati diagnostici per l'accertamento dell'HIV sul proprio Fse. Al riguardo, in una specifica FAQ sul sito dell'Autorità è stato chiarito che la legge n. 135/90 prevede che la comunicazione dei risultati di accertamenti diagnostici diretti o indiretti per l'infezione da HIV possa essere data esclusivamente alla persona cui tali esami sono riferiti e che spetta alla struttura sanitaria individuare le modalità di intermediazione tra medico e paziente in merito al significato diagnostico dei referti. Una volta soddisfatta tale intermediazione, il referto sull'HIV, al pari di ogni altro referto, può essere reso disponibile all'interessato tramite il Fse. Resta fermo, inoltre, che il risultato del test HIV può essere reso accessibile al personale che ha in cura l'interessato solo previo consenso informato dello stesso interessato.

5.2.2. Il dossier *sanitario*

Anche nel 2022 il trattamento dei dati sanitari effettuato attraverso il *dossier* sanitario continua ad essere oggetto di numerose segnalazioni, reclami e notifiche.

Un significativo intervento in materia è stato rappresentato dai provvedimenti sanzionatori nei confronti di due aziende sanitarie della medesima regione e della società informatica regionale (provv.ti 26 maggio 2022, nn. 201, doc. web n. 9790365, e 210 doc. web n. 9777974).

Nei richiamati provvedimenti l'Autorità ha rilevato che la configurazione del *dossier* sanitario predisposta dalla predetta società per tutte le aziende sanitarie regionali consentiva al personale sanitario di accedere ad informazioni relative a qualunque paziente fisicamente presente in azienda a prescindere dall'effettivo coinvolgimento in un percorso di cura nonché ad una pluralità di casistiche preordinate relative anche a pazienti non presenti in azienda. Tale configurazione del *dossier* ha reso possibile che personale sanitario operante presso l'azienda potesse accedere al *dossier* sanitario di colleghi ovvero di interessati che non erano – all'atto dell'accesso – in cura presso gli stessi, in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. *a*) e *f*) e 9 del RGPD, nonché 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. È stato al riguardo rappresentato che, nel rispetto dei principi generali del trattamento, l'accesso deve essere infatti consentito solo al personale effettivamente coinvolto nel percorso di cura del paziente, ferma restando la possibilità per lo stesso di accedere ai *dossier* sanitari per i quali non è stato di *default* abilitato l'accesso al ricorrere di specifici eventi (es. consulto) dichiarati dallo stesso professionista sanitario all'atto dell'accesso. L'Autorità ha inoltre rilevato che la possibilità per gli operatori presenti in un istituto penitenziario di accedere ai *dossier* sanitari di tutti i pazienti dell'azienda sanitaria, e non solo a quelli dei detenuti nel predetto istituto, aveva consentito di fatto gli accessi illeciti contestati.

L'Autorità ha poi rilevato che la configurazione del *dossier* sanitario in parola non correlava la durata dell'accesso a quella del periodo di cura, né prevedeva la rilevazione di eventuali anomalie o l'utilizzo di indicatori (cd. *alert*) volti ad individuare comportamenti a rischio (es. numero degli accessi eseguiti, tipologia o ambito temporale degli stessi) e ad orientare successivi interventi di *audit*, con ciò violando i principi di integrità e riservatezza dei dati personali (artt. 5, par. 1, lett. *f*) e 32 del RGPD).

Inoltre tale configurazione consentiva l'accesso al *dossier* sanitario anche al personale della direzione sanitaria per attività di supporto ai processi organizzativi, per *critical review*, per analisi ed eventuale miglioramento dei percorsi di cura (ad es. *audit*, eventi sentinella, ecc. come previsto dalla normativa) nonché per il processo di prelievo/trapianto (ad es. attività di prelievo d'organo in donatore cadavere a garanzia del migliore processo di cura). Al riguardo, l'Autorità ha ribadito quanto già rappresentato anche nelle linee guida 2015 (doc. web n. 4084632), secondo cui, tenuto conto del diritto di oscuramento esercitabile dall'interessato ai dati accessibili mediante il *dossier* sanitario e quindi della possibile incompletezza di tale strumento informativo, il titolare deve individuare, in relazione alle diverse funzioni a cui è adibito il personale, soluzioni tecniche organizzative che consentano agli organi amministrativi della direzione sanitaria di accedere, nei limiti delle attribuzioni previste per legge, a una base informativa più completa rispetto a quella presente nel *dossier* sanitario aziendale.

Oltre a sanzionare le due aziende sanitarie, l'Autorità ha prescritto alla società informatica regionale di adottare soluzioni tecniche organizzative sul *dossier* sanitario utilizzato dalle aziende sanitarie regionali nei termini sopra riportati.

Ripetuti accessi al *dossier* sanitario aziendale

L'Autorità è intervenuta sanzionando un'azienda sanitaria a seguito di un reclamo a mezzo del quale una interessata aveva lamentato ripetuti accessi al proprio *dossier* sanitario aziendale da parte di un operatore sanitario operante presso una struttura di riabilitazione, ove la stessa aveva dichiarato di non aver mai ricevuto assistenza ed in assenza del proprio consenso (provv. 10 novembre 2022, n. 371, doc. web n. 9819792). Nel corso dell'istruttoria il Garante ha appurato che l'azienda sanitaria aveva intenzionalmente rimosso i filtri *privacy* nel sistema informativo del *dossier* sanitario aziendale, per tutte le prestazioni erogate dal marzo del 2020 al maggio del 2022, nella convinzione che tale misura avrebbe semplificato la gestione dei pazienti durante la pandemia. La rimozione dei predetti filtri aveva determinato l'attivazione del *dossier* sanitario per tutti gli assistiti della azienda, che coincidevano con quelli della regione, anche nel caso gli stessi avessero espressamente negato il consenso all'uso del *dossier* o non lo avessero mai prestato e la possibilità che il *dossier* fosse consultato, sebbene con diverse profondità di accesso, da parte di tutti gli operatori sanitari aziendali a prescindere dal loro coinvolgimento nel percorso di cura dell'interessato.

Il Garante ha rilevato che la predetta scelta aziendale non aveva riguardato solo i pazienti affetti da Covid-19, ma tutti quelli afferenti all'azienda e alle sue articolazioni e non era stata limitata alle sole prestazioni sanitarie rese in emergenza, bensì a tutte quelle erogate dall'azienda dal marzo del 2020 al maggio del 2022. La scelta operata dall'azienda aveva pertanto consentito di fatto ad una operatrice sanitaria di accedere alle informazioni relative alle prestazioni sanitarie erogate alla reclamante (sua collega) alle quali non avrebbe avuto accesso se non fosse stata disposta la rimozione dei predetti filtri *privacy*, ciò in quanto la reclamante non aveva acconsentito all'uso del *dossier* sanitario aziendale e la predetta operatrice non era stata coinvolta nel percorso di cura dell'interessata.

L'Autorità, nel sanzionare l'azienda, ha rappresentato che nessuna disposizione emergenziale avrebbe potuto sospendere l'applicazione delle disposizioni vigenti e che gli interventi legislativi adottati nel corso della pandemia hanno confermato la necessità del consenso dell'interessato anche con riferimento a peculiari trattamenti emergenziali come quello relativo alla refertazione *online* dei test per il Covid-19 o alla consultazione per finalità di cura del Fse, strumento che presenta finalità analoghe al *dossier* sanitario (cfr. art. 12, d.l. n. 179/2012 in relazione alle modifiche apportate dall'art. 11, d.l. n. 34/2020).

5.2.3. La medicina predittiva

Metodologie predittive sui fabbisogni di salute della popolazione

Il decreto-legge 19 maggio 2020, n. 34, convertito con modificazioni in legge 17 luglio 2020, n. 77, ha previsto che il Ministero della salute, nell'ambito dei compiti e delle funzioni istituzionali possa trattare, ai sensi dell'art. 2-*sexies*, comma 2, lett. *v*) del Codice, i 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, comma 1), individuati con decreto del Ministro della salute, di natura non regolamentare, previo parere del Garante (art. 7, comma 2).

Con successiva disposizione è stato previsto che il Ministero della salute, nelle more dell'adozione del richiamato decreto, può avviare le attività relative alla classificazione delle patologie croniche presenti nella popolazione italiana, limitatamente alla costruzione di modelli analitici prodromici alla realizzazione del modello predittivo del fabbisogno di salute della popolazione, garantendo che gli interessati non siano direttamente identificabili (art. 7, comma 2-*bis*, d.l. n. 34/2020, introdotto dalla legge di conversione del d.l. n. 139/2021, in vigore dall'8 dicembre 2021).

A tal fine il Ministero della salute ha istituito un gruppo interistituzionale, cui sono state invitate a partecipare anche sette regioni e una provincia autonoma (Lazio, Emilia-Romagna, Lombardia, Piemonte, Puglia, Toscana e Veneto e la Provincia autonoma di Bolzano) nonché il Garante in qualità di uditore.

In relazione all'attività svolta dal gruppo l'Ufficio ha avviato un'istruttoria preliminare culminata nell'adozione di 8 provvedimenti di ammonimento (provv. ti 24 febbraio 2022, nn. 63, 64, 65, 66, 67, 68, 69 e 70, doc. web nn. 9752177, 9752221, 9752260, 9752299, 9752410, 9752433, 9752490 e 9752524).

È emerso infatti che, su richiesta del Ministero, le Regioni e la Provincia autonoma avevano elaborato e poi aggregato un *set* di dati sulla salute di tutta la popolazione assistita regionale, attraverso l'uso di algoritmi contenenti informazioni di natura demografica (sesso ed ampie classi d'età) in assenza di un idoneo presupposto giuridico.

Tali Enti, quindi, al fine di rispondere alla richiesta del Ministero della salute, avevano effettuato l'elaborazione e la successiva aggregazione dei dati sanitari presenti nei propri sistemi informativi sanitari che detengono, *ex lege*, in qualità di titolari del trattamento, in assenza di un idoneo presupposto giuridico. Nei predetti provvedimenti il Garante ha rilevato che qualora un soggetto terzo, nel caso in esame il Ministero della salute, chieda a un titolare di effettuare operazioni di trattamento su dati personali, indicandone anche le modalità, ciò non comporta l'automatica attribuzione della titolarità in capo al richiedente, né tantomeno la perdita della titolarità da parte del soggetto che legittimamente detiene i dati. Spetta a quest'ultimo, invero, valutare la legittimità della richiesta e, in particolare, la sussistenza di una idonea base giuridica per effettuare le operazioni di trattamento richieste, tanto più che, nel caso di specie, le predette operazioni hanno riguardato dati sulla salute di tutta la popolazione regionale assistita attraverso l'uso di algoritmi.

Secondo l'Autorità il trattamento di estrazione e aggregazione dei dati è stato effettuato al di fuori delle finalità legittimamente perseguibili dai predetti Enti, tenuto anche conto che la disciplina attribuiva al solo Ministero della salute il compito di trattare i dati personali raccolti nei sistemi informativi del Ssn, per lo sviluppo di metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione.

I predetti Enti non hanno inoltre svolto alcuna valutazione di impatto in relazione alle elaborazioni di dati svolte, nonostante essa, prevedendo il trattamento di dati sulla salute riferiti ad un elevato numero di soggetti vulnerabili, fosse certamente necessaria (art. 35 del RGPD; Gruppo Art. 29, 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, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017).

Per tali ragioni il Garante, tenuto conto, in particolare, che i dati trattati risultavano pseudonimizzati e che la comunicazione al Ministero aveva avuto ad oggetto dati aggregati, con i provvedimenti del 24 febbraio 2022, ha rivolto nei confronti dei richiamati enti un formale avvertimento, ai sensi dell'art. 58, par. 2, lett. *b*), del RGPD.

In tema di medicina predittiva, nel 2022 sono state sanzionate tre aziende sanitarie, per aver effettuato in assenza di un idoneo presupposto giuridico e attraverso l'uso di algoritmi, un'attività di stratificazione della popolazione assistita, volta a classificare gli assistiti in relazione al rischio di complicanze in caso di infezione da Covid-19, per individuare per tempo i percorsi diagnostici e terapeutici più idonei (violazione degli artt. 9 e 5, par. 1 lett. *a*), del RGPD e art. 2-*sexies* del Codice) (provv.ti 15 dicembre 2022, nn. 414, 415 e 416, docc. web nn. 9844989, 9845156, 9845312).

Il trattamento era avvenuto senza fornire agli interessati le informazioni previste

5

dagli artt. 13 e 14 del RGPD (in particolare sulle modalità e finalità del trattamento) in violazione del principio di trasparenza, di cui all'art. 5, par. 1, lett. *a*), del RGPD e senza aver effettuato preliminarmente la necessaria valutazione d'impatto sulla protezione dei dati personali ai sensi dell'art. 35 del RGPD.

Come già ribadito dall'Autorità in passato, la profilazione dell'utente del servizio sanitario determinando un trattamento automatizzato di dati personali volto ad analizzare e prevedere l'evoluzione della situazione sanitaria del singolo assistito e l'eventuale correlazione con altri elementi di rischio clinico (nel caso di specie l'infezione da Sars-Cov-2), può essere effettuata solo nel rispetto di requisiti specifici e garanzie adeguate per i diritti e le libertà degli interessati (cfr. artt. 4, par. 1, n. 4; 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), ovvero sulla base di una disposizione che abbia i requisiti previsti dalla disciplina in materia di protezione dei dati personali, di cui al richiamato art. 2-*sexies*, comma 1, del Codice, assenti nel caso di specie.

Al riguardo, è stato altresì evidenziato che l'utilizzo di sistemi di medicina predittiva da parte del Ministero della salute è stato previsto dal richiamato art. 7 del cd. decreto rilancio (d.l. n. 34/2020 di cui si è riferito sopra).

In tali provvedimenti sanzionatori il Garante ha ribadito che la circostanza che un soggetto terzo, nel caso in esame rappresentato dalla regione, abbia chiesto a un titolare (azienda sanitaria), anche per il tramite del proprio responsabile, di effettuare operazioni di trattamento su dati personali rispetto ai quali quest'ultimo è titolare, indicandone anche le modalità, non esclude che spetti a quest'ultimo, anche in base al principio di responsabilizzazione (artt. 5, par. 2 e 24 del RGPD), valutare la legittimità della richiesta e, in particolare, la sussistenza di una idonea base giuridica per effettuare le operazioni di trattamento richieste, tanto più che, nel caso di specie, le predette operazioni hanno riguardato dati sulla salute di un ingente numero di assistiti a livello regionale attraverso l'uso di algoritmi.

Con specifico riferimento alla violazione dell'art. 35 del RGPD il Garante ha rappresentato che per i trattamenti effettuati dalle aziende sanitarie ricorrono certamente due dei criteri indicati dal Cepd per individuare i casi in cui un trattamento debba formare oggetto di una preventiva valutazione di impatto. In particolare, si fa riferimento ai seguenti criteri: trattamento di dati sensibili o aventi carattere altamente personale e di dati relativi ad interessati vulnerabili tra i quali si annoverano i malati (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 RGPD adottate il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017, e fatte proprie dal Cepd il 25 maggio 2018 -WP 248 rev.01, III, lett. B, punti 4 e 7). L'Autorità ha anche evidenziato che, con riferimento al caso di specie, possono essere soddisfatti anche i criteri relativi al trattamento di dati su larga scala, considerato sia che il trattamento ha riguardato un numero elevato di interessati, sia l'uso innovativo di nuove soluzioni tecnologiche od organizzative (cfr. richiamate linee guida, III, lett. B, punti 5 e 8).

Inoltre le disposizioni d'urgenza adottate nel corso degli ultimi mesi non hanno derogato (e non avrebbero potuto) alle disposizioni in materia di protezione dei dati personali relative alla valutazione di impatto sulla protezione dei dati (art. 35 del RGPD), come dimostrano i numerosi interventi dell'Autorità in materia (cfr., provv. ti 27 gennaio 2022, n. 18, doc. web n. 9742129; 18 febbraio 2022, n. 57, doc. web n. 9746905 e 13 gennaio 2022, n. 9, doc. web n. 9744496).

L'Autorità, tenuto conto che le operazioni di trattamento hanno comportato l'uso di algoritmi e hanno riguardato dati sulla salute di un ingente numero di assistiti, ha ordinato a ognuna delle tre aziende di procedere alla cancellazione dei dati elaborati.

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

Anche nel corso del 2022 il Garante ha continuato a fornire i pareri di competenza con riguardo agli aspetti di protezione dei dati personali connessi all'attuazione dei sistemi informativi sanitari centrali.

Anagrafe nazionale degli assistiti

Un importante intervento ha riguardato il parere reso il 24 febbraio 2022, n. 75, sullo schema di d.P.C.M. relativo all'Anagrafe nazionale degli assistiti (Ana), di cui all'art. 62-*ter*, comma 2, d.lgs. n. 82/2005 (doc. web n. 9751939).

Scopo dell'Ana è quello di agevolare il monitoraggio della spesa sanitaria, accelerare il processo di automazione amministrativa assicurando alle singole aziende sanitarie la disponibilità delle informazioni esatte e aggiornate per lo svolgimento delle funzioni di propria competenza.

L'Ana subentrerà alle anagrafi e agli elenchi degli assistiti tenuti dalle singole aziende sanitarie locali, che mantengono la titolarità dei dati di propria competenza e ne assicurano l'aggiornamento. Le asl cesseranno di fornire ai cittadini il libretto sanitario personale e, in caso di trasferimento di residenza, l'Ana ne darà immediata comunicazione telematica alle aziende sanitarie locali interessate.

Il testo definisce inoltre i contenuti dell'Ana, tra i quali le scelte del medico di medicina generale e del pediatra di libera scelta nonché il codice esenzione e il domicilio. Lo schema stabilisce inoltre il piano per il graduale subentro dell'Ana alle anagrafi e agli elenchi degli assistiti tenuti dalle singole asl e le garanzie e le misure di sicurezza nonché le modalità con cui gli interessati possano accedere in rete ai propri dati personali contenuti nell'Ana, ovvero richiederne copia cartacea presso l'asl competente.

Lo schema di decreto su cui l'Autorità ha reso il proprio parere (che consente, tra l'altro, di dare attuazione all'investimento "potenziamento del Fse", previsto dalla Missione 6 del Pnrr) è stato elaborato tenendo anche conto delle indicazioni fornite dall'Ufficio relative in particolare alla puntuale indicazione del periodo di conservazione dei dati relativi alle variazioni, alle situazioni pregresse, nonché, a quelli degli assistiti non più iscritti; ai dati necessari a garantire la corretta identificazione dell'interessato in relazione all'alimentazione dell'Ana da parte di asl, regioni e province autonome, nonché dal Ministero della salute; alla necessità che il codice identificativo unico a livello nazionale, reso disponibile alle asl da Ana, per i contatti privi di codice fiscale possa essere utilizzabile limitatamente all'ambito sanitario; all'esercizio dei diritti sanciti dal RGPD e alle modalità con cui sono rese le informazioni agli interessati ai sensi degli artt. 13 e 14 del RGPD; alle modalità di accesso dell'interessato, anche per il tramite del Fse, ai dati contenuti in Ana, e di acquisizione di copia informatica del libretto sanitario personale previsto dall'art. 27, l. n. 833/1978.

Scheda di dimissione ospedaliera

Nel 2022 il Garante, considerata l'esigenza manifestata dal Ministero della salute di adeguare il contenuto informativo della scheda di dimissione ospedaliera dei ricoveri riabilitativi allo scopo di fornire una migliore descrizione di tale tipologia di ricovero e di rappresentarne l'esito, ha reso il parere di competenza sullo schema di decreto del predetto Ministro che definisce il regolamento recante integrazioni al decreto 27 ottobre 2000, n. 380 e successive modificazioni, concernente la Scheda di dimissione ospedaliera (Sdo) (parere 28 aprile 2022, n. 141, doc. web n. 9774861).

L'Autorità ha infatti rilevato che l'integrazione prevista afferisce a informazioni di carattere medico scientifico relative alle scale di valutazione della disabilità e della complessità assistenziale da utilizzare nel caso di ricovero di tipo riabilitativo di cui è stata manifestata la necessità di acquisizione nell'ambito del percorso assistenziale e del processo di analisi dei dati e che le misure poste a garanzia degli interessati

individuate, anche a seguito del provvedimento del Garante 26 marzo 2015, n. 178, rimangono pienamente in vigore (doc. web n. 3878687).

Nascite e decessi

Specifiche misure a tutela dei dati personali sono state richieste anche nel parere reso il 26 maggio 2022, n. 193 sullo schema di decreto del Mef, di concerto con il Ministero della salute e con il Ministero dell'interno, attuativo dell'art. 12, d.l. 19 maggio 2020, n. 34, concernente l'accelerazione dell'acquisizione delle informazioni relative alle nascite e ai decessi (doc. web n. 9780893). Con specifico riferimento agli aspetti sanitari, il Garante ha ottenuto che nello schema di decreto fosse garantito il rispetto delle garanzie previste dall'ordinamento a tutela della volontà della madre di non essere nominata nella dichiarazione di nascita (art. 30, d.P.R. n. 396/2000) e del conseguente limite all'accesso a tali informazioni da parte del figlio biologico (artt. 28, l. n. 184/1983 e 93 del Codice). Su richiesta dell'Autorità nelle modalità di dematerializzazione e di invio telematico al Sistema TS delle informazioni relative alle nascite (attestazione e dichiarazione di nascita) e ai decessi (avviso di decesso, certificato necroscopico e denuncia della causa di morte) è stato previsto che l'attestazione di nascita sia resa immediatamente disponibile al Sistema TS e all'Istat priva degli elementi identificativi diretti della donna.

Erogazione di farmaci senza obbligo di prescrizione alle parafarmacie

Parere favorevole condizionato è stato invece reso sullo schema di decreto del Mef da adottare di concerto con il Ministero della salute, concernente le modifiche al decreto del Mef 30 dicembre 2020 per l'estensione dell'erogazione di farmaci senza obbligo di prescrizione alle parafarmacie (parere 24 novembre 2022, n. 400, doc. web n. 9837089). Nell'ambito delle interlocuzioni con i Ministeri competenti l'Ufficio aveva espresso alcune osservazioni circa la necessità di fornire elementi di dettaglio in merito al sistema di reportistica per il monitoraggio dei servizi del Sistema TS offerto in relazione alla dematerializzazione delle ricette bianche, l'assenza di misure tecnico organizzative (quali il *disaster recovery* dei sistemi) nonché l'autenticazione degli utenti al Sistema TS.

Ciò stante, tenuto conto del carattere di urgenza dello schema di decreto – atteso il disposto della sentenza del Tar Lazio 2 novembre 2022, n. 7908 – e al contempo della necessità di assicurare l'uniformità del livello di sicurezza già previsto per le diverse modalità di accesso al Sistema TS da parte degli operatori sanitari, considerate altresì le misure implementate dal Ministero sulla base delle osservazioni formulate dall'Ufficio, l'Autorità ha reso parere favorevole, condizionato, all'introduzione, entro 6 mesi dall'entrata in vigore dello schema di decreto, di procedure di autenticazione informatica a due o più fattori con riferimento ai servizi offerti attraverso il Sistema TS.

5.2.5 Protezione dei dati personali e app *sanitarie*

App di contatto tra pazienti e professionisti sanitari

Nel 2022 l'Autorità è tornata a occuparsi dei trattamenti di dati sulla salute effettuati attraverso *app* volte a facilitare i rapporti tra medico e paziente.

Tra le varie istruttorie avviate dall'Ufficio si evidenzia il provvedimento 20 ottobre 2022, n. 336, con il quale il Garante ha sanzionato un'associazione con riferimento al trattamento dei dati effettuato attraverso una *app* volta a mettere in contatto un paziente Covid-19 con un professionista sanitario (doc. web n. 9831081).

In particolare, il Garante ha contestato una non chiara e corretta definizione dei ruoli del trattamento tra l'associazione e i medici alla stessa aderenti che si ripercuoteva anche sulla corretta individuazione delle basi giuridiche del trattamento e sulle informazioni rese agli interessati risultate contradditorie e incomplete. L'Autorità ha rilevato l'omessa designazione da parte dell'associazione dei professionisti sanitari in qualità di responsabili del trattamento e la non conformità della richiesta del consenso agli interessati ai requisiti richiesti dal Regolamento.

Il Garante ha poi ritenuto che il trattamento in esame rientra tra quelli che

necessitano di una preventiva valutazione d'impatto alla luce della natura dei dati trattati e della potenziale numerosità dei soggetti interessati (art. 35 del RGPD e criteri individuati dal Gruppo Art. 29 nelle 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, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017) ed ha contestato la mancata tempestiva adozione del registro dei trattamenti (art. 5, par. 2).

In tale ambito rileva anche il provvedimento 10 novembre 2022, n. 368, con il quale il Garante ha sanzionato una società con riferimento al trattamento dei dati personali effettuato attraverso una piattaforma, accessibile sia via web che via *app*, funzionale alla prenotazione di prestazioni sanitarie (doc. web n. 9843319). In particolare, il Garante ha contestato che all'atto della prenotazione della prestazione sanitaria da parte dell'interessato la società non avesse fornito informazioni chiare sui diversi trattamenti svolti sia in qualità di titolare che nel ruolo di responsabile dei professionisti sanitari a cui l'interessato poteva rivolgersi, non garantendo quindi un trattamento corretto e trasparente, in violazione degli artt. 5, par. 1, lett. *a*); 12 e 13 del RGPD. L'erronea indicazione nell'informativa all'interessato del ruolo della società ha comportato anche un'errata informazione all'interessato circa la tipologia di dati trattati. Il Garante ha quindi rilevato che all'interessato sono state fornite informazioni non corrette e incongruenti, in quanto da un lato era stato affermato che la società nella fase della prenotazione era titolare del trattamento (sebbene sia stata invece designata responsabile) e dall'altro che la stessa non trattava dati sulla salute. Il Garante ha infine evidenziato che la violazione dei principi di correttezza e trasparenza si è poi riverberata nella corretta individuazione delle basi giuridiche e delle finalità del trattamento.

Sistema di monitoraggio del glucosio

Merita altresì di essere segnalato il provvedimento 7 luglio 2022, n. 242, con il quale è stata sanzionata una società statunitense, per violazioni sui dati personali nell'utilizzo del proprio sistema di monitoraggio del glucosio e per aver comunicato illecitamente indirizzi di posta elettronica e dati sulla salute di circa 2.000 pazienti diabetici italiani (doc. web n. 9809998). L'istruttoria aveva avuto origine dal *data breach* in cui la società aveva rappresentato che un proprio dipendente, nell'ambito di una campagna informativa, aveva inviato un messaggio di posta elettronica, inserendo gli indirizzi dei destinatari nel campo "cc" invece che nel campo "ccn". Ciascun destinatario aveva avuto così la possibilità di visualizzare gli indirizzi *e-mail* di tutti gli altri. Il Garante ha ribadito che in base al Regolamento, l'indirizzo di posta elettronica è da considerarsi un dato personale e che, considerato che la comunicazione era indirizzata a persone affette da diabete, le informazioni contenute nella *e-mail*, erano idonee a rivelare lo stato di salute e quindi potevano essere comunicate a terzi solo sulla base di una delega scritta dell'interessato o di un idoneo presupposto giuridico.

Nel corso dell'istruttoria sono emerse ulteriori violazioni relative all'utilizzo del sistema di monitoraggio del glucosio. Scaricando l'apposita *app*, infatti, gli utenti erano chiamati ad accettare con un unico clic sia le condizioni contrattuali del servizio sia il contenuto dell'informativa *privacy*, rendendo così impossibile formulare specifici consensi per i diversi trattamenti dei dati, quale quello per il trattamento dei dati sulla salute che richiede un consenso esplicito, ciò in violazione del principio di liceità del trattamento (artt. 5, par. 1, lett. *a*), e 9 par. 2, lett. *a*), del RGPD).

Il Garante ha inoltre accertato la violazione dei principi di correttezza e trasparenza avendo la società fornito agli utenti un'informativa priva di alcuni degli elementi essenziali previsti dalla disciplina vigente (artt. 5, par. 1, lett. *a*), 12 e 13 del RGPD)

Dispositivi medico-diagnostici in vitro

nonché la violazione dell'obbligo di designare per iscritto il proprio rappresentante nell'Unione europea (art. 27 del RGPD). Con il predetto provvedimento il Garante ha ingiunto al titolare del trattamento una sanzione pecuniaria e l'adozione di specifiche misure correttive in conformità alle disposizioni del RGPD, cui la società ha dato seguito nei termini indicati.

L'Autorità è anche intervenuta con parere 26 maggio 2022, n. 190, sullo schema di decreto legislativo, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del reg. (UE) 2017/746, relativo ai dispositivi medico-diagnostici in vitro (doc. web n. 9789069). In particolare, il Garante ha reso un parere condizionato rilevando come necessaria l'integrazione normativa con alcune misure a tutela della protezione dei dati personali. In tal senso, l'Autorità ha chiesto di inibire l'accesso ai dati anagrafici e anamnestici del paziente, salva l'indispensabilità ai fini dell'erogazione del servizio di manutenzione e telediagnosi/teleintervento, rendendo comunque tracciabile ogni operazione di intervento/accesso, nonché di prevedere che sia designata quale responsabile del trattamento, ai sensi dell'art. 28 del RGPD, la società produttrice del dispositivo medico, per le attività di controllo della funzionalità dell'apparecchiatura anche a distanza svolta per conto del titolare (cd. servizi di manutenzione e di assistenza).

Il Garante ha inoltre chiesto di indicare i tempi di conservazione dei dati personali eventualmente forniti a corredo delle comunicazioni di incidenti verificatisi dopo l'immissione in commercio di un dispositivo, ai sensi dell'art. 13, comma 8, del citato schema di decreto.

5.3. *Trattamenti per finalità di cura e amministrative correlati alla cura*

5.3.1. Provvedimenti derivanti da data breach

Molteplici istruttorie avviate a seguito di notifiche di violazione di dati personali, pervenute ai sensi dell'art. 33 del RGPD, hanno avuto come esito dei provvedimenti correttivi.

In particolare, a seguito di una notizia stampa e di una notifica di violazione è stato esaminato un trattamento di dati effettuato da un'azienda sanitaria mediante un sistema di acquisizione e gestione dati dello *screening* Covid-19. È emerso che il QR *code* consegnato ai partecipanti era generato tramite una codifica sequenziale, con una associazione diretta partecipante-esito tampone. Pertanto, generando QR *code* in sequenza rispetto a un primo codice in possesso di un soggetto terzo era possibile visualizzare dati anagrafici e, ove presente, il numero di cellulare del soggetto coinvolto nello *screening*, nonché gli esiti del tampone. Era stato, inoltre, constatato che la piattaforma che gestiva il servizio consentiva la decodificazione del codice fiscale; inserendo infatti il codice fiscale di un assistito, erano restituiti il suo nome e cognome e, in un primo momento, anche il numero di cellulare eventualmente presente all'interno della banca dati. Oltre a tali vulnerabilità, è stato constatato che la comunicazione dell'esito dei tamponi era effettuata per mezzo di sms. Tale scelta, motivata dalla semplicità e dalla necessità di evitare assembramenti, in considerazione della situazione emergenziale, è risultata, tuttavia non conforme alle linee guida in tema di referti *online* del 19 novembre 2009 (doc. web n. 1679033), alle disposizioni del d.P.C.M. 8 agosto 2013 e alle normative emergenziali, in base alle quali può essere comunicato via sms solo il numero unico di referto elettronico (Nrfe) del tampone e non anche il suo esito (art. 19, d.l. n. 137/2020; decreto Mef 3 novembre 2020, cfr. doc. web n. 9563445). Nell'ambito della stessa istruttoria è emerso che il titolare del trattamento non aveva effettuato una valutazione di impatto, ai sensi dell'art. 35

del RGPD. L'Autorità ha, pertanto, adottato un provvedimento correttivo, che ha tenuto conto del fatto che l'istruttoria ha riguardato un trattamento di dati personali effettuato nella fase emergenziale e che è stata avviata a seguito di notizie stampa e di comunicazione di violazione effettuata dal titolare del trattamento (provv. 13 gennaio 2022, n. 9, doc. web n. 9744496).

Alcune notifiche ricevute dall'Autorità ai sensi dell'art. 33 del RGPD hanno riguardato la comunicazione di dati sulla salute, anche contenuti in documentazione sanitaria, a soggetti diversi dall'interessato, in mancanza di un presupposto giuridico legittimante. In particolare, è stata comminata una sanzione ad un'azienda socio sanitaria territoriale, che aveva comunicato un referto relativo ad un esame diagnostico eseguito presso un ambulatorio a persona non legittimata a riceverlo (provv. 10 febbraio 2022, n. 47, doc. web n. 9754355).

In un altro caso, la comunicazione, avvenuta in due circostanze in occasione dell'imbustamento di documentazione sanitaria da parte di un'azienda usl, aveva determinato una violazione dei principi di integrità e riservatezza di cui all'art. 5, par. 1, lett. *a*) e *f*), del RGPD nonché degli artt. 9 e 32 del RGPD medesimo (provv. 10 marzo 2022, n. 85, doc. web n. 9762945).

Analogamente, è stata sanzionata un'azienda socio sanitaria territoriale, in relazione alla consegna di un supporto digitale riferito ad una prestazione neuroradiologica a un soggetto non legittimato a riceverlo. Nella determinazione dell'ammontare della sanzione comminata all'azienda, è stato considerato tra l'altro il carattere colposo della violazione che ha riguardato un unico soggetto e la circostanza che l'Autorità ha preso conoscenza dell'evento a seguito della notifica di violazione dei dati personali effettuata dal titolare (provv. 12 maggio 2022, n. 176, doc. web n. 9781947).

Tale ultimo elemento è stato, altresì, considerato nell'adozione di un provvedimento nei confronti di un'azienda usl che aveva notificato ai sensi dell'art. 33 del RGPD una violazione realizzatasi attraverso l'inserimento di una cartella infermieristica di un paziente nella cartella clinica di altro paziente e allo stesso consegnata. La violazione, anche in considerazione di specifici aspetti, è stata valutata come minore sicché si è ritenuto sufficiente ammonire il titolare del trattamento ai sensi degli artt. 58, par. 2, lett. *b*) e 83, par. 2, del RGPD (provv. 20 ottobre 2022, n. 343, doc. web n. 9828208).

L'Autorità, a seguito di due notifiche di *data breach*, effettuate ai sensi dell'art. 33 del RGPD, da una azienda sanitaria della Toscana e aventi ad oggetto, entrambi, una comunicazione di dati relativi alla salute in assenza di un idoneo presupposto giuridico per errore nell'imbustamento di documentazione sanitaria da inviare ai pazienti, disposta la riunione dei procedimenti istruttori (trattandosi di fattispecie analoghe afferenti al medesimo titolare del trattamento), ha sanzionato l'azienda medesima per la violazione degli artt. 5 par. 1, lett. *a*) e *f*), 9 e 32 del RGPD (provv. 10 marzo 2022 n. 85, doc. web n. 9762945).

Anche in un'altra vicenda, in presenza di due notifiche di *data breach*, effettuate ai sensi dell'art. 33 del RGPD da parte di una stessa azienda sanitaria, riguardanti, in entrambi i casi, lo smarrimento di parte della documentazione medica della cartella clinica relativa a due pazienti, l'Autorità ha disposto la riunione dei relativi procedimenti e sanzionato l'azienda citata per violazione del principio di integrità e riservatezza di cui all'art. 5, par. 1, lett. *f*), nonché per l'inosservanza degli obblighi in materia di sicurezza di cui dell'art. 32 del RGPD (provv. 21 luglio 2022, n. 263, doc. web n. 9809520).

Una sanzione pecuniaria è stata inflitta a un'azienda sanitaria della Lombardia per aver comunicato, nello svolgimento delle attività istituzionali relative all'Urp aziendale, dati relativi alla salute di una paziente a un soggetto terzo, non autorizzato

dall'interessata, in violazione dell'art. 9, par. 1, del RGPD, degli obblighi di sicurezza di cui all'art. 32 del RGPD e dei principi di base del trattamento di cui all'art. 5, par. 1, lett. *f*), del RGPD medesimo (provv. 10 marzo 2022, n. 84, doc. web n. 9763968).

Le notifiche di violazioni in ambito sanitario sono state effettuate anche da soggetti privati: in particolare, un importante ospedale ha notificato due violazioni aventi ad oggetto l'inserimento, nel campo denominato "copia conoscenza" (cc) in luogo del campo "copia conoscenza nascosta" (ccn) alcuni indirizzi *e-mail* dei destinatari di una *newsletter* diretta, in un caso, ai pazienti dell'Unità operativa di neurologia, e, in un altro, ai pazienti dell'Unità chirurgia trapianti e metabolico-bariatrica. Nel provvedimento è stato rappresentato che gli indirizzi *e-mail* costituiscono informazioni personali e che dal contesto delle comunicazioni poteva desumersi che i destinatari erano pazienti delle predette unità operative. Pertanto, erano stati inseriti senza giustificato motivo e in assenza di presupposto giuridico, rivelati reciprocamente, ai destinatari delle comunicazioni, lo stato di salute degli altri pazienti. L'ospedale è stato, pertanto, destinatario di una sanzione per aver effettuato un trattamento in violazione dei principi base di cui agli artt. 5, lett. *f*) e 9 del RGPD (provv. 28 aprile 2022, n. 164, doc. web n. 9779057).

5.3.2. Provvedimenti derivanti da reclami e segnalazioni

Anche nel 2022 sono pervenuti numerosi reclami ed istanze concernenti il trattamento di dati personali effettuato per il perseguimento di finalità di cura e amministrative correlate alla cura. Alcune istruttorie si sono concluse con l'adozione di provvedimenti correttivi.

A seguito di un reclamo il Garante ha sanzionato la Regione Lazio con riferimento ad un invito di una asl rivolto alla figlia della reclamante, deceduta quasi vent'anni prima, a partecipare al programma di *screening* del tumore del collo dell'utero (provv. 15 settembre 2022, n. 304, doc. web n. 9810028). L'Autorità ha ricordato che le informazioni, acquisite da un sistema informativo regionale dedicato allo *screening*, si qualificano come informazioni sulla salute degli interessati in quanto, oltre ad indicare prestazioni sanitarie erogate nei confronti di specifiche categorie di interessati, si riferiscono anche all'anamnesi personale e familiare (cons. n. 35 e art. 4, par. 1, n. 15 del RGPD; cfr. provv.ti 12 marzo 2020, n. 49, doc. web n. 9310804 e 21 aprile 2021, n. 147, doc. web n. 9591223).

L'Autorità ha inoltre invitato la Regione ad individuare correttamente la titolarità del trattamento anche in funzione delle finalità che la normativa di settore attribuisce ai soggetti che intervengono nel trattamento (regione e aziende sanitarie), poiché l'erronea attribuzione dei ruoli aveva determinato una errata individuazione delle basi giuridiche del trattamento, nonché delle informazioni rese agli interessati. Nel medesimo provvedimento l'Autorità è intervenuta anche sul mancato rispetto del principio di esattezza dei dati trattati attraverso il predetto sistema informativo sullo *screening*, in quanto la Regione, in qualità di titolare del trattamento, non aveva adottato misure tecniche e organizzative idonee a garantire l'aggiornamento dei dati trattati attraverso tale sistema informativo. Il Garante ha inoltre ribadito che ai dati personali concernenti le persone decedute continuano ad applicarsi le tutele previste dalla disciplina in materia di protezione dei dati personali (cfr. ex *multis* parere 7 febbraio 2019, n. 27, doc. web n. 9090308).

Da un'istruttoria avviata a seguito di un reclamo di una paziente di un centro radiologico è emerso che la società che lo gestiva aveva omesso di fornire agli interessati una serie di elementi informativi previsti dall'art. 13 del RGPD (quali quelli relativi al diritto di proporre reclamo all'autorità di controllo, all'indicazione del periodo di

conservazione delle informazioni o ai criteri utilizzati per determinare tale periodo, nonché dei dati di contatto del Rpd). Inoltre, il Rpd non era stato designato in conformità alle disposizioni del Regolamento e, in ogni caso, i dati di contatto dello stesso non erano stati pubblicati sul sito web né comunicati al Garante, violando, in questo modo, l'art. 37 del RGPD. Tale inosservanza, contrariamente all'impegno dichiarato dal titolare del trattamento nel corso dell'audizione, è risultata persistente anche al momento dell'adozione del provvedimento, con la conseguenza che il Garante ha adottato, sul punto, un provvedimento sanzionatorio e prescrittivo (provv. 10 novembre 2022, n. 372, doc. web n. 9843603), che il titolare del trattamento ha impugnato in giudizio.

Una reclamante aveva lamentato la trasmissione di informazioni sulla sua salute da parte di una società ad un'altra, presso la quale praticava attività sportiva. Nel provvedimento sanzionatorio nei confronti della prima società, il Garante ha chiarito che, alla luce della specifica normativa di settore (art. 3, commi 2 e 4, d.m. 24 aprile 2013; cfr. anche decreto 8 agosto 2014, all. n. 1, punti 2 e 3), la notizia relativa alla sospensione dell'idoneità all'attività sportiva non agonistica, rendendosi necessari specifici esami di accertamento, rivela di per sé informazioni sullo stato di salute del soggetto il cui giudizio di idoneità è stato sospeso (sospetto diagnostico o patologie croniche e conclamate) (art. 4, par. 1, n. 15, del RGPD e cons. n. 35). Considerato che la reclamante non aveva prestato il proprio consenso alla comunicazione, è stata rilevata l'illiceità dei trattamenti effettuati dalla società (provv. 24 novembre 2022, n. 388, doc. web n. 9842370).

Un cittadino aveva segnalato di aver ricevuto, da un'azienda ospedaliero-universitaria, un referto di anatomia patologica, relativo ad un altro paziente, avente un cognome simile. Il Garante ha al riguardo evidenziato che la trasmissione delle menzionate informazioni da parte della citata azienda, quale responsabile del trattamento, non esonera da responsabilità il titolare del trattamento, un istituto di prevenzione oncologica, che avrebbe dovuto svolgere attività di vigilanza e controllo sull'attività svolta, per proprio conto, dall'azienda (artt. 24 e 28 del RGPD).

Infatti l'obbligo del titolare di mettere in atto misure adeguate ed efficaci anche con riferimento alla predisposizione di misure tecniche e organizzative che soddisfino i requisiti del Regolamento sotto il profilo della sicurezza (cons. n. 74 e artt. 24 e 32 del RGPD), sussiste anche quando talune operazioni di trattamento siano poste in essere da un responsabile che agisce per suo conto e quando utilizza servizi realizzati da terzi. Per tali ragioni, è stata rilevata l'illiceità del trattamento effettuato dall'istituto, in qualità di titolare del trattamento, in relazione alla comunicazione di dati relativi alla salute di una sua paziente effettuata in assenza di una base giuridica, in violazione dell'art. 9, nonché dei principi di base di cui all'art. 5, par. 1, lett. *f*), del RGPD (provv. 20 ottobre 2022, n. 344, doc. web n. 9828965).

La circostanza che il trattamento fosse stato effettuato da un altro soggetto, un'azienda ospedaliero-universitaria, designata responsabile del trattamento, ha portato ad aprire l'istruttoria anche nei confronti di quest'ultima per la comunicazione di dati sulla salute di una paziente dell'istituto a un soggetto non legittimato a riceverli. L'azienda, destinataria anch'essa di un provvedimento sanzionatorio, ha impartito indicazioni agli operatori di scaricare nella cartella di servizio un solo referto per volta, eliminandolo dopo aver effettuato la trasmissione, e ha avviato un confronto con i tecnici informatici per migliorare le misure di segregazione fisica o logica dei dati personali (provv. 20 ottobre 2022, n. 345, doc. web n. 9832526).

A seguito di un reclamo nei confronti di un medico per un presunto illecito trattamento di dati personali, l'Autorità ha sanzionato il titolare del trattamento che, nel rispondere all'interessato allegando i *file* di un esame diagnostico, aveva omesso

5

di verificare che l'interessato fosse l'unico destinatario della Pec, inviando i citati *file* anche all'ordine dei medici e odontoiatri del territorio di appartenenza. In ragione delle circostanze, la violazione è stata considerata come minore, ai sensi del cons. 148 del RGPD e delle linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del RGPD, adottate dal Gruppo Art. 29 il 3 ottobre 2017, WP 253 e fatte proprie dal Cepd con l'*Endorsement* 1/2018 del 25 maggio 2018 (provv. 1° dicembre 2022, n. 403, doc. web n. 9842754).

5.4. *Trattamenti per finalità ulteriori rispetto a quelle di cura e/o amministrative correlati alla cura*

Alcune istanze hanno riguardato il trattamento di dati sulla salute per finalità non riconducibili alla cura o alle attività amministrative correlate alla cura. In particolare, in un caso un reclamante aveva contestato la condotta di un'azienda sanitaria che lo diffidava dal reiterare le sue molteplici richieste. La predetta comunicazione, nella quale erano riportati taluni riferimenti alle condizioni di salute relative alla madre, veniva trasmessa, per conoscenza, ad una serie di soggetti istituzionali, destinatari anch'essi delle richieste del reclamante, nonché al direttore generale di una università, al fine di segnalare un presunto utilizzo improprio da parte del reclamante della *e-mail* istituzionale dell'ateneo. All'esito dell'istruttoria, il trattamento è risultato non rispettoso dei principi di liceità, correttezza e trasparenza, di limitazione della finalità e di minimizzazione dei dati, di cui agli artt. 5 lett. *a*), *b*) e *c*) e 9 del RGPD. Tuttavia, considerati una serie di elementi (tra i quali la circostanza che l'azienda aveva richiamato l'attenzione delle strutture coinvolte sulla necessità di evitare che dati sanitari relativi a persone fisiche, anche se indicate solo con le iniziali, fossero portate a conoscenza di soggetti non autorizzati al trattamento di tali dati ed il comportamento insistente del reclamante in un momento di particolare complessità per l'azienda a causa della gestione dell'emergenza sanitaria allora in atto) il caso è stato valutato quale violazione minore ed il titolare del trattamento è stato ammonito (provv. 12 maggio 2022, n. 175, doc. web n. 9781912).

Una condotta lesiva degli interessati è stata riscontrata nella vicenda segnalata da una coppia di reclamanti che aveva lamentato la pubblicazione sul sito web relativo all'attività di una psicologa, di una tesi di specializzazione dalla stessa redatta, nella quale era rappresentata la storia familiare dei reclamanti ed erano indicati per esteso i nomi di battesimo, le età di tutti gli appartenenti alla famiglia, le professioni svolte, con i dettagli sui luoghi, e la storia delle rispettive famiglie di origine. Nel provvedimento è stato sottolineato che la circostanza che i reclamanti avevano ricevuto prestazioni di psicoterapia costituisce un dato sulla salute (cfr., altresì, provv. 19 maggio 2022, n. 188, doc. web n. 9774696, provv. 29 settembre 2021 n. 358, doc. web n. 9720448). Nel ricordare le tecniche per anonimizzare le informazioni (cfr. cons. n. 26 del RGPD e WP29 *Opinion 05/2014 on Anonymisation techniques*), è stato ritenuto che l'eliminazione del riferimento al cognome degli interessati non costituisce una procedura idonea a garantire il processo di anonimizzazione dei dati personali degli interessati sicché la psicologa aveva diffuso dati personali e sulla salute dei due reclamanti (nonché, inevitabilmente, anche di altri soggetti, come figli e familiari), rispetto ai quali la legittima aspettativa di confidenzialità e riservatezza era ancora più elevata, anche in considerazione del rapporto professionale e fiduciario instauratosi. Pertanto, è stata rilevata l'illiceità del trattamento di dati personali effettuati dalla dottoressa per la violazione degli artt. 5, 6, 9 e 32 del RGPD nonché dell'art. 2-*septies*, comma 8, del Codice (provv. 24 novembre 2022, n. 387, doc. web n. 9844780).

Si segnala, inoltre, l'apertura di un'istruttoria, avviata sulla base di articoli di stampa *online*, nei confronti di un'agenzia regionale, in relazione ad un progetto riguardante l'installazione di *dashcam* e la fornitura di *bodycam* agli operatori in servizio sui mezzi di soccorso per finalità di sicurezza.

In tale occasione è stato in particolare rappresentato che la consultazione preventiva deve contenere l'indicazione delle misure che sono state individuate per affrontare e, di conseguenza, ridurre i rischi che uno specifico trattamento può comportare per i diritti e le libertà delle persone fisiche.

Nella medesima occasione, è stata richiamata l'attenzione sulla esigenza di valutare attentamente la proporzionalità dell'iniziativa in esame, tenendo presente il necessario rispetto in particolare del principio di minimizzazione dei dati raccolti, da considerarsi anche in relazione alla possibile raccolta di dati relativi all'audio evidenziando che spetta al titolare, in base al principio di responsabilizzazione (art. 5 del RGPD) e sulla base degli accordi raggiunti con le organizzazioni sindacali, valutare se, nel caso concreto, la raccolta dell'audio sia necessaria per il perseguimento della prospettata finalità di sicurezza. Analogamente, una stringente valutazione in termini di proporzionalità e necessità del trattamento in questione deve essere effettuata anche con riguardo, alla funzionalità di geolocalizzazione che potrebbe essere integrata nelle cd. *bodycam*, tenuto conto della particolare invasività delle diverse tecnologie congiuntamente impiegate e degli specifici rischi per gli interessati nel contesto lavorativo. A tal riguardo, è stato fatto presente che, il titolare del trattamento, per impostazione predefinita, deve raccogliere solo i dati personali necessari per la specifica finalità del trattamento (cfr. linee guida 4/2019, adottate il 20 ottobre 2020 dal Cepd, spec. punti 7 e 39, 42, 44 e 49). In tale quadro, come messo in evidenza di recente dal Garante, in ambito lavorativo, ancorché in un diverso contesto (v., nei confronti di un'azienda ospedaliera, provv. 7 aprile 2022, n. 134, doc. web n. 9768363), il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve eseguire una attenta valutazione dei rischi e accertarsi che siano disattivate le funzioni che possono comportare trattamenti di dati non necessari o comunque in contrasto con la disciplina di protezione dei dati e la normativa di settore (nota 30 novembre 2022).

6 La ricerca scientifica

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

Nel campo della ricerca scientifica si evidenziano quattro provvedimenti con i quali il Garante, adito in consultazione preventiva ai sensi degli artt. 110, comma 1, ultimo capoverso del Codice e 36 del RGPD, ha espresso parere favorevole in ordine al trattamento dei dati personali per finalità di ricerca medica, biomedica ed epidemiologica in ragione della impossibilità di acquisire il consenso da parte degli interessati convolti nella ricerca.

Un'azienda ospedaliera universitaria ha presentato un'istanza di consultazione preventiva in qualità di promotore di uno studio *no profit*, monocentrico, osservazionale, retrospettivo, non farmacologico volto a descrivere l'effetto della pandemia da Sars-CoV-2 sull'occorrenza dei ricoveri e degli accessi in pronto soccorso negli ospedali di una regione, a causa dell'impossibilità di acquisire, per motivate e comprovate ragioni organizzative, temporali ed economiche, il consenso dell'elevato numero di interessati coinvolti.

Nella prima versione del progetto era prevista l'estrazione, da parte del titolare del trattamento, di dati relativi alla salute in forma pseudonimizzata dai flussi informativi derivanti dalle schede di dimissione ospedaliera e dagli accessi di pronto soccorso. A tale riguardo, l'Autorità ha ribadito che la procedura di cui all'art. 110, comma 1, secondo capoverso del Codice non può costituire di per sé la sola base normativa per consentire a soggetti che trattano dati per l'esecuzione di compiti di interesse pubblico di comunicarli per scopi di ricerca scientifica. Tale trattamento è infatti ammesso solo se espressamente previsto da una specifica base normativa che soddisfi i requisiti di cui all'art. 2-*sexies* del Codice.

L'istanza di consultazione preventiva ex art. 110 del Codice rappresenta, invece, una norma di chiusura per consentire che trattamenti di dati personali che si sarebbero dovuti fondare sul consenso degli interessati possano comunque essere svolti. Tale disposizione non può pertanto essere utilizzata surrettiziamente per svolgere operazioni di trattamento per le quali il consenso degli interessati non potrebbe costituire un idoneo presupposto giuridico (cons. 43).

Successivamente ai rilievi formulati dall'Ufficio, la seconda versione del progetto ha previsto la raccolta dei dati direttamente presso i centri partecipanti, quali autonomi titolari. Tenuto conto del corretto inquadramento delle basi giuridiche del trattamento, delle misure tecniche e organizzative indicate nella valutazione d'impatto, con particolare riferimento alla pseudonimizzazione dei dati trattati, nonché all'avvenuta pubblicazione dell'informativa sui siti internet dei centri partecipanti (cfr. artt. 14, par. 5, lett. *b*), del RGPD e 6, comma 3 delle regole deontologiche, per trattamenti a fini statistici o di ricerca scientifica del 19 dicembre 2018, n. 515, doc. web n. 9069637), il Garante ha reso parere favorevole (provv. 7 aprile 2022, n. 118, doc. web n. 9772545).

Un secondo parere ha riguardato un'istanza di consultazione preventiva presentata da un'azienda ospedaliera universitaria promotrice di uno studio osservazionale interdipartimentale, prospettico, retrospettivo, non farmacologico volto alla creazione di un registro o banca dati strutturati funzionali ad esaminare la popolazione dei

pazienti affetti da patologie neoplastiche e non del distretto toracico, per avviare specifici progetti di ricerca successivamente oggetto di appositi protocolli e della valutazione dei comitati etici territorialmente competenti. Il progetto prevedeva non solo il trattamento di dati sulla salute ma anche di quelli relativi all'origine razziale ed etnica degli interessati molti dei quali, all'esito di comprovati tentativi di contatto, erano risultati deceduti o non contattabili.

Il Garante ha ritenuto che l'azienda abbia correttamente individuato le basi giuridiche (consenso o art. 110 del Codice) per la costituzione del predetto *database*, ma non per le successive fasi del trattamento relative ad ulteriori e specifici studi.

Il Garante ha valutato la fattispecie in esame riconducibile a quella di cui al cons. 33 del RGPD il quale consente, quando al momento della raccolta dei dati non è possibile individuare pienamente le specifiche finalità del trattamento, che l'interessato possa prestare il consenso per il trattamento dei dati personali per scopi di ricerca scientifica nelle fasi successive a quella iniziale, autorizzando in un primo momento solo la raccolta e conservazione dei dati (artt. 6 e 7 del RGPD e punto 7.2 delle linee guida 5/2020 sul consenso ai sensi del RGPD adottate il 4 maggio 2020).

Il Garante ha stabilito pertanto che l'azienda dovrà integrare le manifestazioni di volontà degli interessati già raccolte con specifici consensi per giungere in via progressiva ad ottenere un presupposto giuridico idoneo al trattamento dei dati per gli scopi di ricerca scientifica indicati nei protocolli che verranno approvati ovvero, laddove si trovasse in una delle condizioni di cui all'art. 110 del Codice e al punto 5.3 delle prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, all. 5 al provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, d.lgs. 10 agosto 2018, n. 10 (doc. web n. 9124510), dovrà avanzare specifiche istanze di consultazione preventiva ai sensi del predetto art. 110 del Codice.

In merito ai dati inerenti all'origine razziale ed etnica degli interessati, il Garante ha raccomandato la scrupolosa applicazione di quanto stabilito dal punto 5.4 delle citate prescrizioni nei singoli progetti di ricerca per i quali sarà previsto il trattamento di tali informazioni.

Infine, con riferimento all'anonimizzazione dei dati al termine del periodo di conservazione degli stessi, ha prescritto all'azienda di rimuovere ogni dato riferibile esclusivamente ad una singola persona (singolarità) qualora, con qualsiasi mezzo, ne venga a conoscenza in una fase successiva all'applicazione delle tecniche di anonimizzazione e a tenere traccia di tali eventi in modo da ripetere la valutazione del rischio di re-identificazione al raggiungimento del 1% di singolarità individuate sul totale di informazioni incluse nella banca dati (provv. 30 giugno 2022, n. 238, doc. web n. 9791886).

In un altro caso una società farmaceutica aveva presentato un'istanza di consultazione preventiva, ex art. 110 del Codice, in qualità di promotore e titolare del trattamento di uno studio clinico, osservazionale, retrospettivo, multicentrico in ragione del fatto che tra i pazienti arruolati vi erano anche soggetti risultati deceduti o non più contattabili. Lo studio era volto, in via prioritaria, a descrivere l'approccio diagnostico e terapeutico nei pazienti affetti da carcinoma testa collo a cellule squamose HNSCC per la realizzazione del quale era prevista la raccolta di dati in forma pseudonimizzata.

La società aveva rappresentato di aver sottoposto il protocollo di studio ai competenti comitati etici allo scopo di ottenere il previo parere positivo e si era avvalsa del supporto di una società esterna, quale CRO (*Contract Research Organization*), nominata responsabile del trattamento ai sensi dell'art. 28 del RGPD.

La società aveva dichiarato, inoltre, che in riferimento ai dati non raccolti presso

6

gli interessati gli oneri informativi sarebbero stati assolti attraverso la pubblicazione dell'informativa sul proprio sito internet e su quello di centri partecipanti (artt. 14, comma 5, lett. *b*), del RGPD e 6, comma 3 delle regole deontologiche).

Con riferimento alle basi giuridiche del trattamento, la società aveva indicato altresì la disciplina della farmacovigilanza ritenuta dall'Ufficio, *prima facie*, inconferente, attesa la natura dello studio e successivamente la disciplina di cui al d.m. 30 aprile 2015 ed aveva altresì previsto di consentire l'accesso a dati in forma aggregata e anonima, a liberi professionisti per la stesura di articoli scientifici e del rapporto clinico finale.

Il Garante, con riferimento alle numerose tecniche di anonimizzazione prospettate, ha evidenziato che l'esiguità del numero di interessati (pari a circa 300), la loro localizzazione dispersa nel territorio nazionale e la rarità della patologia, rappresentano fattori contestuali ineliminabili ad elevato potere identificativo, con l'effetto che, per il caso di specie, non appare percorribile l'ipotesi di un'anonimizzazione a livello di singoli *record*, quali la generalizzazione dei dati.

Il Garante, al fine di scongiurare il rischio di ricostruzione di dati riferibili a singoli individui ha quindi chiesto alla società al termine del periodo di conservazione dei dati per lo svolgimento dello studio e comunque in ipotesi di condivisione dei dati con soggetti terzi, che il numero di statistiche aggregate da rendere conoscibili, sia significativamente inferiore rispetto al numero delle variabili considerate.

È stato inoltre prescritto alla società di rimuovere ogni singolarità, qualora, con qualsiasi mezzo, ne venga a conoscenza in una fase successiva all'applicazione delle predette tecniche di anonimizzazione e di tenere traccia di tali eventi in modo da ripetere la valutazione del rischio di re-identificazione al raggiungimento del 1% di singolarità individuate sul totale di *record* inclusi nel *dataset* (provvedimento non pubblicato ai sensi dell'art. 24 del reg. Garante 1° agosto 2013).

In altro caso similare una fondazione aveva presentato un'istanza di consultazione preventiva, ai sensi degli artt. 110 del Codice e 36 del RGPD, per la realizzazione di uno studio clinico, osservazionale, retrospettivo, multicentrico da condurre presso sette centri sperimentali di eccellenza, riguardante dati sulla salute e genetici di persone (circa 500), risultate non contattabili all'esito di documentati tentativi. In particolare, lo studio è volto a costruire una fonte di campioni biologici clinicamente registrati al fine di alimentare i laboratori di un consorzio, appositamente istituito, per l'implementazione della ricerca traslazionale di precisione nei tumori al seno. A tale riguardo, ciascun obiettivo del consorzio avrebbe avuto un promotore (non necessariamente la fondazione istante) ed una specifica e autonoma valutazione dei presupposti di liceità del trattamento dei dati a tali fini necessari; i dati sarebbero stati raccolti in forma pseudonimizzata attraverso l'attribuzione di un codice alfanumerico la cui chiave di decodificazione sarebbe rimasta esclusivamente in possesso dei centri partecipanti.

Nell'istanza trasmessa era stata rappresentata la natura flessibile del progetto organizzato in quattro differenti livelli di indagine. L'istanza di consultazione preventiva riguardava esclusivamente il livello iniziale, consistente in una raccolta di dati retrospettiva relativa anche pazienti deceduti ovvero non contattabili. Con riguardo ai successivi livelli di indagine (cd. *tier* 1, 2 e 3) il trattamento dei dati personali si basava sul consenso degli interessati.

Gli oneri informativi in relazioni ai dati raccolti presso i centri sperimentali, sarebbero stati assolti attraverso la pubblicazione delle informative sui relativi siti internet (artt. 14, par. 5, lett. *b*), del RGPD e 6, comma 3, delle regole deontologiche).

Il Garante ha ritenuto adeguati i tempi di conservazione dei dati trattati (dati clinici e i campioni dei pazienti arruolati) individuati in un arco temporale almeno

pari a quello del progetto finanziato (7 anni più ulteriori 7 anni in caso di possibile rinnovo).

La fondazione aveva poi prospettato la possibilità di sottoporre il *database*, privato degli identificatori e delle relative chiavi di *decripting* ad un notaio, quale garante della sua conservazione e del suo non utilizzo, anche al fine di avviare nuove ricerche.

Al riguardo il Garante ha sottolineato che il principio di limitazione della conservazione dei dati prevede che essi possano essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati raccolti e che in caso di prosecuzione dello studio la fondazione potrebbe definire un ulteriore periodo di conservazione.

In tale ipotesi il titolare dovrà preventivamente informare gli interessati non contattabili attraverso specifiche inserzioni sul proprio sito internet e su quelli dei centri sperimentali, e dovrà informare direttamente gli interessati in vita, con i quali, attraverso i centri sperimentali, dovesse entrare in contatto (artt. 13 e 14, par. 5, lett. *b*), del RGPD), dando sin d'ora nell'informativa notizia di tale eventualità.

Tenuto conto che lo studio prevede il trattamento di dati genetici, il Garante ha sottolineato l'importanza di evidenziare che lo studio potrebbe avere significative ricadute personalizzate in termini di terapia (art. 9, par. 2, lett. *h*), del RGPD e provv. 7 marzo 2019, n. 55, doc. web n. 9091942), anche per le notizie inattese per gli interessati che potrebbero derivarne, il cui trattamento deve essere effettuato in conformità a specifiche disposizioni (art. 8 delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica all. A5 al Codice, prescrizioni relative al trattamento dei dati genetici, all. 4 al provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali 5 giugno 2019, n. 146 (doc. web n. 9124510, punto 4.3).

Il Garante ha evidenziato poi come la prospettata nomina di un custode, anche di elevato profilo e affidabilità, per la conservazione di una copia della base dati cifrata e delle relative chiavi di *decripting*, non costituisca altro che una misura di sicurezza e di minimizzazione dei dati da svolgersi comunque nel rispetto degli ulteriori principi e obblighi previsti dal RGPD (artt. 5, par. 1, lett. *a*) e 2, 6, 9, 24 e 28 del RGPD).

Con riguardo a eventuali trattamenti ulteriori rispetto allo studio oggetto del parere per rinnovati scopi di ricerca scientifica, il Garante ha evidenziato che spetta al titolare, in omaggio al principio di responsabilizzazione, verificare la sussistenza di idonei presupposti giuridici anche alla luce delle indicazioni del Garante europeo e dal Cepd (artt. 5, 24 e 25 del RGPD; cfr. parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati, del 23 gennaio 2019 del Cepd; *A preliminary Opinion on data protection and scientific research*" del 6 gennaio 2020, del Garante europeo; *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, del 2 febbraio 2021 del Cepd; provv. 1° novembre 2021, doc. web n. 9731827). Il Garante ha espresso quindi parere favorevole ponendo al titolare le condizioni sopra richiamate (provv. 24 novembre 2022, n. 402, doc. web n. 9842737).

6.2. *Trattamenti di dati personali per scopi di ricerca medica in ambito Covid-19*

L'Ufficio ha concluso l'istruttoria preliminare in relazione ad alcune notizie di stampa relative ad un *memoradum* di collaborazione tra l'Istituto nazionale per le

malattie infettive, San Lazzaro Spallanzani (Inmi) e il Centro nazionale russo di ricerca epidemiologica e microbiologica Gamaleya, per lo studio del vaccino Sputnik, anche attraverso uno scambio di informazioni e materiali biologici e con il coinvolgimento *in loco* di ricercatrici russe. Nell'attività istruttoria è emerso che l'Istituto, sulla base del consenso delle persone interessate, aveva svolto un progetto di ricerca per il trattamento di dati sulla salute e campioni biologici di circa 900 volontari in forma pseudonimizzata, ponendo specifici limiti di accesso alle ricercatrici russe ai richiamati dati (art. 2-*quaterdecies* del Codice; 17-*bis*, comma 4, d.l. 17 marzo 2020 n. 18, recante misure di potenziamento del servizio sanitario nazionale e di sostegno economico per le famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da Covid-19 convertito con modificazioni dalla l. 24 aprile 2020, n. 27). In particolare, le ricercatrici del Centro di ricerca Gamaleya avevano operato presso l'Inmi, nel rispetto dei ruoli e degli accordi sottoscritti nel *memorandum* e nessun campione era stato inviato presso laboratori terzi diversi da quelli dell'Inmi. Alla luce della documentazione in atti e delle dichiarazioni rese dagli enti, l'Ufficio non ha ravvisato gli estremi di una violazione in materia di protezione dei dati personali (art. 11, reg. Garante n. 1/2019 del 4 aprile 2019) (nota 29 settembre 2022).

6.3. *Comunicazioni ai sensi dell'art. 2*-ter*, comma 3, del Codice*

Una regione ha inviato al Garante una notizia di comunicazione di dati personali, diversi da quelli di cui agli artt. 9 e 10 del RGPD (cd. dati comuni), non prevista da una norma di legge o di regolamento o da atti amministrativi generali, richiesti dal Consiglio per la ricerca in agricoltura (Crea) per effettuare studi sulle aziende agricole che ricevono misure di sostegno a favore dell'agricoltura biologica ivi compreso il Codice unico azienda agricola di identificazione delle aziende agricole (Cuaa), funzionale ai rapporti con la p.a., ai sensi dell'art. 1, comma 2, d.P.R. n. 503/99 e che in molti casi è costituito dal codice fiscale dell'imprenditore agricolo.

È altresì emerso che il Crea, nell'ambito della verifica delle attività della Rete rurale nazionale (v. reg. (UE) 1305/2013), stava realizzando alcune attività di analisi e valutazione delle politiche a favore dell'agricoltura biologica tra le quali lo studio del profilo delle aziende agricole che ricevono il sostegno per verificare se siano più sostenibili dal punto di vista ambientale ed economico di quelle che non lo ricevono.

Al riguardo l'Ufficio ha preso atto della notizia pervenuta ed ha tenuto conto che la raccolta e il successivo trattamento di dati personali relativi al Cuaa costituisce una operazione di trattamento pertinente e non eccedente rispetto alle specifiche finalità perseguite dal Crea nell'ambito dei compiti istituzionali ad esso attribuiti in attuazione del reg. (UE) n. 1305/2013. Ha osservato, altresì, che il trattamento di dati personali per scopi di ricerca scientifica deve essere svolto nel rispetto, non solo del RGPD (cfr. in particolare art. 89) e del Codice (cfr. artt. 104 e ss.) ma anche sulla base di uno specifico progetto di ricerca secondo quanto previsto dalle richiamate regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, all. A5 al Codice (cfr. art. 2- *quater* del Codice) (nota 16 novembre 2022).

Si menziona altresì un'istanza di consultazione preventiva ai sensi dell'art. 110 del Codice e dell'art. 36 del RGPD, per la realizzazione di un progetto di ricerca di rete finalizzata, promosso dal Ministero della salute e presentato da alcuni professori dell'Istituto nazionale di ricovero e cura per anziani (Inrca). A tale riguardo, l'Ufficio, in conformità all'art. 110 del Codice ha rimarcato che spetta all'Inrca, in qualità di titolare del trattamento, valutare se il progetto di ricerca indicato

corrisponda a quelli per i quali non è necessario acquisire il consenso degli interessati al trattamento dei dati personali, in quanto rientrante tra quelli previsti dall'art. 12-*bis*, d.lgs. 30 dicembre 1992, n. 502 e che, qualora ricorra tale condizione, l'Istituto è tenuto a svolgere e pubblicare la valutazione d'impatto unitamente a tutti gli altri adempimenti comunque previsti dal RGPD (nota 6 dicembre 2022).

Con provvedimento 7 aprile 2022, n. 136 (doc. web n. 9773977) il Garante ha fornito parere favorevole, seppur a specifiche condizioni, sullo schema di decreto, presentato dal Ministero della salute, relativo all'istituzione del Registro nazionale dei tumori (artt. 36, par. 4, 57, par. 1, lett. *c*), del RGPD, dell'art. 12, comma 13, d.l. del 18 ottobre 2012, n. 179, come da ultimo modificato con il d.l. 27 gennaio 2022, n. 4 e dell'art. 6 del d.P.C.M. 3 marzo 2017).

Il testo istituisce, presso il predetto Dicastero, un archivio contenente i dati personali della popolazione affetta da patologie neoplastiche di cui al d.P.C.M. 3 marzo 2017; titolare del trattamento dei dati personali è il Ministero della salute e un comitato tecnico scientifico, deputato a fornire supporto gestionale, è nominato responsabile del trattamento (v. art. 28 del RGPD). Inoltre i centri di riferimento regionali e delle province autonome avrebbero accesso ai dati in forma aggregata riferiti ai propri residenti e ai residenti delle altre regioni o province autonome, per fini comparativi e di programmazione sanitaria.

Lo schema di decreto si compone altresì di un disciplinare tecnico recante l'indicazione delle misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio del trattamento.

Il Registro è alimentato ad opera del centro di riferimento regionale e delle province autonome, con cadenza annuale, dai registri dei tumori delle regioni e delle province autonome a loro volta alimentati da fonti indicate nello schema di decreto con dati riferiti ai relativi pazienti, indipendentemente dalla residenza. I dati sono trasmessi in forma codificata al fine di non consentire l'identificazione diretta degli interessati.

Nel Registro i dati sono conservati per 120 anni dal decesso dell'interessato, ma qualora il decesso dell'interessato non sia tracciato nel Registro nazionale tumori, sono comunque cancellati trascorsi 150 anni dal loro inserimento.

Lo schema di decreto trasmesso ha tenuto conto delle indicazioni rese dall'Ufficio nell'ambito di interlocuzioni informali e di carattere tecnico intercorse con il Ministero relative, tra l'altro: ai richiami normativi contenuti nel preambolo ai fini della corretta individuazione della disciplina, di rango primario, di riferimento e, segnatamente, all'esatta individuazione delle finalità sottese al Registro; alle definizioni; al rispetto dei principi di responsabilizzazione e di minimizzazione dei dati nella fase di accesso ai dati contenuti nel Registro da parte dei soggetti legittimati; all'approccio alla sicurezza sottesa ai trattamenti, ai sensi dell'art. 32 del RGPD, con i connessi obblighi di adozione di misure adeguate rispetto al rischio implicato dal trattamento, nonché di periodica verifica di tale adeguatezza.

Il Garante ha ritenuto inconferente il riferimento alla raccolta dei dati dagli archivi dei programmi di *screening* e attraverso il Fse.

Con riguardo ai dati del Fse, ha considerato che i dati e i documenti in esso accessibili coincidono con quelli già detenuti presso le banche dati e che, anche alla luce dei recenti interventi normativi (d.l. n. 4/2022), il Ministero della salute può trattare i dati, per finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico esclusivamente senza l'utilizzo dei dati identificativi degli assistiti e secondo livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati definiti, con il decreto di cui all'art. 12, comma 7, d.l. n. 179/2012, ovvero con il d.P.C.M. n. 178/2015 che, allo stato, non prevede tale trattamento. A ciò

6

si aggiunga che, fermo restando il diritto di oscuramento esercitabile da parte dell'interessato sui dati accessibili attraverso il Fse (art. 9, d.P.C.M. n. 178/2015), l'attuale disciplina prevede in ogni caso che il trattamento di tali dati per finalità di ricerca sia effettuato in conformità a quanto previsto dall'art. 110 del Codice e quindi sulla base di presupposti di liceità diversi da quelli applicabili al trattamento dei dati esame.

Da un punto di vista tecnico, infine, il Garante ha richiesto, in particolare, che per gli accessi al Registro si faccia riferimento all'obbligo di procedure di autenticazione a più fattori. Inoltre, nelle more della definizione del quadro di garanzie e regole delle identità Spid a uso professionale, nel caso di utilizzo di identità Spid a uso personale, occorrerebbe escludere la raccolta di dati personali attinenti alla sfera privata del dipendente (es. *e-mail* e numero di cellulare personale, domicilio privato) forniti ai *service provider* (provv. 24 febbraio 2022, n. 75, doc. web n. 9751939).

7 La statistica

7.1. *La statistica ufficiale*

L'Istat ha richiesto il parere di competenza del Garante sullo schema di Programma statistico nazionale 2020-2022, Aggiornamento 2022 (Psn o Programma), ai sensi dell'art. 6-*bis*, comma 1-*bis*, d.lgs. n. 322/1989 e dell'art. 4-*bis* delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistan, all. A.4 al Codice. Come per il Psn 2020-2022, aggiornamento 2021-2022, l'Istituto ha previsto che, prima dell'indicazione dei lavori statistici di titolarità dei diversi soggetti Sistan, siano indicate le misure tecniche e organizzative implementate da ciascuno di essi. Nel parere 30 giugno 2022, n. 237, (doc. web n. 9794929), il Garante ha in primo luogo formulato specifiche osservazioni ed evidenziato talune criticità che possono anche essere di ausilio per i singoli titolari del trattamento tenuti alla compilazione dei prospetti informativi relativi ai lavori statistici, anche ribadendo quanto già rappresentato dal Garante nel parere reso sullo schema di Psn 2020-2022, aggiornamento 2021-2022, (provv. 16 settembre 2021, n. 315, doc. web n. 9717477). Infatti, persiste nella maggior parte delle sezioni denominate misure di sicurezza, compilate da ciascuna amministrazione titolare dei trattamenti statistici inseriti nel Psn, la descrizione in termini del tutto generali delle misure tecniche e organizzative implementate dal titolare a seguito dell'entrata in vigore del Regolamento, senza, nella maggior parte dei casi, l'indicazione delle garanzie adeguate per i diritti e le libertà degli interessati adottate, con particolare riferimento alle misure tecniche e organizzative volte a garantire il rispetto del principio di minimizzazione nell'ambito dei trattamenti per scopi statistici menzionati nel Psn (art. 89 del RGPD).

Il Garante ha inoltre evidenziato le principali criticità in relazione a taluni specifici lavori statistici, sottolineando come la formulazione del previsto parere non esaurisce i poteri di indagine dell'Autorità. In via preliminare, il Garante ha rappresentato che il lavoro statistico ALM-00001: razionalizzazione e valorizzazione delle indagini sugli esiti occupazionali dei laureati, al fine di realizzare una base-dati integrata sul tema dell'istruzione universitaria riproposto nel Psn in esame deve intendersi ancora sospeso, tenuto conto dell'istruttoria ancora pendente, dalla quale è emersa la persistenza di molteplici criticità relative, in particolare, all'effettiva applicazione dei principi di liceità e trasparenza.

Il Garante ha poi sospeso il lavoro statistico EMR-00028 volto ad analizzare le caratteristiche socio-demografiche e tipologiche della clientela che soggiorna negli esercizi ricettivi (alberghieri e complementari) della regione, tenuto conto che, *prima facie* le strutture recettive non appaiono tenute ad acquisire tutte le informazioni indicate nel prospetto informativo.

In relazione ai lavori statistici IST-02493: Sistema integrato censimento permanente e indagini sociali, componente areale e IST-02494: Sistema integrato censimento permanente e indagini sociali, componente da lista, il Garante ha prescritto che non vengano utilizzati dati provenienti da abbonamenti ferroviari e bus del gruppo Ferrovie dello Stato raccolti presso il Mef; abbonamenti ferroviari gruppo Italo, raccolti presso Italo spa; abbonamenti Telepass raccolti presso

Telepass spa-gruppo Atlantia; traffico ferroviario viaggiatori provenienti dal lavoro statistico FES-00018 (questi ultimi limitatamente al lavoro IST-02493) e vengano conseguentemente modificati i relativi prospetti informativi, in quanto il Mef, il gruppo Italo spa, il gruppo Telepass spa e i lavori statistici di titolarità delle Ferrovie dello Stato non sono indicati, né dalla legge di bilancio del 27 dicembre 2017 n. 205 (art. 228) né dal Piano generale di censimento come fonti impiegabili a fini censuari. Da una prospettiva sostanziale è stato poi rilevato che il trattamento di informazioni relative agli spostamenti sul territorio determina un'ingerenza particolarmente invasiva nella vita privata degli interessati, rilevante anche sulla libertà di movimento (art. 16 Cost.). Inoltre, l'accesso di un'articolazione dello Stato a dati personali gestiti *iure privatorum*, quali quelli relativi ai detti abbonamenti potrebbe risultare del tutto imprevedibile per gli interessati e sproporzionato, se non corroborato da specifiche misure di trasparenza e bilanciamento. Nel caso specifico, l'eccedenza delle informazioni si accentua alla luce della crescente numerosità di banche dati impiegata per scopi statistico censuari come già rilevato nel provvedimento 16 dicembre 2021, n. 434 (doc. web n. 9738899) (art. 5, par. 1, lett. *c*), del RGPD).

Il Garante ha poi sospeso il lavoro statistico IST-02629: Sviluppo di indicatori di morbosità diagnosticata volto ad identificare le principali fonti informative e banche dati che offrano la possibilità di calcolare stime di incidenza e prevalenza di malattie, traumatismi e cause esterne, tramite una procedura di interconnessione delle fonti NSIS effettuata dal Ministero della salute ai fini dello studio delle coorti di riferimento per le varie patologie. Per la realizzazione del lavoro è previsto l'utilizzo in particolare, delle LAC (IST-02492: Rilevazione delle liste anagrafiche comunali) nell'ambito delle quali gli interessati sono identificati attraverso il codice SIM, generato a partire dal codice fiscale degli interessati. Ciò premesso, atteso che i dati contenuti nel nuovo sistema informativo del Ministero della salute (NSIS) sono privi del codice fiscale dell'assistito, non appare chiaro come i dati provenienti da queste due fonti possano essere messi in correlazione.

Il Garante ha pertanto sospeso il lavoro al fine di avviare un'istruttoria preliminare, volta a verificare, anche alla luce della valutazione di impatto svolta ai sensi dell'art. 35 del RGPD, la correttezza dei trattamenti di dati personali svolti in tale ambito e la conformità alla disciplina di settore, con specifico riferimento all'applicazione delle tecniche di pseudonimizzazione e dei limiti entro i quali il Ministero della salute può trattare i dati contenuti nel NSIS (v. d.m. n. 262/2016, artt. 2 e 3).

Il Garante ha poi ribadito la sospensione del lavoro ISS-00053: Osservatorio epidemiologico sui suicidi e tentativi di suicidio riproposto nel Psn in esame, rispetto al quale è tuttora in corso una specifica istruttoria (cfr. provv.ti 9 maggio 2018, n. 271, doc. web n. 9001732; 13 febbraio 2020, n. 29, doc. web n. 9283929 e 10 dicembre 2020, n. 261, doc. web n. 9520567). La principale criticità rilevata in riferimento a tale lavoro statistico concerne la possibilità di interconnettere dati contenuti nei flussi del nuovo sistema informativo del Ministero dalla salute, che il Dicastero detiene in forma pseudonimizzata, con dati provenienti da fonti esterne a tale sistema, utilizzando come chiave di *record linkage* il codice fiscale, non presente nel NSIS; ciò a detrimento dell'efficacia e della robustezza delle misure di pseudonimizzazione implementate ai sensi del sopra richiamato d.m. n. 262/2016.

Rileva poi il lavoro IST-02832: Prestazioni sanitarie ambulatoriali e farmaci erogati dal Ssn (descritto come evoluzione dello studio progettuale IST-02776), volto tra l'altro a monitorare l'erogazione di prestazioni del Ssn per le valutazioni statistiche sulle condizioni di salute della popolazione e il funzionamento dei servizi, in relazione ai bisogni di cure e di assistenza dei cittadini. Per la realizzazione del lavoro, l'Istituto intenderebbe acquisire presso il Mef, indicato come titolare del

trattamento, informazioni relative a prestazioni sanitarie ambulatoriali (visite mediche, test diagnostici e di laboratorio) e farmaci. A tale riguardo, il Garante ha ribadito che il Mef, qualora non rivesta il ruolo di titolare in riferimento alle informazioni che sono trattate attraverso il Sistema TS, può conservare le stesse solo per il tempo strettamente necessario al completamento delle operazioni di comunicazione e verifica, cancellandole irreversibilmente al termine delle predette operazioni (cfr. decreto Mef 27 luglio 2005 con riferimento alle ricette e l´art. 50, comma 10, d.l. n. 269/2003; provv. 26 luglio 2017, n. 339, doc. web n. 6930323). Il Garante ha pertanto ritenuto necessario che l'Istat verifichi il ruolo del Mef in relazione ai dati oggetto di trattamento nel lavoro in esame e, di conseguenza, aggiorni il relativo prospetto informativo (artt. 24 o 28 del RGPD).

Il lavoro statistico IST-00220: Indagine sull'inserimento professionale dei laureati prevede l'utilizzo di dati provenienti da altri trattamenti statistici, tra i quali: Indagine Almalaurea sulla condizione occupazionale dei laureati a dieci anni dal titolo ALM-00003 e l'utilizzo di liste di partenza tra cui quelle MUR-00026 istruzione universitaria (I-II-III ciclo), che risultano sospesi con il provvedimento 13 febbraio 2020, n. 29, (doc. web n. 9283929) e sui quali l'Ufficio è in attesa di riscontri da parte dei rispettivi titolari del trattamento. Pertanto è stato evidenziato che i dati relativi a tali lavori non possono essere utilizzati neanche per la realizzazione del lavoro statistico in esame.

L'attenzione del Garante si è poi concentrata sugli studi longitudinali sulle disuguaglianze di salute determinate da differenze socio-economiche di titolarità di otto regioni /provincie autonome volti a individuare e valutare, eventuali differenze di salute tra gruppi di popolazione con diversa condizione demografica, socio-economica e ambientale e a fornire indicazioni per programmare idonei interventi. Tenuto conto in particolare che gli studi in esame prevedono il trattamento su larga scala di dati relativi alla salute nonché della necessità di approfondire i profili relativi alle misure di pseudonimizzazione, l'Autorità ha avviato una specifica istruttoria al fine di verificare la conformità alla disciplina vigente in materia di protezione dei dati personali, con particolare riferimento alle relative valutazioni di impatto redatte ai sensi dell'art. 35 del RGPD (cfr. parere 16 settembre 2021, n. 315, doc. web n. 9717477). In sede istruttoria sono state in particolare chiarite le tecniche di pseudonimizzazione implementate, con la specificazione che i codici pseudonimi attribuiti per la realizzazione dei lavori statistici non solo non coincidono con quelli di cui al d.m. n. 262/2016 ma neanche, in fase di elaborazione dei dati, con quelli attribuiti nell'ambito dei sistemi informativi sanitari regionali o anagrafici. Inoltre, a seguito degli specifici chiarimenti resi all'Ufficio, è stato definito il tempo di conservazione dei dati pari a 20 anni, vista la natura longitudinale di tali lavori statistici. È stata pertanto disposta l'archiviazione senza l'adozione di specifici provvedimenti correttivi o sanzionatori da parte del Collegio (v. artt. 11 e 14, reg. Garante n. 1/2019 del 4 aprile 2019).

7.2. *Istruttorie relative ai lavori statistici del Psn*

Con il parere 9 giugno 2022, n. 235, il Garante ha concluso l'istruttoria di due lavori statistici, denominati rispettivamente IST 02834-Studio dei *Mobile Network Data* a fini statistici e IST 02829-La violenza raccontata dai *social* (doc. web n. 9802796).

Il primo è una rivisitazione del lavoro statistico IST-02589-Uso a fini statistici dei *big data*, sospeso con parere 9 maggio 2018, n. 271, (doc. web n. 9001732), relativo a

7

una sperimentazione che, attraverso l'utilizzo di dati derivanti dai servizi di telefonia mobile ha come finalità la stima di: (i) indicatori di popolazione (popolazione residente, popolazione abitualmente dimorante, popolazione insistente) e di flussi di spostamento (ad es. matrice del pendolarismo, trasfrontalieri); (ii) misura di indicatori SDG (*Sustainable Development Goals*); (iii) flussi turistici *inbound* (stranieri che viaggiano in Italia) e *domestic* (residenti in Italia che viaggiano sul territorio nazionale).

In via preliminare, il Garante, nell'aderire alla posizione di Eurostat e di ESS (Sistema statistico europeo) che sottolineano, nel dibattito comunitario, la necessità, comprovata e urgente, di utilizzare i cd. *big data* per una produzione statistica adeguata al contesto storico di riferimento, ha evidenziato come non si possa prescindere da una disciplina omogenea a livello europeo che tenga anche conto delle rilevanti implicazioni sui diritti e le libertà fondamentali degli interessati, in linea con quanto stabilito dalla Carta dei diritti fondamentali dell'Unione europea e dal RGPD.

Sotto altro profilo, il Garante ha rappresentato di aver già avuto modo di esprimersi in merito all'uso di dati provenienti da fonti private, in particolare dai consumi energetici per scopi censuari, sottolineando come l'intromissione nella dimensione più intima e privata degli individui, ossia quella domestica, esiga che vengano individuate specifiche misure a tutela degli interessati anche per prevenire violazioni del divieto di ricadute amministrative (cfr. parere sullo schema di protocollo di intesa tra Istituto nazionale di statistica e Acquirente Unico spa, per la regolamentazione dell'acquisizione da parte di Istat dei dati sui consumi di energia elettrica e gas, del 16 dicembre 2021, n. 434, doc. web n. 9738899). Ha pertanto ribadito la necessità – in vista della sistematizzazione dell'uso dai dati *Business-to-Government* nel panorama delle fonti utilizzabili per scopi di statistica ufficiale –, di individuare a livello comunitario garanzie adeguate a salvaguardare la legittima pretesa di riservatezza vantata da ogni individuo (inteso come utente/contraente) rispetto ad indebite ingerenze dello Stato nella sua vita privata. Al riguardo, infatti, se ben può riconoscersi una certa prevedibilità che dati amministrativi siano ulteriormente utilizzati dalle diverse articolazioni statali per scopi statistici, l'accesso dello stesso a dati personali gestiti *iure privatorum*, inerenti aspetti particolarmente intimi della vita degli interessati (come le comunicazioni personali e gli spostamenti sul territorio) potrebbe risultare del tutto imprevedibile e sproporzionato, se non corroborato da specifiche misure di trasparenza e bilanciamento.

Il lavoro statistico in esame va pertanto considerato come una preliminare sperimentazione di queste nuove modalità di realizzazione della statistica. Poste tali premesse, il Garante ha ritenuto che l'Istituto abbia da una parte motivato la necessità di sperimentare l'uso dei dati di telefonia mobile a fini di statistica ufficiale, alla luce delle tempestività informativa che i cd. *real world data* sono capaci di assicurare e dell'apporto che gli stessi possono fornire alla qualità dell'informazione statistica in termini di accuratezza, con ciò assicurando ai decisori pubblici la possibilità di ancorare le proprie scelte sulla base di dati più aggiornati e aderenti alla realtà fattuale. Dall'altra, anche la proporzionalità del trattamento è risultata motivata viste le misure implementate da Istat per ridurre il rischio di reidentificazione degli interessati.

Il lavoro statistico denominato "La violenza raccontata sui *social*" si pone l'obiettivo di utilizzare i messaggi veicolati dai *social* Twitter, Facebook e Instagram e rassegna stampa Web per valutare, attraverso un'analisi di tipo *opinion mining*, il fenomeno della violenza di genere e la presenza di stereotipi. In particolare, si vuole restituire un indice di positività o negatività del fenomeno e cogliere la sua stessa

evoluzione attraverso i *social* (come, ad es., nelle forme peggiori il cyberbullismo e il *bodyshaming*) al fine di monitorarne le sue diverse forme digitali.

La rilevazione riguarda la definizione di una piattaforma (denominata Iride) che acquisisce e classifica in tempo reale i messaggi *social* raccogliendo i contenuti pubblici dalle fonti Twitter, Facebook e Instagram e Rassegna stampa Web, afferenti a violenza di genere, e stereotipi di genere e linguaggio di odio. La metodologia consiste nell'addestrare un algoritmo sulla base della taggatura, ovvero attribuendo un valore (positivo, negativo o neutro) e una *emotion* (amore, gioia, sorpresa, rabbia, tristezza, paura, neutro), a un *set* di conversazioni su cui la macchina è stata addestrata. L'Istat a tal fine acquisisce tramite le API (*Application Programming Interface*), messe a disposizione dai *social network* selezionati, il contenuto testuale del messaggio e come metadato, l'informazione temporale ad esso associata. I messaggi vengono classificati e aggregati, con supervisione umana, a livello giornaliero, in *tweet* negativi, *tweet* neutri e *tweet* positivi, per un totale di circa 105 messaggi al giorno, al fine di ottenere un algoritmo che riproduce le decisioni umane, con un margine d'errore fissato.

È stato altresì chiarito che "il modello prodotto dagli annotatori umani, [...], viene usato per addestrare il modello BERT (*Bidirectional Encoder Representations from Transformers*), facente parte della piattaforma Iride, con l'obiettivo di far lavorare l'algoritmo creato ai fini della classificazione al posto degli umani; questi possono comunque sempre intervenire per modificare eventuali distorsioni [...]".

Con riguardo all'uso dei dati identificativi degli interessati desumibili da Url e *@account* degli utenti, Istat ha chiarito che le "API sono pubbliche e non è prevista da parte dei social *network*, che rendono disponibili gratuitamente i contenuti pubblici postati dagli utenti, alcuna forma di anonimizzazione o di pseudonimizzazione o di cifratura di tali dati (che è quindi un onere di chi ne fruisce)". Sotto altro profilo è stato chiarito che "il motivo per cui Istat acquisisce anche *account* e Url (ossia dati personali) è per garantire l'accuratezza, l'esattezza e l'integrità del dato statistico [...]".

Con il citato parere il Garante ha osservato che l'Istituto ha motivato sia la necessità che la proporzionalità dei trattamenti inerenti al lavoro statistico in esame. Con specifico riferimento alla proporzionalità è stato evidenziato che il lavoro statistico non è volto a profilare l'autore del messaggio, ma ad intercettare la dimensione del fenomeno attraverso la restituzione di indici di positività o negatività. Ciò che rileva nell'analisi è unicamente l'occorrenza, eventualmente congiunta, dei termini chiave prescelti dall'Istituto, senza effettuare alcun monitoraggio individuale del comportamento degli utenti nella libera espressione del loro pensiero. Infatti, il lavoro non prevede alcuna classificazione degli utenti quali utenti maggiormente attivi tra istituzioni, *opinion leaders*, utenti comuni. Il Garante ha inoltre accolto con favore l'individuazione di una misura di cifratura (*hashing*) delle informazioni identificative degli interessati per tutto il periodo per il quale l'identità degli stessi non risulta necessaria per lo svolgimento del lavoro. Cionondimeno, al fine di assicurare l'effettiva applicazione del principio di minimizzazione dei dati e conformare la misura implementata allo stato dell'arte tecnologica, si è ritenuto necessario condizionare il parere favorevole a due condizioni: i) che le chiavi di cifratura applicate a *@account* e Url siano aggiornate con una cadenza di 48 ore; ii) tenuto conto della natura sperimentale del lavoro statistico e dell'impiego di tecniche algoritmiche, che l'Istat fornisca un *report* al Garante entro 6 mesi dall'avvio della sperimentazione, indicando in particolare le modalità seguite per addestrare il modello BERT facente parte della citata piattaforma Iride.

7

7.3. Data breach *nell'ambito della statistica ufficiale*

L'Istat ha notificato al Garante, ai sensi dell'art. 33 del RGPD, due violazioni di dati personali, consistite in un attacco informatico che ha comportato l'esfiltrazione di alcune informazioni e il potenziale accesso non autorizzato da parte di terzi a informazioni di carattere personale, fra cui credenziali di autenticazione contenute, rispettivamente, nei portali Coeweb e Indata. In particolare, con riferimento al portale Coeweb la violazione avrebbe causato la potenziale perdita di confidenzialità di dati anagrafici, di contatto, di accesso e identificazione riferiti a circa 27.000 interessati tra dipendenti, consulenti, utenti anche di altri Paesi appartenenti e non allo Spazio economico europeo. A seguito della violazione e per ridurne gli effetti, l'Istat ha immediatamente reso indisponibile il sito e sono state disabilitate tutte le utenze del sistema. Con riferimento al portale Indata, utilizzato per la raccolta dati della rilevazione statistica dei permessi per costruire, la violazione è stata resa pubblica tramite segnalazione del CSIRT-ITA e del CERT-GARR, senza che il titolare riuscisse a identificare il momento dell'attacco.

In entrambi i casi l'Istat ha comunicato la violazione agli interessati attraverso la pubblicazione di uno specifico messaggio in un'apposita pagina di cortesia, ed ha poi adeguato la *privacy policy* dei predetti portali agli *standard* dell'Istituto. Ai sensi degli artt. 58, par. 2, lett. *i*) e 83 del RGPD, il Garante ha al riguardo adottato un provvedimento sanzionatorio (provv. 10 febbraio 2022, n. 46, doc. web n. 9751194).

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

8.1. *Trattamenti in ambito giudiziario*

Attività di investigazione privata

In due casi il Garante ha ammonito ai sensi dell'art. 58, par. 2, lett. *b*), del RGPD uno stesso investigatore privato per avere acquisito dati personali presso l'interessato in assenza di informativa ed averli utilizzati in violazione degli artt. 13 del RGPD e 2-*decies* del Codice. Sulla base dei criteri indicati dall'art. 83 del RGPD, considerato che la condotta aveva esaurito i suoi effetti, che il numero di interessati al trattamento era limitato, che il titolare aveva fornito in sede procedimentale piena collaborazione e che non sussistevano precedenti, il Garante ha ritenuto non sussistenti i presupposti per infliggere una sanzione amministrativa pecuniaria (provv.ti 12 maggio 2022, nn. 186, doc. web n. 9779119 e 187, doc. web n. 9789512).

Produzione di dati in giudizio

Anche nel 2022 l'Autorità ha ricevuto diversi reclami concernenti la conformità alla normativa in materia di protezione di dati personali della produzione di informazioni personali in giudizio. Al riguardo, secondo un consolidato orientamento, i reclami sono stati archiviati per incompetenza del Garante, in quanto spetta al Giudice, ove ritualmente richiesto, valutare la liceità del trattamento in giudizio dei dati personali dell'interessato (cfr. art. 160-*bis* del Codice), tenuto conto, in particolare, che l'utilizzabilità nel processo di atti basati sul trattamento di dati personali illegittimo resta disciplinata dalle pertinenti disposizioni processuali (si vedano i conformi provvedimenti del Garante adottati anche con riferimento all'art. 160, comma 6, del previgente testo del Codice, di contenuto pressoché identico a quello dell'attuale art. 160-*bis*, 23 settembre 2010, doc. web n. 1756065; 4 novembre 2010, doc. web n. 1770943; 17 novembre 2010, doc. web n. 1779765).

Nell'archiviare i reclami in questione, l'Autorità ha sottolineato che la medesima disciplina eurounitaria e codicistica prevede che, al fine di salvaguardare l'indipendenza della magistratura nell'adempimento dei suoi compiti giurisdizionali (cfr. cons. 20 del RGPD), l'autorità di controllo (nella specie, il Garante) non è competente per il controllo dei trattamenti effettuati dalle Autorità giudiziarie nell'esercizio delle loro funzioni (cfr. artt. 55 par. 3, del RGPD e 154, comma 7, Codice).

Tali principi sono stati applicati in diversi casi, fra cui quelli di seguito brevemente descritti.

L'Autorità si è occupata di un reclamo concernente il deposito di una memoria e di documentazione allegata da parte di un avvocato, nell'ambito di un procedimento civile finalizzato alla modifica delle condizioni divorzili, ritenuto dal reclamante gravemente lesivo della propria immagine. L'Autorità ha innanzitutto rilevato che il trattamento dei menzionati dati era avvenuto in occasione dell'istaurazione di un processo e in tali casi spetta al Giudice adito valutare la liceità del trattamento dei dati personali dell'interessato (cfr. art. 160-*bis* Codice). Inoltre il Garante, nell'archiviare il reclamo, ha precisato che la legittimità del trattamento dei dati in tale ambito è assicurata, per le particolari categorie di dati, dall'art. 9, par. 1, lett. *f*), del RGPD, secondo cui il trattamento è lecito se necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali e *a fortiori*, per tutti i dati personali, dall'art. 6, par. 1, lett. *f*), del medesimo RGPD secondo il quale il trattamento è lecito se necessario

per perseguire un interesse legittimo del titolare (tra le altre, note 26 maggio, 12 e 16 settembre 2022).

In altro reclamo l'interessato aveva lamentato che il provvedimento con il quale era stata dichiarata l'apertura di un procedimento di liquidazione dei beni ex art. 14-*ter* della legge n. 3/2012 fosse stato adottato in violazione della normativa in materia di protezione dei dati personali. In particolare, il reclamante aveva contestato che il liquidatore nominato dal tribunale, "nell'esercizio delle sue funzioni", aveva esercitato il diritto di accesso alla documentazione relativa ad una società, in sostituzione del reclamante, socio di minoranza e che il medesimo liquidatore si faceva assistere da un soggetto terzo, consentendo quindi allo stesso di venire a conoscenza della situazione di sovraindebitamento del reclamante e della documentazione riservata. Al riguardo, il Garante ha rappresentato che il trattamento effettuato dal liquidatore è disciplinato dal RGPD e dalle relative disposizioni di adeguamento di cui al Codice, applicabili anche ai trattamenti di dati personali effettuati dall'Autorità giudiziaria nell'esercizio di funzioni giurisdizionali diverse da quelle penali, pur con alcune deroghe previste, in particolare, dagli artt. 23, par. 1, lett. *f*), del RGPD e *2-duodecies* del Codice. In tali casi tuttavia, come già precedentemente dichiarato, l'autorità di controllo (nella specie, il Garante) non è competente sui trattamenti effettuati dalle Autorità giudiziarie nell'esercizio delle loro funzioni, né su quelli svolti da altri soggetti da esse incaricati a vario titolo in funzione ausiliaria, come nel caso di specie il liquidatore, nominato dal tribunale ai sensi dell'art. 14-*ter*, l. n. 3/2012. Pertanto il reclamo è stato archiviato ai sensi dell'art. 11 del reg. del Garante n. 1/2019 (nota 5 settembre 2022).

Analogamente è stato archiviato un altro reclamo concernente l'asserita violazione della disciplina in materia di protezione dati da parte di un avvocato, nominato custode giudiziario in una procedura esecutiva immobiliare in relazione alla quale il reclamante risultava esecutato. Tenuto conto che il custode giudiziario rientra tra gli ausiliari del giudice (artt. 65-67 c.p.c.) ed in applicazione del già citato art. 160-*bis* del Codice, l'Autorità ha rilevato la propria incompetenza a valutare l'eventuale illiceità del trattamento ed ha archiviato il reclamo (note 5 settembre, 17 ottobre, 4 e 8 novembre 2022).

8.2. *Trattamenti da parte di Forze di polizia*

Divulgazione su Facebook di immagini relative a persone in stato di detenzione

L'Autorità ha comminato al Ministero dell'interno, in qualità di titolare del trattamento, due sanzioni amministrative pecuniarie di euro 60.000 e di euro 50.000 per la violazione dell'art. 3, comma 1, lett. *a*), d.lgs. n. 51/2018, a seguito della divulgazione di immagini di persone in stato di detenzione.

Nel primo caso, era stato divulgato sulle pagine Facebook di una questura un video con il quale era stata data notizia dell'arresto di otto persone indagate avvenuto nel febbraio 2015. Tale video, contenente le immagini dei volti associate ai rispettivi nominativi degli indagati, era stato rimosso solo nel dicembre 2020 a seguito dell'avvio dell'istruttoria da parte del Garante (provv. 24 febbraio 2022, n. 61, doc. web n. 9766445).

Nel secondo caso, si era trattato della divulgazione dell'immagine in primo piano dell'interessato, in stato di detenzione carceraria già da qualche mese, da parte di una questura nel corso di una conferenza stampa in cui si dava notizia di un ulteriore provvedimento restrittivo nei confronti del medesimo interessato (provv. 24 febbraio 2022, n. 62, doc. web n. 9766469, cfr. 9.2.1).

Ai trattamenti descritti, effettuati per finalità di polizia, sono risultati applicabili la

direttiva (UE) 2016/680, che nel preambolo richiama la Carta dei diritti fondamentali dell'Unione europea, nonché la Convenzione europea dei diritti dell'uomo (cfr. cons. 1 e 46 direttiva); il d.lgs. n. 51/2018 ed il d.P.R. n. 15/2018 che individua le modalità di attuazione dei principi del Codice relativamente al trattamento dei dati effettuato, per finalità di polizia, da organi, uffici e comandi di polizia (tuttora vigente ai sensi dell'art. 49, d.lgs. n. 51/2018). In entrambi i casi, anche alla luce delle citate disposizioni sovranazionali e della giurisprudenza della Corte EDU e nazionale (cfr. in particolare Cass. civ., sez. III, 6 giugno 2014 n. 12834; Cass. civ., sez. III, 13 maggio 2020 n. 8878, nonché dei precedenti del Garante provv.ti 25 febbraio 2021, n. 76, doc. web n. 9568040; 7 febbraio 2019, n. 38, doc. web n. 9101651; 26 novembre 2003, doc. web n. 1053631; provv. 19 marzo 2003, doc. web n. 1053451), la divulgazione di immagini di persone sottoposte allo stato di detenzione non è risultata necessaria per l'espletamento delle finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali delle autorità competenti (cfr. artt. 3, c. 1, lett. *a*) e 5, d.lgs. n. 51/2018), né è stato dimostrato il contrario dal Ministero (cfr. artt. 3, comma 4, d.lgs. n. 51/2018 e 4, par. 4, direttiva (UE) 2016/680). Per tali ragioni, il trattamento, consistente nella divulgazione dei dati in parola è risultato in violazione degli artt. 3, comma 1, lett. *a*) e *c*); 5, d.lgs. n. 51/2018 e 14 del d.P.R. n. 15/2018.

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

Il Garante ha espresso il parere di competenza, ai sensi degli artt. 36, par. 4, del RGPD e 154, comma 5-*bis*, del Codice, in merito ad uno schema di decreto, non avente natura regolamentare, del Ministro della giustizia riguardante la tenuta, in forma automatizzata, di un registro dei provvedimenti di applicazione delle sanzioni pecuniarie civili ai sensi dell'art. 11, d.lgs. n. 7/2016 (Disposizioni in materia di abrogazione di reati e introduzione di illeciti con sanzioni pecuniarie civili, a norma dell'art. 2, comma 3, l. 28 aprile 2014, n. 67). L'art. 6 del d.lgs. citato, rubricato reiterazione dell'illecito, stabilisce che si ha reiterazione nel caso in cui l'illecito sottoposto a sanzione pecuniaria civile sia compiuto entro quattro anni dalla commissione, da parte dello stesso soggetto, di un'altra violazione sottoposta a sanzione pecuniaria civile, che sia della stessa indole e che sia stata accertata con provvedimento esecutivo. L'art. 11 del d.lgs., rubricato registro informatizzato dei provvedimenti in materia di sanzioni pecuniarie, stabilisce che con apposito decreto del Ministro della giustizia sono adottate le disposizioni relative alla tenuta di un registro, in forma automatizzata, in cui sono iscritti i provvedimenti di applicazione delle sanzioni pecuniarie civili, per gli effetti di cui all'art. 6. Il Garante ha espresso parere favorevole sullo schema di decreto, ad alcune condizioni ovvero la previsione di un termine di conservazione delle iscrizioni nel registro conforme al principio della limitazione della conservazione rispetto alla finalità del trattamento perseguita (art. 5, par. 1, lett. *e*), del RGPD) nonché l'individuazione di specifiche garanzie al fine di agevolare l'esercizio dei diritti da parte degli interessati. Nello stesso parere, il Garante ha invitato l'Amministrazione a valutare l'adozione di un sistema automatico di cancellazione dei dati allo scadere del termine di conservazione previsto, nonché la sottoposizione al parere del Garante del provvedimento del direttore della Direzione generale per i sistemi informativi automatizzati del Ministero della giustizia, a cui rinvia l'art. 2, comma 2, dello schema per l'adozione delle regole tecniche (provv. 6 ottobre 2022, n. 315, doc. web n. 9821538).

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

A seguito di segnalazioni ricevute, anche nel 2022 l'Autorità, nei limiti delle proprie competenze, ha assicurato il riscontro da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e di uffici periferici della Polizia di Stato alle richieste degli interessati, sia di accesso e comunicazione dei dati conservati presso il Ced, sia di eventuale rettifica dei dati medesimi, nel rispetto delle disposizioni previste dall'art. 10 della legge 1° aprile 1981, n. 121, come modificato dall'art. 175 del Codice.

8.5. *Il controllo sul Sistema di informazione Schengen*

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

8.5.1. Follow up *della valutazione Schengen dell'Italia*

Con riferimento alle raccomandazioni della Commissione risultanti dalla valutazione Schengen dell'Italia tenutasi nel 2021, l'Autorità ha svolto una attività ispettiva (18-19 novembre e 22 dicembre), nell'ambito dei controlli quadriennali previsti dall'art. 55 del reg. (UE) 2018/1861 riguardante "l'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006".

I soggetti destinatari delle attività di verifica, sono stati individuati facendo riferimento all'elenco dei soggetti istituzionali indicati dalla Commissione europea, ai sensi dell'art. 7 del citato regolamento (ufficio NSIS, ufficio SIRENE, uffici della Polizia di frontiera, uffici immigrazione delle questure).

Tale attività è stata svolta in relazione alle valutazioni, contenute nel *report* relativo alla valutazione del 2021, le quali, per quanto riguarda la parte di competenza dell'Autorità, sono state di conformità, pur richiedendo alcuni miglioramenti (*compliant but improvement necessary*).

Al riguardo, occorre tenere presente che la Commissione considera necessaria la predisposizione di regolari attività di ispezione presso le strutture sopra nominate e di analisi dei cd. *log file*, che insieme assicurano l'espletamento del monitoraggio a cui è tenuta l'Autorità in suddetta materia. Con riguardo alle attività di *audit* sui dati trattati dall'NSIS, il *team* di valutazione, pur riconoscendo che l'Autorità aveva iniziato a svolgere detta attività nel luglio del 2017, proseguendola con interlocuzioni varie fino all'ottobre-novembre 2018, ha tuttavia rilevato come la medesima non fosse stata ancora completata ed ha quindi esortato l'Autorità a portarla a compimento al cessare dell'emergenza pandemica. Per quanto sopra esposto, sul punto la valutazione è stata *non-compliant in relation to carrying out the audit*.

L'attività ispettiva è stata svolta presso l'ufficio nazionale SIS II della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza del

Ministero dell'interno, nonché presso l'ufficio di Polizia di frontiera presso l'Aeroporto internazionale di Fiumicino, con particolare riguardo alla verifica della legittimità del trattamento dei dati contenuti nel sistema ed al controllo dei relativi *log file*.

La valutazione delle risultanze di detta attività è in programma nei primi mesi del 2023.

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

Come noto, il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nel SIS II, in virtù dei quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale dell'archivio Schengen, ossia al Dipartimento della pubblica sicurezza (cd. accesso diretto).

Al riguardo, il Ministero invia trimestralmente *report* statistici, privi di dati di natura personale, contenenti informazioni di dettaglio (nazionalità dei richiedenti, questure coinvolte, tipologia delle richieste, ecc.), idonee a monitorare il flusso delle istanze degli interessati e la conseguente attività di riscontro compiuta dalla Divisione NSIS, in conformità con la raccomandazione formulata all'esito della precedente valutazione sull'applicazione dell'*acquis* di Schengen.

Tali *report* sono strumentali alla finalità istituzionale del Garante di assicurare il controllo e il monitoraggio del Sistema, con particolare riguardo all'esercizio dei diritti degli interessati ai sensi dei regolamenti (CE) 1861/2018 e 1862/2018.

Nel corso del 2022, si è assistito ad un parziale aumento del numero delle richieste degli interessati indirizzate direttamente al Garante rispetto all'anno precedente; tra queste poi sono risultate costanti in termini percentuali quelle che lamentano un insoddisfacente o erroneo riscontro alle proprie richieste da parte dell'autorità nazionale di polizia e, pertanto, ricorrono al Garante al fine di vederle soddisfatte.

Infine, si è assistito ad un moderato ma costante calo delle richieste di accesso da autorità nazionali di controllo di altri Stati UE, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane.

Le relative informazioni vengono comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni di cui all'art. 57 del regolamento (CE) 1861/2018 ed all'art. 71 del regolamento (CE) 1862/2018.

9 L'attività giornalistica

Le tematiche legate alla libertà di manifestazione del pensiero e al suo rapporto con il diritto alla protezione dei dati personali e all'identità personale hanno continuato ad essere oggetto di particolare attenzione da parte dell'Autorità, anche nel periodo di riferimento. Ciò, anche in considerazione del rilevante numero di reclami e segnalazioni, con i quali è stata lamentata dagli interessati una violazione dei propri diritti a seguito della diffusione, anche *online*, di notizie da parte degli organi di informazione e dei *social media*.

9.1. *Dati statistici ed aspetti procedurali*

Le istanze rivolte all'Autorità nell'ambito indicato sono pervenute in prevalenza sotto forma di reclami, per i quali in diversi casi è stato necessario richiedere la regolarizzazione in quanto carenti dei necessari presupposti di forma e di sostanza indicati dalla normativa di riferimento. In circostanze frequenti, in cui è stata chiesta la regolarizzazione, si è trattato di reclami in materia di esercizio dei diritti di cui agli artt. 15-22 del RGPD, rispetto ai quali risultava assente il preventivo interpello dell'interessato al titolare del trattamento, richiesto dall'art. 15 del reg. del Garante n. 1/2019. Un numero significativo di istanze è pervenuto anche sotto forma di segnalazioni, parte delle quali hanno dato vita, a seguito di una valutazione preliminare, all'avvio di un'istruttoria, secondo la procedura dei reclami, essendo stata ravvisata la sussistenza dei presupposti di una possibile violazione di legge.

Diverse sono state anche le istanze di natura mista (atti di diffida e/o interpelli preventivi destinati in via diretta ai titolari del trattamento ed inviati all'Autorità per conoscenza), nonché segnalazioni provenienti dall'Autorità giudiziaria e riguardanti notizie di reato aventi una supposta rilevanza anche in materia di protezione dei dati personali.

Una parte rilevante dei reclami definiti nell'anno di riferimento ha riguardato le istanze rivolte ai gestori dei motori di ricerca, – in particolare, per rilevanza e numero di casi, Google – dirette ad ottenere la deindicizzazione di contenuti reperibili in associazione al nominativo dell'interessato (cd. *delisting*). Non mancano casi coinvolgenti altri motori di ricerca quali Microsoft Corporation e Verizon Media Emea Limited, titolare del motore di ricerca Yahoo!.

Una parte ugualmente rilevante dei reclami ha interessato gli organi di informazione (testate giornalistiche in senso stretto, *blog*, siti di informazione ecc.). Le doglianze degli interessati hanno riguardato principalmente la pubblicazione di articoli (ma anche commenti ed *e-book*) contenenti dati personali ritenuti eccedenti (in particolare rispetto al principio di essenzialità dell'informazione nei trattamenti per fini giornalistici) o diffusi in violazione di specifici limiti, soprattutto con riguardo a dati relativi alla salute (in alcune ipotesi in quanto connessi alla diagnosi di Covid-19), alla sfera sessuale, nonché coinvolgenti minori. Un ulteriore ambito di intervento ha riguardato la lamentata pubblicazione di fotografie, commenti e video anche sui *social network* in assenza del consenso dell'interessato o di un'altra idonea base giuridica.

Nei diversi casi esaminati il vaglio dell'Autorità ha riguardato anche il rispetto delle disposizioni in materia di esercizio dei diritti (artt. 15-22 del RGPD), come pure la valutazione dei comportamenti dei titolari del trattamento rispetto alla mancata comunicazione delle informazioni richieste dall'Autorità ai sensi dell'art. 157 del Codice, cui hanno fatto seguito le relative contestazioni ed i conseguenti provvedimenti sanzionatori (fra gli altri provv. 28 luglio 2022, n. 275, doc. web n. 9813385).

Nel periodo di riferimento si è comunque registrata una significativa adesione da parte dei titolari del trattamento alle richieste pervenute dai reclamanti che ha consentito la definizione dei reclami senza l'adozione di provvedimenti collegiali.

Una parte dei reclami è stata tuttavia definita attraverso decisioni del Collegio, il quale, a seguito dello specifico esame degli elementi caratterizzanti ogni singola fattispecie, si è espresso in merito alla fondatezza della doglianza prospettata, effettuando spesso un bilanciamento tra le richieste del singolo e l'interesse pubblico generale all'informazione e ricorrendo ai poteri correttivi, ivi incluso quello sanzionatorio, previsti dal RGPD. Nei casi più gravi il Garante ha ritenuto di applicare, rispetto alla rilevata illiceità della condotta del titolare del trattamento, quale deterrente, anche misure sanzionatorie di tipo pecuniario, tenendo comunque conto delle peculiarità legate all'esercizio di tale potere correttivo in un ambito di particolare delicatezza, come quello della libertà di manifestazione del pensiero.

Le segnalazioni sono state esaminate ed istruite nei casi di particolare complessità o comunque sulla base della sussistenza dei presupposti per una verifica circa la conformità del trattamento alla normativa sulla protezione dei dati personali, ovvero sono state trattate, sempre nell'ambito delle competenze dell'Autorità, in maniera unitaria con riguardo a temi di carattere generale.

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

9.2.1. Dati giudiziari

Anche nel 2022 il Garante ha affrontato il tema ricorrente dell'utilizzo, a corredo di articoli giornalistici di cronaca giudiziaria, di immagini riprese in situazioni apparse lesive della dignità dell'individuo. In tal senso è stato valutato un reclamo in cui si lamentava l'illiceità del trattamento posto in essere da una questura e da alcune testate giornalistiche in relazione alla diffusione, in occasione di una conferenza stampa delle Forze di polizia locali, di fotografie del reclamante che, per le relative caratteristiche (tipologia dello scatto e posizione dell'interessato), ne evidenziavano lo stato di detenzione, essendo state scattate – come risulta dalla documentazione acquisita – in coincidenza con il fermo di polizia disposto nei suoi confronti.

Il Garante, nel valutare il caso di specie, ha ricordato da una parte che, in base al principio di "essenzialità dell'informazione riguardo a fatti di interesse pubblico" – operante anche con riferimento alle cronache relative a procedimenti penali (art. 12 delle regole deontologiche) – la pubblicazione dei dati identificativi delle persone a carico delle quali il procedimento è instaurato non può ritenersi preclusa dall'ordinamento vigente e va inquadrata nell'ambito delle garanzie volte ad assicurare trasparenza e controllo da parte dei cittadini sull'attività di giustizia; dall'altra, ha tuttavia ritenuto fondato il reclamo rilevando, in linea con il proprio consolidato orientamento in materia, un'eccedenza informativa nella pubblicazione delle immagini sopra descritte (provv. 28 aprile 2022, n. 165, doc. web n. 9778094) stante altresì l'acclarata assenza di comprovate ragioni di giustizia e di polizia ai fini della relativa diffusione (cfr. per tale profilo anche il provv. 24 febbraio 2022, n. 62,

doc. web n. 9766469 relativo al medesimo reclamo, in base al quale il trattamento di dati personali effettuato dal Ministero dell'interno mediante la divulgazione delle immagini in questione risulta illecito, in violazione degli artt. 3, comma 1, lett. *a*) e *c*) e 5 del d.lgs. n. 51/2018 e 14 del d.P.R. n. 15/2018, cfr. par. 8.2).

9.2.2. Dati relativi a minori

La tutela dei minori è stata una delle priorità dell'Autorità anche nell'anno di riferimento, con particolare riguardo al rispetto delle garanzie previste per il trattamento dei relativi dati personali dalle regole deontologiche (art. 7) e dalla Carta di Treviso.

Rispetto a quest'ultima, alla luce delle proposte di modifica deliberate dal Consiglio dell'Ordine dei giornalisti il 6 luglio 2021 (cfr. Relazione 2021, p. 116) e comunicate al Garante con nota del successivo 12 luglio, l'Autorità ha trasmesso, nel mese di maggio 2022, alcune osservazione al testo rendendosi disponibile ad un confronto sui relativi punti focali ed in generale sulle tematiche in materia di giornalismo.

Una particolare attenzione è stata riservata ai trattamenti di dati coinvolgenti i minori, procedendosi ad un tempestivo esame delle istanze pervenute all'Autorità, molte delle quali, nel periodo di riferimento, hanno riguardato l'indebita diffusione in rete di dati di minori, ovvero la denuncia di avvenuta creazione di *account* falsi nell'ambito dei *social network*.

Non sono mancati reclami e segnalazioni, provenienti da genitori di minorenni, riguardanti la pubblicazione non autorizzata di fotografie degli stessi su *social network* come Instagram. Il Garante è intervenuto ottenendo, in certi casi, attraverso una previa interlocuzione con i soggetti responsabili di tale pubblicazione, la spontanea rimozione dei contenuti.

9.2.3. Dati di personaggi noti

Nel periodo di riferimento il Garante ha avuto modo di precisare l'ambito di un corretto trattamento per finalità giornalistiche anche laddove esso riguardi dati personali relativi a personaggi noti. L'occasione è stata offerta, in particolare, da un reclamo diretto a denunciare l'illiceità del trattamento dei dati personali di un noto cantante che lamentava l'avvenuta pubblicazione, all'interno di una rivista settimanale, di informazioni che lo riguardavano relative al suo stato di salute, peraltro incluse in un virgolettato. Ciò ingenerando nel pubblico, secondo quanto rappresentato nel reclamo, il convincimento che si trattasse di circostanze dichiarate dall'interessato e riportate come se fossero una notizia attuale, laddove, invece, erano stati utilizzati estratti di testi di canzoni o sue presunte dichiarazioni, fornendo così una rappresentazione ritenuta dal medesimo del tutto distorta.

L'Autorità, tenuto conto del fatto che alcune delle frasi citate all'interno dell'articolo erano dichiaratamente tratte da testi di canzoni del reclamante, mentre altre risultavano ascrivibili a dichiarazioni pubblicamente rese dal medesimo, non ha ritenuto ravvisabili, anche in virtù della notorietà del personaggio, profili di violazione riconducibili alla normativa in materia di violazione di dati personali (provv. 10 marzo 2022, n. 86, doc. web n. 9838578).

9.2.4. Pubblicazione di fotografie a corredo di articoli giornalistici

L'Autorità è intervenuta anche rispetto all'indebita pubblicazione di fotografie su pagine *social* di testate giornalistiche, accogliendo un reclamo in cui l'interessato richiedeva la rimozione dalla pagina Instagram di un quotidiano di una fotografia che lo ritraeva mentre praticava la corsa, pubblicata in associazione ad un *post*

ritenuto denigratorio nei confronti delle persone che praticavano *footing* nel periodo di emergenza sanitaria. L'Autorità ha ritenuto che la fotografia – idonea a rendere identificabile il reclamante – non era da considerarsi essenziale per le finalità informative perseguite, ben potendosi associare immagini di altra natura (inquadrature a distanza, non focalizzate su singole persone), inoltre, in associazione al contenuto del *post*, la stessa risultava idonea a fornire un'informazione non corretta e potenzialmente inesatta riguardo al reclamante (provv. 7 aprile 2022, n.125, doc. web n. 9774819).

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

Anche nel 2022 l'esame di reclami e segnalazioni, con riguardo a vicende di cronaca che hanno comportato il trattamento dei dati personali degli interessati, ha costituito occasione per ribadire i principi fondamentali della disciplina relativa alla protezione dei dati personali in ambito giornalistico.

Tra questi, in particolare, assume rilievo il principio di "essenzialità dell'informazione" – sancito sia nel Codice (art. 137) sia nelle regole deontologiche (artt. 6, 8, 10 e 11) – il quale deve orientare in primo luogo il giornalista e successivamente l'Autorità, nell'ottica di un'informazione corretta e rispettosa dei diritti della persona.

Sulla base di tali premesse è stata definita una complessa istruttoria originata da un'istanza volta a denunciare un illecito trattamento in relazione alla pubblicazione integrale, in una rivista di carattere giuridico, di un'ordinanza della Corte di cassazione concernente il riconoscimento in Italia di un provvedimento di adozione di un minore da parte di una coppia omosessuale emesso da un giudice statunitense; ciò nonostante sull'ordinanza fosse stata apposta d'ufficio l'annotazione (art. 52 del Codice) diretta a prescrivere l'omissione delle generalità degli interessati in caso di riproduzione o diffusione dell'atto. L'Autorità, nel rilevare la violazione di diverse disposizioni a tutela anche dei minori e dei dati attinenti alla sfera sessuale, previste dal RGPD (art. 9), dal Codice (artt. 50, 52, comma 4, e 137) e dalla Carta di Treviso, ha disposto il divieto di trattamento dei dati in questione e una sanzione amministrativa pecuniaria; inoltre ha disposto la misura dell'avvertimento in relazione ad alcune carenze riscontrate relativamente al rispetto, da parte dell'editore, delle disposizioni in materia di esercizio dei diritti (provv. 28 aprile 2022, n. 157, doc. web n. 9779098).

La fondatezza del reclamo è stata rilevata anche nel caso in cui si lamentava l'illiceità del trattamento di dati personali da parte di un'organizzazione sindacale la quale, sulla propria pagina Facebook, aveva diffuso il contenuto di un esposto presentato dalla medesima organizzazione sindacale contenente dati personali di un lavoratore. Ciò in quanto nell'esposto pubblicato nella pagina Facebook ad accesso libero risultavano presenti dati identificativi eccedenti del reclamante (provv. 24 febbraio 2022, n. 73, doc. web n. 9760865).

Analogamente l'Autorità è intervenuta con una declaratoria di fondatezza rispetto ad un reclamo con cui si lamentava l'illiceità del trattamento posto in essere attraverso la pubblicazione di un *e-book* e di altri articoli attinenti ai fatti che avevano avuto una vasta eco mediatica, in quanto emersi a seguito delle denunce di violenza sessuale sporte da alcune giovani nei confronti di un imprenditore. La reclamante, in particolare lamentava la diffusione di dati personali in violazione del principio di essenzialità dell'informazione (nel caso dell'*e-book*, il nome, cognome e città di origine; nel caso degli articoli il nome e cognome o il solo nome) unitamente ad informazioni attinenti ad episodi di vita dell'indagato, che avrebbero coinvolto anche l'interessata, ritenuti peraltro non corrispondenti al vero.

9

L'Autorità ha ritenuto che, pur se i contenuti dell'*e-book* e degli articoli erano volti a fornire un quadro generale relativo ad una persona cui venivano ascritti reati di particolare gravità, dando rilievo ad aspetti diversi e contraddittori della sua personalità, attinenti anche al suo passato (al percorso di studi svolto, ai traguardi professionali raggiunti, alle relazioni affettive o sentimentali instaurate), dei quali aveva fatto parte anche la reclamante, la pubblicazione dei dati personali relativi a quest'ultima non costituisse un elemento necessario in rapporto alla finalità informativa perseguita, potendosi ricorrere, nella narrazione, a soluzioni più in linea con le disposizioni a tutela della sfera privata della reclamante, quali ad es. il ricorso ad un nome di fantasia (provv.ti 15 settembre 2022, nn. 307, doc. web n. 9879182 e 308, doc web n. 9878014).

Il principio di essenzialità dell'informazione è stato richiamato anche nei provvedimenti di limitazione provvisoria del trattamento adottati dall'Autorità nei confronti di varie testate giornalistiche a seguito dell'avvenuta pubblicazione, nel mese di aprile 2022, di articoli relativi alla vicenda legata ad una presunta relazione tra la dirigente scolastica di un liceo scientifico romano ed uno studente dell'ultimo anno. Si è infatti ritenuto che i dettagli riportati all'interno dei predetti articoli – in particolare i contenuti delle *chat* condivise dai protagonisti dei fatti narrati – fossero eccedenti riguardo alla finalità informativa e lesivi dei diritti delle persone coinvolte, con particolare riguardo alla dirigente scolastica rispetto alla quale, peraltro, i fatti contestati risultavano essere ancora al vaglio dell'istituzione scolastica interessata (cfr. ex *pluribus*, provv.ti 31 marzo 2022, doc. web n. 9759899 e 1° aprile 2022, n. 115, doc. web n. 9759795).

Nessuna eccedenza informativa è stata invece ravvisata nel caso di reclami che lamentavano l'illiceità del trattamento posto in essere dalle testate coinvolte attraverso la diffusione di informazioni relative ad una vicenda giudiziaria che aveva riguardato l'interessata e per la quale la medesima era stata condannata (si trattava, nello specifico, di diffamazione avvenuta a danno di altra persona tramite *social network*). Tale condanna era stata confermata dalla Corte di cassazione nel 2018 e per tale ragione gli editori avevano pubblicato nuovi articoli in merito. Ciononostante, in nessuno dei casi sottoposti all'attenzione del Garante risultavano essere stati diffusi dati idonei ad identificare l'interessata (solo in uno dei tre casi, la pubblicazione aveva riguardato le sole iniziali) con conseguente declaratoria di infondatezza dei reclami da parte dell'Autorità (provv.ti 27 gennaio 2022, nn. 28, doc. web n. 9747522; 29, doc. web n. 9747552 e 30, doc. web n. 9747871).

L'infondatezza del reclamo è stata anche riscontrata dal Garante nel caso in cui il reclamante richiedeva la deindicizzazione di un articolo del 2017 riferito a fatti avvenuti nel 2016 rilevando che gli stessi non avrebbero risposto ad alcun interesse pubblico, tenuto conto del tempo decorso e dell'assenza di ulteriori sviluppi; l'interessato aveva altresì lamentato il mancato riscontro all'interpello preventivo da parte del titolare del trattamento, rilevando una carenza informativa all'interno del sito. L'Autorità, nel valutare gli elementi dedotti dalle parti, ha ritenuto che nel caso in esame non vi fossero i presupposti per limitare la visibilità della notizia, trattandosi di informazioni pubblicate in epoca recente e tenuto conto della pendenza del procedimento penale riguardante l'interessato. A fronte della declaratoria di infondatezza del reclamo nel merito, l'Autorità ha comunque rilevato la violazione degli artt. 13 e 14 del RGPD, prescrivendo al titolare del trattamento di implementare un'informativa idonea e comminando altresì un ammonimento per le violazioni riscontrate (provv. 6 ottobre 2022, n. 323, doc. web n. 9838542).

9.3. *Attività svolta nei confronti di TikTok*

Nell'ambito delle attività in ordine ai trattamenti di dati personali effettuati dai *social network* il Garante ha continuato a monitorare le modalità relative trattamento dei dati da parte di TikTok.

In data 7 luglio 2022, l'Autorità ha adottato un provvedimento con il quale ha avvertito la piattaforma che è illecito utilizzare dati personali archiviati nei dispositivi degli utenti per profilarli e inviare loro pubblicità personalizzata in assenza di un esplicito consenso (n. 248, doc. web n. 9788429).

Il *social network* aveva informato i propri utenti che, a partire dal 13 luglio, le persone maggiori di 18 anni sarebbero state raggiunte da pubblicità "personalizzata", basata cioè sulla profilazione dei comportamenti tenuti nella navigazione su TikTok e aveva modificato la sua *privacy policy* prevedendo come base giuridica per il trattamento dei dati non più il consenso degli interessati, ma non meglio precisati "legittimi interessi" di TikTok e dei suoi *partner*.

Il Garante aveva immediatamente avviato un'istruttoria sulla modifica della *privacy policy* e chiesto informazioni al *social network*.

Sulla base degli elementi forniti dalla Società, l'Autorità ha concluso che tale mutamento della base giuridica risulta incompatibile con la direttiva europea 2002/58, la cd. direttiva *e-privacy*, e con l'art. 122 del Codice (che ne dà attuazione), norme che prevedono espressamente come base giuridica "per l'archiviazione di informazioni, o l'accesso a informazioni già archiviate, nell'apparecchiatura terminale di un abbonato o utente" esclusivamente il consenso degli interessati.

Oltre alla base giuridica inadeguata, il Garante ha messo in luce un aspetto che desta particolare preoccupazione e che riguarda la tutela dei minori iscritti alla piattaforma. Le attuali difficoltà mostrate da TikTok nell'accertare l'età minima per l'accesso alla piattaforma non consentono infatti di escludere il rischio che la pubblicità "personalizzata" basata sul legittimo interesse raggiunga i giovanissimi, con contenuti non appropriati.

L'Autorità, avvalendosi di uno dei poteri previsti dal RGPD, ha pertanto inviato un "avvertimento" formale alla Società, avvisando che un trattamento effettuato sulla base giuridica del "legittimo interesse", almeno in relazione alle informazioni archiviate sui dispositivi degli utenti, si porrebbe al di fuori della cornice normativa in vigore, con le evidenti conseguenze, anche di carattere sanzionatorio.

L'Autorità si è pertanto riservata l'adozione di eventuali provvedimenti anche di urgenza qualora TikTok non avesse receduto dal proprio proposito.

La violazione della direttiva *e-privacy* ha consentito al Garante di intervenire direttamente e in via d'urgenza nei confronti di TikTok, al di fuori della procedura di cooperazione prevista dal RGPD, che avrebbe visto l'esercizio dell'iniziativa da parte dell'Autorità di protezione dati irlandese, Paese ove TikTok ha fissato il proprio stabilimento principale.

In ogni caso, poiché anche il trattamento di informazioni diverse rispetto a quelle archiviate sui dispositivi degli utenti sulla base del legittimo interesse appare incompatibile con la disciplina europea in materia di protezione dei dati personali – in questo caso quella dettata dal RGPD – il Garante ha contestualmente informato il Comitato europeo delle autorità di protezione dei dati personali e l'Autorità irlandese per la valutazione delle ulteriori iniziative da intraprendere.

TikTok Ireland, a seguito del provvedimento, ha instaurato una collaborazione con l'Autorità irlandese e ha dichiarato di volersi adeguare all'ordine ricevuto, impegnandosi a non effettuare annunci personalizzati.

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

I reclami presentati nei confronti dei motori di ricerca hanno costituito, anche nel 2022, una parte considerevole di quelli complessivamente presentati all'Autorità con riguardo ai trattamenti effettuati nell'ambito della libertà di informazione.

Con riferimento ai reclami proposti nei confronti dei gestori dei motori di ricerca, conformemente a quanto già evidenziato nelle precedenti Relazioni, si è provveduto, relativamente alle istanze presentate dagli interessati già in regola con i requisiti previsti dalla normativa di riferimento, ad avviare l'istruttoria notificando ai titolari del trattamento le relative richieste di informazioni. Queste ultime sono state indirizzate in particolare a Google nei cui confronti l'Autorità ha, come noto, un potere decisorio autonomo quale effetto delle scelte organizzative operate dalla Società. Sono state inoltre avviate istruttorie anche nei confronti di Microsoft Corporation e di Verizon Media Emea Limited, alcune delle quali sono state definite per intervenuta adesione, mentre in altri casi i relativi procedimenti sono parzialmente proseguiti in IMI (in particolare con riguardo a Verizon) essendo stato espresso un diniego alla rimozione da parte del titolare del trattamento, avente il proprio stabilimento principale in Irlanda.

In relazione al totale dei reclami pervenuti nel corso del 2022 una parte, seppure circoscritta, è stata definita per intervenuta adesione dei titolari del trattamento. Altra parte ha reso necessaria la preliminare regolarizzazione delle istanze pervenute, essendo stata rilevata la mancanza di alcuni presupposti, spesso per la mancanza del preventivo interpello, richiesto dall'art. 15 del reg. del Garante n. 1/2019 trattandosi di reclami in materia di esercizio dei diritti, o per la mancata esplicitazione delle ragioni della richiesta.

Nel periodo di riferimento occorre evidenziare che una parte delle richieste avanzate nei confronti di Google è stata soddisfatta per l'adesione spontanea del titolare del trattamento a seguito della trasmissione del reclamo da parte dell'Autorità. La restante parte è stata definita tramite provvedimenti collegiali (circa 43) di seguito sommariamente menzionati in relazione alla fattispecie trattata e alla natura della decisione assunta.

I provvedimenti emanati hanno riguardato richieste di deindicizzazione di risultati reperibili tramite motore di ricerca in associazione al nominativo dell'interessato in ragione dell'asserita insussistenza di un attuale interesse del pubblico ad avere conoscenza di determinate informazioni.

Dei casi esaminati una parte si è conclusa con una decisione di accoglimento del reclamo presentato al Garante. Un numero rilevante ha riguardato vicende giudiziarie che hanno coinvolto gli interessati e rispetto alle quali questi ultimi hanno lamentato il pregiudizio derivante dalla circolazione di notizie non aggiornate alla luce della conclusione favorevole del procedimento penale, tenuto anche conto, in alcuni casi, delle indicazioni di recente fornite dal legislatore con il decreto legislativo relativo alla riforma del processo penale cd. riforma Cartabia (cfr. provv.ti 10 febbraio 2022, n. 52, doc. web n. 9750669; 24 marzo 2022, n. 105, doc. web n. 9767743; 16 giugno 2022, n. 227, doc. web n. 9793921; 7 luglio 2022, n. 245, doc. web n. 9813349; 21 luglio 2022, n. 259, doc. web n. 9815689; 21 luglio 2022, n. 258, doc. web n. 9813878; 20 ottobre 2022, n. 352, doc. web n. 9838182; 24 novembre 2022, n. 394, doc. web n. 9838106) o comunque della concessione di benefici di legge, quali il beneficio della non menzione della condanna nel casellario giudiziale (tra gli altri provv. 10 febbraio 2022, n. 53, doc. web n. 9751153). In alcune ipotesi si è tenuto conto dell'intervenuta definizione della vicenda giudiziaria rispetto alla quale non emergevano aggiornamenti né negli articoli contestati, né in ulteriori contenuti

comunque presenti in rete (come nel caso dei provv.ti 28 luglio 2022, n. 274, doc. web n. 9809538 e 24 novembre 2022, n. 395, doc. web n. 9838077).

A questi casi si sono poi aggiunte altre fattispecie nelle quali l'Autorità, in considerazione delle caratteristiche specifiche della vicenda rappresentata, non ha ravvisato la sussistenza di ragioni di interesse pubblico prevalenti rispetto al diritto all'oblio invocato dagli interessati (tra gli altri, provv.ti 10 febbraio 2022, n. 55, doc. web n. 9750647; 7 aprile 2022, n. 128, doc. web n. 9768456; 28 aprile 2022, n. 156, doc. web n. 9778076; 20 ottobre 2022, n. 351, doc. web n. 9838200; 10 novembre 2022, n. 373, doc. web n. 9838253; 15 dicembre 2022, n. 432, doc. web n. 9852668); in alcuni casi rilevando un'eccedenza di trattamento effettuata dallo stesso sito fonte (provv.ti 27 gennaio 2022, n. 27, doc. web n. 9747505 e 28 aprile 2022, n. 155, doc. web n. 9777312).

La restante parte dei provvedimenti adottati ha riguardato, invece, una decisione di infondatezza motivata dalla ritenuta sussistenza di un perdurante interesse del pubblico a conoscere le informazioni riferite all'interessato e riguardanti, nella maggior parte dei casi, vicende giudiziarie non ancora concluse (cfr. provv.ti 27 gennaio 2022, n. 25, doc. web n. 9750630; 10 febbraio 2022, n. 51, doc. web n. 9751169; 7 aprile 2022, n. 129, doc. web n. 9768508) oppure definite in epoca recente (tra gli altri provv.ti 10 febbraio 2022, n. 55, doc. web n. 9750647; 12 maggio 2022, n. 183, doc. web n. 9789593; 9 giugno 2022, n. 219, doc. web n. 9795366; 9 giugno 2022, n. 216, doc. web n. 9789124; 21 luglio 2022, n. 256, doc. web n. 9812455 e 15 dicembre 2022, n. 434, doc. web n. 9843758).

Tra le decisioni di infondatezza si possono inoltre citare i casi nei quali la richiesta di rimozione avanzata dall'interessato appariva collegata, non tanto all'accertamento di inesattezze oggettive presenti negli articoli reperibili tramite gli Url indicati, quanto a doglianze riferite ad un'asserita falsità delle informazioni diffuse (cfr. provv. 7 aprile 2022, n. 124, doc. web n. 9833024). In un altro caso analoghe doglianze avevano formato oggetto di accertamento da parte dell'Autorità giudiziaria anteriormente alla presentazione del reclamo il quale, tuttavia, non faceva parola di tale circostanza rilevata, invece, nel corso del procedimento dal titolare del trattamento (cfr. provv. 28 aprile 2022, n. 154, doc. web n. 9777246).

Parimenti infondata è stata ritenuta l'istanza volta ad ottenere (sia da Google che dal sito fonte) il diritto all'oblio da parte del reclamante – figura di rilievo di una sigla sindacale particolarmente rappresentativa nel bolognese e in ambito nazionale – con riferimento ad articoli che si riferivano ad una vicenda giudiziaria che aveva visto coinvolto il reclamante e la testata nei cui confronti era rivolto il reclamo, in seguito ad esternazioni pubbliche dalle quali erano scaturite denunce per diffamazione, i cui sviluppi – in termini sfavorevoli per il reclamante – erano stati definiti in epoca recente (provv. 6 ottobre 2022, n.326, doc. web n.9838526).

In un altro caso si è ritenuto che il reclamo fosse infondato rispetto alla lamentata permanenza *online* di un articolo che riportava la vicenda giudiziaria dell'interessato, nonostante il decorso del tempo, in ragione della particolare gravità dei diversi reati richiamati e del quadro definito nell'unica sentenza prodotta dal reclamante, nonché dell'assenza di ulteriori elementi di valutazione stante l'inerzia del medesimo. Lo si è invece ritenuto fondato con riguardo alla richiesta di rimozione della sola immagine dell'interessato in quanto la pubblicazione di tale foto, svincolata dalla pubblicazione della notizia, non è risultata supportata da alcuna esigenza informativa sulla vicenda (provv. 15 dicembre 2022, n. 435, doc. web n. 9856729).

10 Cyberbullismo e *revenge porn*

Le segnalazioni pervenute in materia di cyberbullismo nel periodo di riferimento hanno riguardato, nella maggior parte dei casi, la pubblicazione di *post* aventi un contenuto denigratorio e diffamatorio e sono state trattate tempestivamente attraverso la formulazione di specifiche richieste di intervento al titolare del trattamento/gestore del sito, anche prendendo contatti (per telefono o per *e-mail*) con il segnalante al fine di richiedere ulteriori informazioni o fornire indicazioni utili al caso. Si sono inoltre registrati, come in passato, alcuni casi nei quali non sono stati ravvisati i presupposti per poter procedere. Ciò tenendo conto della normativa di riferimento alla luce di una riscontrata carenza degli elementi che la legge n. 71/2017 indica quali requisiti minimi per qualificare una condotta come atto di cyberbullismo.

Si è ampliato anche l'impegno dell'Autorità per prevenire e contrastare il fenomeno della diffusione, con intenti vendicativi e comunque in assenza del consenso della persona interessata, di immagini a contenuto sessualmente esplicito (*revenge porn*) alla luce della specifica normativa introdotta con il decreto-legge 8 ottobre 2021, n. 139, convertito con modificazioni dalla legge 3 dicembre 2021, n. 205, confluita nel nuovo art. 144-*bis* del Codice in materia di protezione dei dati personali.

A tal fine è stato modificato il reg. del Garante n. 1/2019 attraverso l'inserimento di un apposito articolo dedicato alla disciplina del procedimento da seguire nella gestione delle segnalazioni di *revenge porn*. È stata inoltre prevista l'introduzione di un modello di segnalazione telematica per gli interessati, definendo un percorso differente a seconda che si tratti di utenti dotati di una identità digitale e quindi autenticati, oppure di utenti non autenticati. È stata inoltre introdotta l'opzione, ritenuta preferibile, di inviare alle piattaforme il codice *hash* delle immagini prodotte dai segnalanti, anziché la copia in chiaro delle stesse.

Le segnalazioni ricevute (circa 150) nel periodo di riferimento sono state prontamente trattate, fornendo, nella maggior parte dei casi, indicazioni agli interessati, oppure chiedendo integrazioni ai fini della successiva trattazione (in particolare chiedendo la trasmissione del materiale la cui acquisizione è prevista dall'art. 144-*bis* del Codice).

In alcuni casi il materiale inviato dai segnalanti non è risultato idoneo (come nel caso di *screenshot* di videochiamate o di *chat*) all'invio alle piattaforme interessate, stante la possibilità per la persona malintenzionata di caricare l'immagine originale in suo possesso.

L'esame delle segnalazioni si è concluso, con riguardo a diverse fattispecie (circa 60), con l'adozione in via d'urgenza di una determinazione dirigenziale (successivamente ratificata dal Collegio) diretta alle piattaforme coinvolte al fine di ottenere l'intervento di blocco preventivo della diffusione del materiale a contenuto sessualmente esplicito.

11 *Marketing* e trattamento di dati personali

11.1. *Il fenomeno del* telemarketing *indesiderato e l'azione di contrasto*

A seguito dell'elevatissimo numero di segnalazioni e reclami, volti a lamentare, nella quasi totalità, la ricezione di chiamate indesiderate o, in misura meno significativa, comunicazioni indesiderate tramite *e-mail*, l'Autorità ha proseguito l'attività di contrasto al *marketing* illegale.

Con riguardo alle numerose segnalazioni per telefonate promozionali provenienti da soggetti, o effettuate per conto di committenti, non individuati, o per le quali non è stata indicata la numerazione chiamante e/o altri elementi essenziali ai fini di un'attività di controllo dell'Autorità, il Garante ha fornito riscontro con note-tipo contenenti chiarimenti in merito al fenomeno del *telemarketing* selvaggio ed indicazioni operative per attuare un primo contrasto. L'Autorità ha altresì effettuato sistematicamente una ricerca delle numerazioni chiamanti nel Registro degli operatori di comunicazione (laddove indicate dagli interessati), rilevando numerosi casi di *spoofing*, ossia di utilizzo di numerazioni VoIP fittizie con conseguente occultamento della reale linea telefonica.

Relativamente, invece, al fenomeno delle telefonate cd. mute ovvero quelle nelle quali la persona contattata, dopo aver sollevato il ricevitore, non viene messa in comunicazione con alcun interlocutore, sono stati forniti riscontri, sempre con note-tipo, contenenti le iniziative di carattere ispettivo, prescrittivo e sanzionatorio avviate dal Garante, con particolare riferimento al provvedimento generale del 20 febbraio 2014 (doc. web n. 3017499), unitamente alle FAQ pubblicate nel sito istituzionale dell'Autorità, nella sezione "Telefonate mute: le domande più frequenti".

Laddove possibile e nei casi in cui le segnalazioni e i reclami pervenuti lo hanno consentito (in quanto puntuali, riconducibili a specifici titolari e di rilevanza in tema di protezione dei dati personali), il Garante ha avviato istruttorie, anche lunghe e complesse, all'esito delle quali ha adottato provvedimenti correttivi e/o sanzionatori, illustrati nei successivi paragrafi.

11.1.1. Il telemarketing *illegale nel settore telefonico*

L'Autorità, con riferimento ad un precedente provvedimento adottato nei confronti di una nota compagnia telefonica (cfr. provv. 12 novembre 2020, n. 224, doc. web n. 9485681), ha avviato specifiche istruttorie relative alla sua rete di vendita e ha adottato nei confronti di una agenzia di *call-center* il provvedimento 28 aprile 2022, n. 153 (doc. web n. 9779025). È stato rilevato che l'agenzia di *call-center*, oltre alla specifica attività promozionale per conto della compagnia telefonica, acquisiva liste anagrafiche da soggetti terzi che entravano a far parte delle liste di contattabilità della compagnia telefonica stessa. Al riguardo, è stato osservato che l'acquisizione di tali liste non costituiva un "incarico" proveniente dalla compagnia che aveva commissionato la campagna pubblicitaria all'agenzia, ma un'attività da quest'ultima svolta in piena autonomia e sottoposta solo ad autorizzazioni preventive e a controlli successivi da parte della compagnia telefonica al fine di consentire l'ingresso delle anagrafiche nei *database* aziendali. L'agenzia di *call-center* è risultata quindi aver acquisito, in veste di autonomo titolare del trattamento, le liste anagrafiche, successivamente riversate

nel *database* della compagnia telefonica, realizzando il cd. doppio passaggio di dati personali (dall'originario titolare all'agenzia e dall'agenzia alla compagnia telefonica) per la cui liceità sarebbe stato necessario che ciascun titolare cedente avesse acquisito dagli interessati uno specifico e inequivoco consenso informato. All'agenzia, che non aveva acquisito il predetto consenso, è stato vietato l'ulteriore trattamento dei dati ed è stata applicata una sanzione amministrativa pecuniaria.

Sempre in ambito di *telemarketing*, l'Autorità ha adottato un provvedimento nei confronti di una società che aveva dato corso a un contatto telefonico indesiderato, reiterando tale condotta nonostante l'interessato avesse espresso la propria opposizione fin dal primo momento. Il Garante, nel richiamato provvedimento, ha anche evidenziato che la società aveva omesso di fornire riscontro alle richieste di informazioni inviate ai sensi dell'art. 157 del Codice mediante Pec. Pertanto, oltre al divieto di ulteriori trattamenti dei dati del reclamante, è stata applicata alla società una sanzione amministrativa pecuniaria (provv. 7 aprile 2022, n. 126, doc. web n. 9771529).

È stata altresì svolta un'approfondita istruttoria nei confronti di una compagnia telefonica, in relazione ad un reclamo con il quale una signora aveva lamentato la ricezione di una telefonata promozionale da parte di un'agenzia della rete di vendita della compagnia, a seguito della quale era stata avviata, a sua insaputa, la procedura di cambio dell'operatore telefonico. In riscontro alle richieste della reclamante, la compagnia telefonica aveva rappresentato che il contatto telefonico era stato effettuato sulla base del consenso rilasciato dall'interessata telefonando spontaneamente all'agenzia e comunicando la disponibilità ad essere contattata per promozioni commerciali, affermazione che la reclamante contestava. Nel provvedimento è stato evidenziato che la ricostruzione della compagnia telefonica era "inverosimile" e che, in ogni caso, la vendita del servizio telefonico (e il relativo contatto promozionale) risultava essere stata effettuata il giorno prima dell'asserita telefonata della reclamante (provv. 10 novembre 2022, n. 379, doc. web n. 9826417).

Dall'istruttoria è altresì emerso che alla reclamante era stata data lettura dell'informativa *privacy* e dell'intero contratto per telefono, ad una velocità di circa 200 parole al minuto. Il Garante ha quindi osservato che le oggettive anomalie di una vendita telefonica suggellata da un documento audio, che costituisce a tutti gli effetti la base contrattuale e che risulta in massima parte incomprensibile ad un normale ascoltatore, rendono ogni trattamento svolto in relazione a tale contratto irrimediabilmente viziato sotto il profilo della correttezza. In particolare, l'Autorità ha osservato che "il principio di correttezza non si sovrappone a quello di liceità, ma ne amplifica la portata richiamando ogni titolare non solo a rispettare le specifiche disposizioni di legge, ma a fare proprio il senso complessivo e lo spirito della normativa in materia di protezione dei dati personali al fine di agevolare le scelte dell'interessato, in base ai medesimi canoni utilizzati in sede civilistica per individuare la correttezza del debitore e del creditore (art 1175 c.c.) e la buona fede nell'esecuzione del contratto (art. 1375 c.c.), più ampiamente ricompresi nel principio di solidarietà sociale di cui all'art. 2 della Costituzione". La compagnia telefonica è stata pertanto raggiunta da una sanzione amministrativa pecuniaria e dal divieto di ulteriori trattamenti con i dati personali della reclamante.

Sono state inoltre avviate istruttorie nei confronti di una compagnia telefonica, per verificare il *trend* complessivo delle azioni correttive poste in essere dalla società anche in considerazione della persistenza di un notevole numero di doglianze quotidianamente pervenienti, nonostante il precedente provvedimento del 2020 (cfr. provv. 15 gennaio 2020, n. 7, doc. web n. 9256486). In particolare, l'istruttoria ha avuto ad oggetto la gestione dei diritti degli interessati ai sensi degli artt. 15-22 del

RGPD, ed eventuali persistenti criticità relativamente ai principi di *accountability, privacy by design* e sicurezza dei dati.

11.1.2. Il telemarketing *illegale nel settore energetico*

Con riferimento al *marketing* nel settore energetico, è stato adottato un provvedimento nei confronti di un'importante società del settore, a seguito della ricezione di segnalazioni e reclami relative a comunicazioni promozionali (provv. 15 dicembre 2022, n. 431, doc. web n. 9856345). Le principali criticità hanno riguardato l'informativa predisposta dalla società e l'acquisizione dei consensi degli interessati, non specifici né liberi. Oltre alla sanzione amministrativa pecuniaria pari a euro 4.900.000,00, si è reso necessario adottare alcune misure correttive. In particolare, è stato vietato il trattamento dei dati personali per i quali la società non è risultata in grado di comprovare l'acquisizione di un idoneo consenso ed è stato ingiunto di adottare procedure volte a verificare costantemente, anche mediante controlli a campione, che i dati personali siano trattati nel pieno rispetto delle disposizioni in materia, nonché a facilitare l'esercizio dei diritti degli interessati, recependo il consenso al momento del contatto telefonico ed indicando chiaramente, nello *script* di chiamata, il soggetto a cui dovrà essere indirizzata la richiesta di cancellazione dei dati personali. Infine, è stato ingiunto di fornire agli interessati, tanto nell'ambito delle *app* quanto del sito web, un'idonea informativa nella quale siano indicate le operazioni di trattamento effettivamente svolte.

11.1.3. Il telemarketing *illegale in altri settori commerciali*

Sempre in tema di ricezione di telefonate indesiderate, è stata avviata un'istruttoria a seguito di un reclamo presentato nei confronti di una società che sosteneva di aver ricevuto i dati dell'interessata dal proprio *list provider*, con sede in Germania, in quanto, in occasione dell'iscrizione ad un concorso a premi, la medesima avrebbe prestato il consenso alla comunicazione dei dati a terzi. I dati della reclamante, presenti nella banca dati del *list provider*, sarebbero quindi entrati nella disponibilità della società in forza del citato consenso originariamente acquisito e utilizzati dalla stessa per la propria attività promozionale. L'istruttoria ha consentito di accertare che, in occasione del primo contatto con gli interessati, la società non ha reso una propria informativa completa su tutti gli elementi previsti negli artt. 13 e 14 del RGPD, ma sintetiche informazioni riferite peraltro ai trattamenti svolti dal *list provider*. L'istruttoria ha evidenziato criticità di sistema che hanno reso necessario l'adozione di alcune misure correttive. In particolare, è stato vietato il trattamento dei dati personali per i quali la società non è stata in grado di comprovare l'acquisizione di un idoneo consenso, anche svolgendo verifiche su campioni congrui rispetto alla mole dei dati trattati, e si è ingiunto alla medesima di fornire, in occasione dei contatti promozionali, informazioni complete sul trattamento svolto dal titolare. Si è inoltre vietato il trattamento dei dati acquisiti dal *list provider* e da altri soggetti terzi, qualora nel primo contatto gli interessati non avessero ricevuto un'idonea informativa. Infine si è comminata una sanzione amministrativa pecuniaria (provv. 15 dicembre 2022, n. 429, doc. web n. 9852290).

È stato poi adottato un provvedimento correttivo e sanzionatorio nei confronti di una nota società nel mercato assicurativo (provv. 24 novembre 2022, n. 393, non pubblicato in quanto sospeso in sede di impugnazione). L'Ufficio ha contestato alla società di aver effettuato, in proprio e avvalendosi di terzi, attività di *telemarketing* in assenza di un preventivo consenso degli interessati, proseguita con immotivata insistenza malgrado le numerose richieste di opposizione. Nel provvedimento, si è documentata la mancanza di controllo sulla filiera e la mancata adozione di misure

tecniche e organizzative idonee a garantire la liceità del trattamento. Si è inoltre dato atto del fatto che la società ha presentato copiosa documentazione per dimostrare la presenza di valide procedure ma, in base a quanto dimostrato dall'Ufficio, tali elementi davano atto solo di una "*privacy* di carta" essendo predisposti più con l'intento di documentare l'attività del titolare che non, invece, di tutelare gli interessati da potenziali illeciti trattamenti. Il Garante ha comminato quindi una sanzione pari a euro 5.449.381,88.

Per quanto riguarda le attività promozionali tramite *telemarketing* poste in essere dalle agenzie immobiliari, un reclamante lamentava la ricezione di telefonate indesiderate promozionali e l'acquisizione dei suoi dati in rete, in spregio della regola del consenso informato e dei principi di correttezza e finalità (v. art. 5, par. 1, lett. *a*) e *b*), del RGPD). L'Autorità ha vietato il trattamento dei dati personali reperiti in internet per i quali la società non è risultata in grado di comprovare l'acquisizione di un preventivo consenso informato da parte degli interessati, ha ingiunto di adottare adeguate procedure per garantire un completo e tempestivo riscontro alle istanze di esercizio dei diritti, nonché di rilasciare ai destinatari dei contatti telefonici un'idonea informativa preventiva rispetto al trattamento dei loro dati. Infine è stata imposta una sanzione amministrativa pecuniaria (provv. 10 febbraio 2022, n. 49, doc. web n. 9756869).

11.1.4. Ulteriori violazioni nell'ambito del telemarketing *illegale*

Con riferimento alle modalità di gestione delle richieste di esercizio dei diritti degli interessati, il Garante ha adottato un provvedimento di ammonimento (provv. 15 settembre 2022, n. 306, doc. web n. 9819285) e tre provvedimenti correttivi e sanzionatori (provv.ti 5 agosto 2022, n. 296, doc. web n. 9827135; 5 agosto 2022, n. 297, doc. web n. 9817535 e 20 ottobre 2022, n. 349, doc. web n. 9827153), nell'ambito di istruttorie avviate a seguito di segnalazioni e/o reclami proposti all'Autorità nei confronti di società che avevano inviato *e-mail* in assenza di consenso dell'interessato e/o non avevano fornito riscontro alle richieste di esercizio dei diritti.

In uno dei casi sopra riportati (cfr. provv. 20 ottobre 2022), è emerso che, alla data della presunta acquisizione del consenso del reclamante, il sito internet a cui il medesimo si sarebbe registrato, era un mero "sito vetrina" di un soggetto terzo, senza alcuna informativa, né *form* di acquisizione dei dati e neppure richieste di consenso da selezionare per le distinte finalità promozionali e per la cessione dei dati a terzi per scopi pubblicitari. In tre dei menzionati casi, oltre all'applicazione di una sanzione amministrativa pecuniaria, si è resa necessaria l'adozione di alcune misure correttive, tra cui quella di comprovare l'acquisizione di un idoneo consenso e di verificare costantemente che i dati personali siano trattati nel rispetto delle disposizioni in materia.

Sempre in tema di esercizio dei diritti degli interessati, il Garante ha adottato il provvedimento 27 gennaio 2022, n. 23 (doc. web n. 9746068), in relazione ad un reclamo presentato nei confronti di una società operante nel settore della formazione professionale. Il reclamante, per partecipare ad un corso di formazione professionale, aveva ricevuto dagli organizzatori alcuni moduli da restituire compilati, accorgendosi però che questi erano intestati non al soggetto che lo aveva originariamente contattato ma ad un'altra società, nei confronti della quale il reclamante decideva di formulare richiesta di accesso ai dati, di cancellazione e di opposizione ai sensi degli artt. 15, 17 e 21 del RGPD. La società forniva riscontro comunicando la cancellazione di tutti i dati del reclamante dai propri archivi, ma senza fornire allo stesso le informazioni richieste nell'istanza di accesso e senza assicurare di aver preso atto dell'opposizione dell'interessato a futuri trattamenti. L'Autorità ha rilevato che la società si era inserita

in un rapporto contrattuale tra il reclamante e l'originario proponente senza chiarire il proprio ruolo e la portata dei trattamenti di dati personali che sarebbero stati svolti e senza fornire le ulteriori informazioni di cui all'art. 13 del RGPD. La società aveva inoltre fornito riscontri incompleti anche in occasione del successivo esercizio da parte dell'interessato dei diritti di cui agli artt. 15 e 21 del RGPD (diritto di accesso e di opposizione al trattamento) sottraendo al reclamante il controllo dei propri dati personali. Con il provvedimento, l'Autorità ha vietato alla società ulteriori trattamenti dei dati del reclamante e applicato una sanzione amministrativa pecuniaria.

Un altro provvedimento sanzionatorio è stato poi adottato per mancato riscontro alla richiesta di informazioni formulata dall'Autorità ai sensi dell'art. 157 del Codice, con la quale si invitava una società a chiarire circostanze relative al consenso dell'interessato alla ricezione di telefonate per fini promozionali (provv. 20 ottobre 2022, n. 350, doc. web n. 9832544).

In parallelo alle attività sopra descritte, l'Autorità ha monitorato le misure correttive implementate da alcuni titolari per contrastare le attività di *telemarketing* illegale, anche in relazione a quanto prescritto in provvedimenti correttivi e sanzionatori adottati nei loro confronti.

11.1.5. Utilizzo di call-center *ubicati fuori dall'Unione europea*

Anche nel 2022, con immutata consistenza numerica, sono pervenute notifiche da parte dei titolari che si avvalgono di *call center* ubicati al di fuori dell'Unione europea, in conformità a quanto previsto dall'art. 24-*bis*, d.l. 22 giugno 2012, n. 83, come sostituito dall'art. 1, comma 243, l. 11 dicembre 2016, n. 232.

11.1.6. Scenari evolutivi nel settore del telemarketing *illegale: il codice di condotta*

Con la piena operatività del nuovo Registro pubblico delle opposizioni (Rpo), si è registrato un sensibile incremento di doglianze in materia di *telemarketing* (3.150 istanze in tre mesi, pari a quelle mediamente ricevute in un anno in tale settore). Come noto, con il d.P.R. 27 gennaio 2022, n. 26, nel dare attuazione alla legge 11 gennaio 2018, n. 5 e, dal 27 luglio 2022, è stato reso disponibile il nuovo Registro, dotato di nuove funzionalità tra cui la revoca immediata di tutti i consensi con l'iscrizione e la possibilità di inserire anche utenze riservate e cellulari, con il definitivo superamento del requisito della presenza negli elenchi pubblici. In tale contesto, l'Autorità ha curato la redazione di alcuni pareri al Mise, sia con riguardo alla bozza di decreto ministeriale relativo alle modalità tecniche di inserimento delle numerazioni non presenti negli elenchi telefonici, sia con riguardo ai numerosi quesiti emersi a seguito della consultazione pubblica curata dal Ministero stesso relativa al nuovo Rpo (cfr. par. 3.1.3).

Tenuto conto della quantità di segnalazioni pervenute e del livello di complessità delle indagini necessarie ad individuare i reali realizzatori delle chiamate, è stato creato un sistema automatizzato che consente di raccogliere le istanze dei cittadini e gli elementi utili per eventuali istruttorie direttamente tramite il sito web istituzionale, e, al contempo, di fornire un primo riscontro immediato agli istanti, personalizzato in base alle informazioni inserite nel modulo *online*.

Dal momento della sua introduzione, il 10 novembre 2022, il sistema ha registrato un immediato riscontro da parte dell'utenza.

Già nella prima giornata, senza che vi fosse stato alcun avviso nel sito web e nei consueti canali di comunicazione, sono pervenute centinaia di segnalazioni. Il ritmo è cresciuto nei giorni successivi tanto che, in un solo mese, sono state raggiunte quasi 11.000 segnalazioni, pari a oltre 14.000 telefonate segnalate. Il numero è ancora più impressionante se si tiene presente che nell'anno 2021 le segnalazioni pervenute

all'Autorità, nel settore del *telemarketing*, sono state circa 4.000. Purtroppo, moltissime segnalazioni non risultano utili per via del mancato rispetto delle regole di compilazione da parte dell'utenza.

Nel corso del 2022, nell'ambito dei compiti previsti dall'art. 57, par. 1, lett. *m*), del RGPD, dopo alcune preliminari interlocuzioni con gli *stakeholders* e dopo la creazione di un più ristretto gruppo di lavoro, sono stati avviati specifici incontri con i rappresentanti di tutte le categorie interessate delle attività di *telemarketing* e *teleselling* (committenti, fornitori di banche dati, *call center* e consumatori). All'esito di tali incontri, le associazioni di categoria che si sono fatte promotrici del progetto hanno sottoposto alla consultazione pubblica una bozza di codice di condotta, trasmettendo all'esito il testo definitivo al Garante per l'approvazione. A fine dicembre, è stato fornito riscontro alle associazioni proponenti dando atto di piccole modifiche necessarie per poter giungere all'approvazione del documento. Il lavoro di alto valore e in tempi assai contingentati svolto da tutti i partecipanti ha reso possibile la redazione del testo e la sua messa in consultazione nel giro di pochissimi mesi, segno dell'elevato livello di interesse presente in un settore economico gravemente leso dalle numerose attività di *telemarketing* illegali.

11.1.7. Marketing *e profilazione*

L'Autorità ha individuato e promosso più istruttorie anche con accertamenti ispettivi, volti alla verifica di eventuali criticità nei trattamenti di dati anche con riferimento al settore delle *fidelity card* e della profilazione.

In particolare, il 20 ottobre 2022 è stato adottato un provvedimento (n. 348, doc. web n. 9825667), con il quale il Garante, a conclusione di un procedimento avviato a seguito di un reclamo, ha comminato una sanzione di euro 1 milione e 400 mila. Alla società destinataria del provvedimento è stato ingiunto di adottare una serie di misure per conformarsi alla normativa, con particolare riguardo alla trasparenza dell'informativa e ai tempi di conservazione dei dati per fini di *marketing* e profilazione. La società ha dovuto inoltre modificare l'impostazione della propria *app*, una delle modalità di raccolta dei dati personali dei clienti, distinguendo chiaramente i contenuti dell'informativa e, in particolare, indicando solo i trattamenti effettivamente svolti e le finalità perseguite. Dall'istruttoria è emerso che la società, nata nel 2019 dall'incorporazione di tre aziende del settore, una volta acquisiti i dati dalle aziende incorporate li aveva lasciati per lungo tempo "inerti" e non si era preoccupata di richiedere alcun consenso al trattamento per le proprie attività. La medesima, quindi, ha dovuto cancellare i dati risalenti a più di dieci anni (fatti salvi contenziosi in atto) e scegliere se cancellare, oppure pseudonimizzare, quelli più recenti. Nel caso avesse deciso di pseudonimizzarli, la società è stata invitata a darne pubblicità nel proprio sito ed inviare una comunicazione ai clienti per i quali disponesse delle coordinate di posta elettronica, informandoli che, in caso di mancato rinnovo della *fidelity card*, entro sei mesi i loro dati sarebbero stati cancellati. Alla società è stato infine ingiunto di adottare soluzioni organizzative e tecniche volte ad assicurare la corretta conservazione dei dati dei propri clienti nel rispetto dei principi di finalità e minimizzazione previsti dal Regolamento europeo.

11.1.8. Attività svolte nell'ambito della tutela del consumatore nei servizi di comunicazione elettronica

Il Garante è presente tra le autorità competenti a cooperare nel *network* europeo CPC (*Consumer Protection and Cooperation*) in base al regolamento (UE) 2017/2394 del Parlamento europeo e del Consiglio sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori e che abroga il

regolamento (CE) 2006/2004, entrato in vigore il 12 dicembre 2017 e applicabile a decorrere dal 17 gennaio 2020.

In particolare, il Garante è competente ad intervenire in caso di violazione delle norme di cui all'art. 13 della direttiva 2002/58/CE, attuato nell'art. 130 del Codice *privacy* in materia di comunicazioni indesiderate.

A tal fine, l'Autorità ha preso parte ad una serie di incontri con la Commissione europea e con altre autorità europee in materia di tutela del consumatore, volti ad avviare tavoli di studio e confronto sulle tematiche di comune interesse e sui possibili margini di cooperazione.

12 Servizi di comunicazioni elettroniche e internet

12.1. *Accesso all'*account *di posta elettronica*

Con provvedimento 7 aprile 2022, n. 127 (doc. web n. 9771545) l'Autorità si è occupata dell'utilizzo della casella di posta elettronica aziendale assegnata ai lavoratori e delle tutele spettanti ai medesimi in caso di improvviso impedito accesso e/o utilizzo della stessa. La peculiarità della fattispecie risiede nella tipologia di lavoratore coinvolto (agente di commercio), quindi lavoratore autonomo e non subordinato, come solitamente si rileva negli atti pervenuti all'Autorità. La società, senza alcun preavviso né comunicazione successiva, aveva inibito alla dipendente l'accesso al suo *account*, utilizzato per le relazioni commerciali, che risultava però ancora attivo. La lavoratrice infatti continuava a ricevere nel suo *computer* e nel telefono gli avvisi e le richieste di immettere la nuova *password* di accesso, cambiata da remoto a sua insaputa. L'interessata aveva segnalato l'accaduto alla società, chiedendo il tempestivo ripristino della casella di posta, che conteneva comunicazioni di lavoro e personali, ma non avendo ricevuto risposta si era rivolta al Garante. A seguito dell'accertamento ispettivo, delegato al Nucleo speciale *privacy* della Guardia di finanza, l'Autorità ha ribadito gli obblighi informativi e quelli di corretta e trasparente gestione della casella di posta aziendale a carico della società, precisando che il fatto che la reclamante fosse un'agente e non una lavoratrice subordinata non rilevava ai fini della necessità di tali adempimenti.

Numerose le violazioni contestate all'azienda: omesso riscontro alla richiesta di informazioni del Garante, inosservanza del principio di limitazione della conservazione dei dati, inesistente o incompleta documentazione relativa al rilascio di un'idonea informativa, mancata risposta all'istanza di accesso dell'interessata e inibizione del suo *account* aziendale. Rilevati gli illeciti, il Garante ha erogato una sanzione di euro 50.000,00 ed evidenziato, mediante misure correttive, che il lavoratore, a prescindere dalla tipologia del rapporto con esso intercorrente, va sempre informato in maniera esaustiva sul trattamento dei suoi dati e che il datore di lavoro deve rispettarne i diritti, le libertà fondamentali e la reputazione professionale.

In un altro caso, a seguito di un reclamo nei confronti di un'associazione di volontariato è stato adottato il provvedimento 6 ottobre 2022, n. 325 (doc. web n. 9828076). Al reclamante, già presidente dell'associazione, dopo l'espulsione dal sodalizio, era stato bloccato l'*account* di posta elettronica messogli a disposizione dall'associazione, rendendogli di fatto impossibile il recupero di documenti e missive di sua pertinenza. All'esito dell'istruttoria, il Garante con un provvedimento prescrittivo e sanzionatorio ha osservato che la scelta adottata dall'associazione di impedire al reclamante l'accesso, sia pur temporaneo, alla propria casella di posta elettronica, al fine di recuperare missive e documenti in essa contenuti, era stata errata in diritto e lesiva dei diritti e delle libertà dello stesso reclamante. A questi era stato impedito di riappropriarsi delle informazioni personali presenti nell'*account* dell'associazione, utili anche al fine di opporsi al provvedimento di espulsione adottato nei suoi confronti, nonché di ricostruire il patrimonio informativo relativo alla propria attività in qualità di socio. L'Autorità ha quindi ingiunto all'associazione di dare riscontro alle richieste del reclamante, consentendogli l'accesso al proprio

account di posta e ha applicato alla medesima una sanzione amministrativa pecuniaria che ha tenuto conto della sua finalità non lucrativa ma anche della gravità della condotta, considerata la natura dei dati trattati, oggetto di tutela costituzionale anche in relazione alla libertà della corrispondenza.

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

Anche in ragione delle significative modifiche normative intervenute il 30 settembre 2021, con il d.l. n. 132/2021, che ha modificato ampiamente l'art 132, comma 3, del Codice, nel corso del 2022, un particolare impegno ha richiesto la trattazione di molteplici segnalazioni e reclami in materia di *data retention*, e in particolare, di mancato o tardivo riscontro ad istanze di accesso ai tabulati per finalità giudiziarie.

In particolare, ad una nota società telefonica, è stata comminata, tra l'altro, una sanzione pecuniaria per un importo di euro 200.000,00 dichiarando illecito il diniego opposto alle richieste di accesso ai tabulati e ingiungendole di trasmettere al difensore del reclamante tali dati ex art. 132 del Codice, in modo tale da consentire il diritto di difesa nell'ambito del procedimento penale in corso (provv. 13 gennaio 2022, n. 10, doc. web n. 9744518).

La società era già stata destinataria nel corso degli anni di analoghi provvedimenti (cfr., tra l'altro, provv.ti 27 maggio 2021, n. 216, doc. web n. 9689324; 8 luglio 2021, n. 272, doc. web n. 9693464; 11 novembre 2021, n. 401, doc. web n. 9722894 e 14 maggio 2020, n. 85, doc. web n. 9442587). Anche per esigenze d'uniformità dell'orientamento dell'Autorità, si è tenuto conto in particolare del citato provvedimento dell'8 luglio 2021, che ha sancito l'obbligo della compagnia telefonica di adottare soluzioni tecniche idonee al recupero dei tabulati i quali, essendo ormai decorso il termine di 24 mesi dalla generazione del traffico, sono conservati unicamente nel *database* riservato alle richieste dell'Autorità giudiziaria nelle attività di contrasto a particolari gravi reati (perlopiù connessi alla criminalità organizzata).

Si deve segnalare che i provvedimenti suindicati sono stati impugnati dalla società e che con sentenza n. 21314 del 1° luglio 2022 la Corte di cassazione ha respinto il ricorso del Garante avverso la decisione del Tribunale di Milano che aveva annullato il provvedimento n. 85 del 2020, doc. web n. 9442587 (cfr. par. 20.2).

12.3. Cookie *e profilazione tramite utilizzo di nuove tecnologie*

Nell'ottobre 2022, anche a seguito di segnalazioni e reclami è stata avviata un'istruttoria nei confronti di alcune imprese editoriali che con sistemi e filtri ad *hoc* condizionano l'accesso ai propri contenuti alla sottoscrizione di un abbonamento (cd. *paywall*) o, in alternativa, al rilascio del consenso da parte degli utenti all'installazione di *cookie* e altri strumenti di tracciamento dei dati personali (cd. *cookie wall*). Tali iniziative sono esaminate alla luce del quadro normativo, anche al fine di valutare l'adozione di eventuali interventi in materia.

Nell'ambito dei compiti di sorveglianza sull'evoluzione delle nuove tecnologie che incidono sulla protezione dei dati personali, a gennaio 2022 è scaduto il termine di sei mesi dalla pubblicazione in G.U. (9 luglio 2021) delle linee guida in materia di *cookie* e altri strumenti di tracciamento (doc. web n. 9677876). Da gennaio, pertanto, l'Autorità ha curato numerose istruttorie relative a segnalazioni, quesiti e

richieste di pareri in materia, nonché una serie di accertamenti ispettivi per verificare il rispetto delle indicazioni contenute nelle menzionate linee guida. Il Garante ha proseguito la partecipazione ai lavori della *taskforce* europea sui *cookie banner* iniziata l'8 novembre 2020 su mandato della plenaria dell'EDPB a seguito della ricezione di reclami provenienti dall'organizzazione austriaca senza scopo di lucro NOYB – *European Centre for Digital Rights* – e ha collaborato alla realizzazione di un video informativo istituzionale, pubblicato nel sito del Garante.

Sempre in tema di strumenti di tracciamento dei dati personali, da un reclamo in materia di diritto all'oblio rispetto ai motori di ricerca nazionali, oltre che a Google, è emersa la necessità d'indagare, prima mediante richieste cartolari e, poi, non rivelandosi risolutive, mediante accertamento *in loco*, i trattamenti di dati riconducibili ai titolari dei detti motori, con particolare riguardo alla conservazione dei dati di navigazione ed alla loro comunicazione a Google nonché alle attività di *marketing* e profilazione indicate nei rispettivi siti web. Dall'accertamento condotto lo scorso aprile, sono emerse ipotesi di violazioni con riferimento non solo al citato passaggio di dati, ma anche alla raccolta dei dati (ed ai successivi trattamenti) mediante i *form* relativi a siti web e i *cookie*, venendo in rilievo alcuni meccanismi di consenso non libero e specifico per le singole finalità di trattamento perseguite. Le relative possibili violazioni sono state oggetto di contestazione ex art. 166, comma 5, del Codice, con contestuale avvio del relativo procedimento.

12.4. *Raccolta e pubblicazione dati* online

A seguito di alcuni accertamenti ispettivi, l'Autorità ha adottato un provvedimento nei confronti di una società cui fanno capo due piattaforme di comparazione prezzi per le assicurazioni, utilizzate anche come strumento di raccolta di dati personali per la creazione di banche dati finalizzate ad attività di *marketing* (provv. 15 dicembre 2022, n. 430, doc. web n. 9860553). Gli accertamenti hanno dato atto di alcune anomalie tecniche che avevano comportato una modifica dei consensi acquisiti, documentandone il conferimento all'insaputa degli interessati. Inoltre, i dati personali risultavano conservati *sine die*. Tenuto conto del fatto che la società è stata sempre molto collaborativa e ha tempestivamente provveduto a sanare ogni difformità, non si è ritenuto necessario adottare alcuna misura correttiva. Tuttavia, considerate alcune violazioni accertate, si è applicata una sanzione amministrativa pecuniaria pari a euro 120.000,00.

Nell'ambito dell'istruttoria avviata nei confronti del titolare di un sito web, l'Autorità ha statuito che è illecita la creazione di elenchi telefonici pubblici che non siano stati estratti dal *database* unico (provv. 26 maggio 2022, n. 204, doc. web n. 9780409). Il sito era risultato destinatario di numerose segnalazioni di persone che si trovavano inserite in tale elenco a loro insaputa senza riuscire ad esercitare il diritto di cancellazione. La tematica era stata più volte segnalata al Garante anche con riguardo ad un analogo sito web, per il quale sono stati ultimati complessi accertamenti per individuare il titolare del trattamento, al quale sono state contestate le violazioni accertate. Il provvedimento di divieto del trattamento e sanzionatorio è stato impugnato.

Sempre in tema di pubblicazione di dati *online*, l'Autorità ha adottato un provvedimento sanzionatorio nei confronti del titolare di un sito web, il quale non aveva ottemperato alla richiesta del reclamante di vedere cancellati i suoi dati dal sito in quanto non disponeva di procedure organizzative adeguate a gestire la propria attività. Tale attività era stata completamente delegata ad un responsabile che non

era stato in grado di dare riscontro alle richieste del titolare (provv. 10 febbraio 2022, n. 48, doc. web n. 9756853).

12.5. *Violazione dei diritti dell'interessato in rete*

In esito ad una complessa istruttoria, avviata anche a seguito di alcuni reclami e segnalazioni, il 10 febbraio 2022, è stato adottato il provvedimento n. 50 (doc. web n. 9751362) nei confronti di una società statunitense che aveva sviluppato un sistema di riconoscimento facciale che sfrutta un *database* di immagini (all'epoca degli accertamenti contenente oltre 10 miliardi di immagini di volti di persone di tutto il mondo) raccolte da fonti *online* pubbliche tramite tecniche di *web scraping*. Il sistema, attraverso l'utilizzo dell'intelligenza artificiale, consente la creazione di profili basati sui dati biometrici estratti dalle immagini, eventualmente arricchiti con altre informazioni ad esse correlate, come il titolo e la geolocalizzazione della foto e della pagina web di pubblicazione.

Le risultanze dell'istruttoria hanno rivelato che i dati personali detenuti dalla società, inclusi quelli biometrici e di geolocalizzazione, erano stati trattati senza un'adeguata base giuridica ed in violazione di altri principi fondamentali del Regolamento, come quelli relativi agli obblighi di trasparenza, di limitazione della finalità e della conservazione.

Con il citato provvedimento, adottato al di fuori del meccanismo dello "sportello unico" – pur trattandosi di un trattamento transfrontaliero di dati personali – in quanto la società non è stabilita nell'Unione europea, il Garante ha inflitto alla società una sanzione amministrativa di 20 milioni di euro, ha vietato ogni ulteriore raccolta e trattamento dei dati di persone che si trovano in Italia e ha ordinato la cancellazione di quelli, sempre relativi a persone che si trovano in Italia, già raccolti e trattati. Il Garante ha, infine, imposto alla società di designare un rappresentante nel territorio dell'Unione europea ai sensi dell'art. 27 del RGPD che funga da interlocutore, in aggiunta o in sostituzione del titolare del trattamento dei dati con sede negli Stati Uniti, al fine di agevolare l'esercizio dei diritti degli interessati.

In data 6 ottobre 2022, a seguito di un'istruttoria avviata d'ufficio, il Garante ha adottato il provvedimento n. 377 (doc. web n. 9828901) nei confronti di un'altra società statunitense gestrice di un noto *social network*. Si tratta di una piattaforma disponibile al pubblico tramite la relativa applicazione, basata esclusivamente su interazioni vocali che si svolgono in stanze di conversazione; gli utenti possono scegliere di aprire una stanza tematica o accedere ad una stanza altrui come ascoltatori e, dal gennaio 2022, possono anche conservare e registrare parte delle conversazioni avvenute sulla piattaforma e condividerle con terzi. All'epoca degli accertamenti, il *social* contava più di 16 milioni di utenti globali di cui circa 90 mila in Italia.

Al termine di una complessa attività istruttoria il Garante ha accertato numerose violazioni del Regolamento tra cui una scarsa trasparenza sull'uso dei dati degli utenti e dei loro "amici", la possibilità per gli utenti di memorizzare e condividere gli audio in assenza del consenso delle persone registrate, la profilazione e la condivisione delle informazioni sugli *account* senza l'individuazione di una corretta base giuridica, tempi indefiniti di conservazione delle registrazioni effettuate dal *social* per attività di contrasto ad eventuali abusi.

Il Garante ha ordinato alla società di adottare una serie di misure per conformare i suoi trattamenti al Regolamento; in particolare introdurre una funzionalità che consenta agli utenti di apprendere, prima dell'ingresso nella stanza di conversazione, della possibilità che la *chat* venga registrata, introdurre un meccanismo per informare

coloro che non sono ancora utenti sull'uso che verrà effettuato dei loro dati personali, integrare l'informativa, specificando quale base giuridica si applichi ad ogni finalità del trattamento, i tempi di conservazione dei dati personali e dei *file* audio e le informazioni necessarie con riferimento al rappresentate designato ai sensi dell'art. 27 del RGPD ed, infine, compiere una valutazione d'impatto sui trattamenti di dati effettuati. Il Garante ha inoltre imposto un divieto di ogni ulteriore trattamento delle informazioni svolto per *marketing* e profilazione senza uno specifico consenso ed inflitto una sanzione amministrativa pecuniaria pari a euro 2 milioni.

All'esito di una lunga istruttoria, è stato adottato un provvedimento di avvertimento generale nei confronti di TikTok (provv. 7 luglio 2022, n. 248, doc. web n. 9788429, cfr. par. 9.3) per possibile violazione dell'art. 5, par. 3 della direttiva *e-privacy* e dell'art. 122, d.lgs. n. 196/2003 (che richiedono il consenso degli interessati). L'avvertimento riguarda l'attività di somministrazione di pubblicità commerciale "personalizzata" da parte di TikTok agli utenti maggiorenni, effettuata attraverso la profilazione dei loro comportamenti all'interno del *social network*, almeno nella misura in cui tale profilazione di base, come espressamente riferito dalla società, avviene su "informazioni raccolte automaticamente" e archiviate nel dispositivo degli utenti sulla base non del consenso, bensì di non meglio precisati interessi legittimi del titolare.

Infine, il Garante ha adottato un provvedimento d'urgenza nei confronti di Meta Platforms Ireland Limited circa il trattamento dei dati personali degli utenti raccolti, tramite la funzionalità *Election Day Information*, nelle piattaforme *social* Facebook e Instagram, in occasione delle elezioni politiche del 25 settembre scorso (provv. 21 dicembre 2022, n. 448, doc. web n. 9853406). Il progetto di Meta comporta infatti il trattamento di dati potenzialmente in grado di rivelare gli orientamenti politici di un elevato numero di utenti italiani. La società ha ricevuto un avvertimento formale di diffida dal procedere alla raccolta e aggregazione di tali dati e alla cessione a soggetti terzi non meglio specificati. Il Garante ha agito in via d'urgenza, ai sensi dell'art. 66, par. 1, del RGPD, appropinquandosi il termine ultimo di 90 giorni dalla raccolta previsto da Meta per l'aggregazione dei dati e dopo aver in vano sollecitato l'Autorità capofila sul punto (*Data Protection Commission* irlandese, DPC). Il provvedimento è stato poi notificato alla sede irlandese di Meta e, nel contempo, è stato comunicato proprio alla DPC, al Comitato europeo e alla Commissione, come previsto dalla richiamata disposizione regolamentare, anche in vista di eventuali ulteriori sviluppi ai sensi dell'art. 66, par. 2, del RGPD.

12.6. *Procedure IMI relative a trattamenti transfrontalieri di dati personali effettuati da fornitori di servizi della società dell'informazione*

Il meccanismo dello sportello unico, meglio conosciuto nella formulazione inglese *one stop shop*, costituisce la cartina di tornasole dell'effettività della tutela del diritto fondamentale alla protezione dei dati personali. Come ormai noto, le disposizioni regolamentari hanno disegnato un vero e proprio sistema amministrativo pan-europeo e un meccanismo decisionale condiviso, che si basa sui due principi complementari di cooperazione (tra autorità di controllo) e di coerenza (tra autorità nazionali, Cepd e Commissione). Un meccanismo unico nel suo genere, che è chiamato ad assicurare la tutela degli interessati in tutti i casi di trattamenti transfrontalieri, i quali assumono grande rilevanza soprattutto nell'ambito dei servizi della società dell'informazione.

L'anno 2022 ha confermato la costante, netta affermazione delle procedure

di cooperazione tanto in termini statistici quanto in relazione alla rilevanza delle tematiche trattate, a partire dalla pubblicità comportamentale *online*, al *real time bidding*, fino a giungere alla tutela dei minori nella società dell'informazione, confermandosi così vero e proprio asse portante dell'attività dell'Autorità.

Nel 2022 si è registrato anche un incremento delle procedure di coerenza (artt. 63-67 RGPD) – peraltro tutte su tematiche di grande rilevanza – volte ad ottenere dal Cepd una composizione delle controversie nei casi di disaccordo tra autorità interessate ed autorità capofila. Questo dato è coerente con la progressiva crescita, nel triennio precedente, dei casi di cooperazione e, dunque, con l'ormai piena e completa messa a regime di tutte le procedure sovranazionali previste dal Regolamento.

Tornando, nello specifico, alle procedure di cooperazione, è proseguita la tendenza, già registrata nel 2021, in base alla quale la cooperazione tra le autorità di controllo non è stata limitata alla fase decisionale bensì ricercata e rafforzata sin dalla fase istruttoria, tramite numerose procedure di cooperazione volontaria o di consultazione informale, allo scopo di costruire sin dall'origine dell'istruttoria un consenso condiviso tra le varie autorità, come prescritto anche dall'art. 60, par. 1, del RGPD.

Il Garante ha anche fattivamente contribuito ad alcune rilevanti procedure di assistenza reciproca volontaria. Si tratta di procedimenti che, pur non finalizzati all'adozione di progetti di decisione, rientrano nella prassi di condivisione, ormai da tempo avviata, in particolar modo dalla Autorità irlandese, in relazione alle principali novità ed agli aggiornamenti di cui quest'ultima viene a conoscenza nell'ambito sia della propria attività di controllo sia della interlocuzione con i grandi titolari del mondo delle comunicazioni elettroniche e digitali stabiliti, come noto, presso quello Stato membro.

Molto significativa la collaborazione, già avviata nel 2021, con la *Data Protection Commission* irlandese sull'analisi degli *Smart glasses* "*Ray-ban stories*", un nuovo dispositivo indossabile progettato e commercializzato da Facebook/Meta in collaborazione con Luxottica, dotato anche di assistente vocale.

Nella direzione opposta, è stato il Garante a condividere, tramite una procedura di assistenza reciproca volontaria, con l'Autorità capofila irlandese, ai sensi dell'art. 61 del RGPD, una istruttoria preliminare nei confronti di Apple Distribution International Ltd relativa al servizio di acquisizione di immagini sul suolo nazionale per la realizzazione del servizio *Apple Maps Data Collection*, anche in luoghi inaccessibili alle autovetture e dunque percorribili soltanto a piedi. Il Garante, riconoscendone la competenza, ha ritenuto di richiamare l'attenzione dell'Autorità irlandese in qualità di capofila.

Lo strumento dell'assistenza reciproca volontaria è stato utilizzato anche per trasmettere per competenza all'autorità capofila i reclami di cittadini italiani di cui il Garante è destinatario, nonché la successiva documentazione istruttoria necessaria per giungere alla risoluzione di ciascun caso.

Inoltre, unitamente alle procedure di cooperazione informale (ex art. 60), l'assistenza reciproca volontaria è stata utilizzata per lo scambio di informazioni relative agli orientamenti o alle prassi seguite da ciascuna autorità anche su tematiche di carattere generale. In particolare, il Garante con una procedura di assistenza reciproca volontaria ha richiesto alle altre autorità di controllo di condividere l'interpretazione data, a livello nazionale, del principio di responsabilizzazione (*accountability*) sia a livello amministrativo che giurisprudenziale. La lettura, proposta in più occasioni dal Garante, del principio di *accountability* pare trovare conferma in alcune recenti decisioni e prese di posizione assunte da altre autorità di controllo europee (in particolare, Autorità irlandese, spagnola e tedesca); secondo

tale approccio, il principio in parola richiederebbe un elemento aggiuntivo ed ulteriore rispetto alla sola conformità formale alla disciplina del RGPD.

Quanto ai progetti di decisione, nel 2022 è stata messa a regime e successivamente implementata una nuova procedura. Si tratta di procedimenti denominati di *amicable settlement* ed utilizzati, in particolare, dall'Autorità irlandese, ovverosia progetti di decisione adottati in esito a procedimenti *ad hoc* finalizzati, per l'appunto alla risoluzione amichevole delle controversie tra reclamanti e titolari (in particolar modo riferibili al mancato adempimento all'esercizio dei diritti di cui agli artt. da 15 a 22 del RGPD). Il netto incremento di tali casi era stato previsto, una volta che, a livello europeo, è stato raggiunto un consenso sui presupposti e sulla procedura da seguire per le risoluzioni amichevoli, in esito ad un lungo percorso di cooperazione che si è snodato attraverso l'approvazione di apposite linee guida dell'EDPB (n. 6/2022) sull'*amicable settlement* e di specifici passaggi all'interno delle linee guida (n. 2/2022) sull'applicazione dell'art. 60 del RGPD, nonché attraverso la condivisione degli elementi essenziali di tali progetti di decisione attraverso un caso pilota.

Come sopra anticipato, nel 2022 sono giunte a decisione importanti indagini nei confronti di grandi titolari internazionali stabiliti nell'Unione europea che hanno evidenziato la vitalità del meccanismo dello sportello unico introdotto dal RGPD e l'importanza del coinvolgimento di più autorità nel processo decisionale su tematiche di indiscutibile complessità e attualità.

Tra le numerose decisioni finali cui il Garante ha cooperato, ve ne sono almeno cinque di particolare interesse.

Le prime due si riferiscono a dei progetti di decisione condivisi dall'Autorità irlandese nei confronti di Meta (prima Facebook) rispettivamente in relazione ai servizi offerti attraverso i *social network* Facebook (6 ottobre 2021) e a Instagram (1° aprile 2022). Entrambi i progetti concernevano la liceità della base giuridica contrattuale in relazione al trattamento di dati personali effettuato da Meta sulle rispettive piattaforme all'indomani dell'aggiornamento dei "termini di servizio" (ToS) effettuato a ridosso del 25 maggio 2018, con riferimento al trattamento dei dati degli utenti con finalità di pubblicità personalizzata.

La terza, il cui progetto di decisione è stato condiviso dall'Autorità irlandese il 1° aprile 2022, ha riguardato la liceità della base giuridica contrattuale in relazione al trattamento di dati personali effettuato da WhatsApp nel contesto dell'offerta del servizio di comunicazione e messaggistica, con particolare riferimento ai trattamenti per finalità di miglioramento del servizio e di sicurezza.

Nei confronti di tutti e tre questi progetti di decisione numerose autorità europee, tra cui il Garante, hanno sollevato obiezioni ai sensi dell'art. 60, par. 4, del RGPD, a seguito delle quali, in esito ad un'ulteriore attività di cooperazione che non ha condotto ad una composizione delle divergenze sulle criticità rilevate, l'Autorità irlandese ha avviato la procedura di risoluzione delle controversie avanti al Cepd, ai sensi dell'art. 65, par. 1, lett. *a*), del RGPD.

Il 5 dicembre 2022 il Comitato europeo, in parziale accoglimento delle numerose obiezioni presentate avverso il progetto di decisione irlandese, ha adottato tre decisioni vincolanti (nn. 3/2022, 4/2022 e 5/2022 disponibili *online* su: https://edpb.europa.eu), alla cui stesura il Garante ha fattivamente contribuito, contenenti una serie di principi che l'Autorità irlandese ha recepito nelle sue successive decisioni finali, adottate ai sensi dell'art. 65, par. 6, del RGPD. Tra i punti oggetto di maggiore interesse si segnalano l'interpretazione della base giuridica ex art. 6, par. 1, lett. *b*), del RGPD e del perimetro della "necessità" del trattamento dei dati per l'esecuzione del contratto. In particolare, l'EDPB ha affermato che il concetto di "necessità" non può essere interpretato in modo da violare lo "spirito" del RGPD e che, almeno dal

punto di vista degli interessati, il trattamento dei dati personali per fornire pubblicità personalizzata non è necessario per l'esecuzione del contratto tra loro e Meta che, invece, riguarda la creazione di un profilo sul *social network* e l'utilizzo di questo specifico servizio.

Parimenti rilevante la partecipazione, sempre in sede di Comitato europeo, alla stesura della decisione vincolante in relazione ad un progetto di decisione nei confronti di Meta/Instagram, approvata dall'EDPB in data 28 luglio 2022 (decisione vincolante n. 2/2022, disponibile *online* su: https://edpb.europa.eu) relativa al trattamento di alcuni dati personali di minorenni da parte di Meta nell'ambito del servizio Instagram. Il progetto di decisione riguardava, in particolare, la diffusione da parte del *social network* degli indirizzi *e-mail* e/o numeri di telefono dei minori che utilizzavano la funzione dell'*account* aziendale Instagram, la quale all'epoca dell'accertamento (le impostazioni erano state modificate nelle more) prevedeva l'impostazione pubblica *by default* di tali *account*.

Complessivamente, le sanzioni comminate dall'Autorità irlandese all'esito della procedura di coerenza e in attuazione delle decisioni vincolanti del Comitato europeo ammontano a circa 800 milioni di euro.

Degno di menzione anche l'importante coinvolgimento del Garante nella procedura di cooperazione (definita con condivisione, in seconda battuta, del progetto di decisione proposto dall'Autorità belga da parte delle autorità interessate) relativa al caso I.A.B. Europe. Il procedimento, avviato a seguito della presentazione di una serie di reclami da parte di alcune associazioni europee per la tutela dei diritti civili a diverse autorità di controllo (tra cui anche il Garante, che lo aveva successivamente trasmesso per competenza all'Autorità belga, ai sensi dell'art. 56 del RGPD), concerneva il trattamento di dati personali effettuato da una piattaforma (il cd. TCF, *Transparency and Consent Framework*), sviluppata e gestita da IAB Europe finalizzata alla registrazione delle preferenze e del consenso degli utenti di internet allo svolgimento di aste in tempo reale per la vendita di spazi pubblicitari *online* (cd. *real-time bidding*). Con decisione finale pubblicata il 2 febbraio 2022 (disponibile *online* su: https://edpb.europa.eu) l'Autorità belga, nell'accogliere i reclami presentati, ha ritenuto configurabile la violazione degli artt. 5, par. 1, lett. *a*) e *f*); 6; 12; 13; 14, par. 1; 24; 25; 30; 32; 35 e 37 del RGPD.

Da ultimo, si segnala che, a seguito della decisione adottata al congresso di Vienna nell'aprile 2022 di promuovere ed incentivare un'attività di cooperazione rafforzata in relazione a casi di particolare interesse strategico, il Garante ha deliberato di collaborare con altre autorità di controllo sulla trattazione congiunta di un caso che l'Autorità aveva già delineato come prioritario in quanto di importanza strategica per la tematica correlata (*Internet of Things*).

12.7. *Altre attività di coordinamento a livello europeo*

Inoltre l'Autorità ha seguito stabilmente i lavori relativi all'*iter* di approvazione del nuovo regolamento *e-privacy* presso il Consiglio dell'Unione europea, attualmente in attesa di sviluppi all'esito di diversi triloghi tecnici nel corso della procedura di co-decisione tra Parlamento europeo e Consiglio; al riguardo, ha predisposto diversi contributi per la Presidenza del Consiglio, quale Autorità di coordinamento dei lavori, in vista della predisposizione della posizione comune nazionale sul *dossier*.

Unitamente alle altre delegazioni del *Technology Subgroup*, l'Autorità ha partecipato altresì agli incontri con Google in ambito europeo sulle misure, lo stato

di implementazione e le modalità di profilazione degli utenti alternative ai *cookie* che potrebbero essere realizzate per il tramite della Google *Privacy Sandbox*.

L'Autorità ha inoltre collaborato alla redazione del parere sul regolamento 2021/1232 del 14 luglio 2021 relativo a una "deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali *online* sui minori" ed ha partecipato alla redazione della *Joint Opinion* dell'EDPB e EDPS sulla bozza di regolamento del Parlamento e del Consiglio, dell'11 maggio 2022, che stabilisce regole per prevenire e combattere gli abusi sessuali sui bambini (CSAM - *child sexual abuse materials*).

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

13.1. *Trattamenti di dati mediante dispositivi tecnologici nel rapporto di lavoro privato*

Anche nel corso dell'anno di riferimento, l'Autorità ha ricevuto numerosi reclami e segnalazioni relativi a trattamenti di dati personali effettuati nel contesto del rapporto di lavoro mediante strumenti tecnologici.

Conformemente al proprio orientamento consolidato, 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 CEDU sia alla sfera privata che a quella professionale (v. Niemietz c. Allemagne, 16 dicembre 1992, ric. n. 13710/88, par. 29; Copland c. UK, 3 aprile 2007, ric. n. 62617/00, par. 41; Barbulescu v. Romania [GC], 5 settembre 2017, ric. n. 61496/08, parr. 70-73; Antović and Mirković v. Montenegro, 28 novembre 2017, ric. n. 70838/13, parr. 41-42).

I provvedimenti dell'Autorità in materia tengono conto della necessità di applicare il vigente quadro normativo caratterizzato da reciproci rinvii operati dal legislatore – anche in sede di adeguamento dell'ordinamento nazionale alle norme del RGPD – alla disciplina in materia di protezione dei dati personali (artt. 113, 114 e 171 del Codice; art. 88 del RGPD) e alle norme di settore sui controlli a distanza (l. n. 300/1970 e succ. mod.).

Il Garante ha anche fornito prime indicazioni in materia di protezione dei dati a seguito dell'entrata in vigore del d.lgs. 27 giugno 2022, n. 104 in materia di condizioni di lavoro trasparenti e prevedibili (cd. decreto trasparenza). Con una comunicazione inviata al Ministero del lavoro e all'Ispettorato nazionale del lavoro in risposta ai numerosi quesiti ricevuti da p.a. e imprese, l'Autorità ha trasmesso un documento di indirizzo volto a fornire alcuni chiarimenti sul coordinamento tra le nuove disposizioni e la disciplina in materia di trattamento dei dati personali. Il Garante, in particolare, ha chiarito che gli obblighi di informazione dei lavoratori in caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati ai fini della assunzione o del conferimento dell'incarico, o per altre attività collegate al rapporto di lavoro e alla sua gestione, non sostituiscono quelli già previsti dal RGPD. Restano inoltre salve le tutele previste dalla legge n. 300/1970 (Statuto dei lavoratori), espressamente richiamate (come sopra ricordato) e dal Codice. L'adozione di sistemi di monitoraggio nel contesto lavorativo deve quindi essere oggetto di una preliminare verifica, da parte del datore di lavoro, delle condizioni di liceità stabilite dalla disciplina in materia di controlli a distanza, nonché di una valutazione dei rischi per verificarne l'impatto sui diritti e sulle libertà degli interessati. Infine, con riguardo a sistemi particolarmente invasivi, come gli strumenti di *machine learning*, di *rating* e *ranking*, il Garante ha sottolineato che il loro impiego pone dubbi di compatibilità con il principio di proporzionalità nonché con gli altri principi di protezione dei dati e con le norme nazionali di settore a tutela della libertà, della dignità e della sfera privata del lavoratore (doc. web n. 9844960).

Account di posta elettronica aziendale

Il Garante ha adottato un provvedimento nei confronti di una società che, in qualità di titolare del trattamento, aveva effettuato alcune operazioni di trattamento in violazione della disciplina in materia di protezione dei dati personali, con riguardo

13

sia all'*account* di posta elettronica aziendale individualizzato (assegnato durante il rapporto di lavoro) sia all'esercizio del diritto di accesso ai dati ex art. 15 del RGPD, per avere fornito alla reclamante un riscontro tardivo ed inidoneo.

Per quanto riguarda il trattamento relativo all'*account* di posta elettronica aziendale, è stato verificato che la società, a seguito della cessazione del rapporto di lavoro, aveva:

- mantenuto attivo per alcuni mesi lo stesso con lo scopo, dichiarato durante l'istruttoria, di garantire l'operatività aziendale e di difendersi nel contenzioso nel frattempo insorto con la reclamante;
- recuperato 34.000 *e-mail* che, secondo quanto dichiarato dalla società, erano state cancellate dal predetto *account*;
- attivato un sistema di indirizzamento automatico delle *e-mail* ricevute dal predetto *account*, successivamente alla cessazione del rapporto di lavoro, ad altro indirizzo di posta elettronica della società, accessibile da propri dipendenti;
- conservato le comunicazioni elettroniche inviate e ricevute attraverso gli *account* di posta aziendali, compreso quelle oggetto di reclamo, per dieci anni dalla data di registrazione del messaggio nella casella di posta.

La condotta della società, consentendo di ricostruire l'attività di un dipendente e di effettuare un controllo sulla stessa, al di là delle finalità tassativamente ammesse dall'art. 4, l. n. 300/1970 e comunque in assenza delle garanzie procedurali previste nello stesso art. 4, ha comportato un trattamento di dati personali illecito, in violazione del principio di liceità del trattamento (art. 5, par. 1, lett. *a*), del RGPD), in relazione all'art. 114 del Codice laddove richiama l'art. 4., l. n. 300/1970, come condizione di liceità del trattamento, nonché dell'art. 88 del RGPD. L'art. 114 costituisce infatti una delle norme del diritto nazionale "più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro" individuate dal citato art. 88 del RGPD. L'Autorità ha ribadito in proposito che "tale disciplina […] pure a seguito delle modifiche disposte con l'art. 23 del d.lgs. 14 settembre 2015, n. 151 non consente l'effettuazione di attività idonee a realizzare il controllo massimo, prolungato e indiscriminato dell'attività del lavoratore".

In relazione a tali condotte il Garante ha, altresì, accertato:

- la violazione dell'art. 13 del RGPD per non avere la società informato l'interessata del trattamento, nonché dell'art. 5, par. 1, lett. *a*), del RGPD, in quanto in tale ambito l'obbligo di informare il dipendente è espressione del principio generale di correttezza;
- che il regolamento aziendale per l'utilizzo degli strumenti informatici, adottato successivamente alla cessazione del rapporto di lavoro con la reclamante, non era conforme ai principi di cui all'art. 5 del RGPD in merito alle attività di controllo sui propri dipendenti;
- la violazione del principio di minimizzazione dei dati. In proposito è stato richiamato l'orientamento dell'Autorità secondo il quale l'adozione di appropriate misure organizzative e tecnologiche consente di individuare i documenti che, nel corso dello svolgimento dell'attività lavorativa, devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile; i sistemi di posta elettronica non consentono, per loro stessa natura, di assicurare tali modalità.

In merito, inoltre, alla rappresentata necessità di conservazione delle *e-mail* per dieci anni per fini probatori, è stato 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".

L'attività di indirizzamento delle comunicazioni elettroniche su altro *account* è stata effettuata in violazione dell'art. 5, par. 1, lett. *a*), *c*), *e*) nonché dell'art. 6 del RGPD.

Per quanto riguarda infine il diritto di accesso, è risultata comprovata la violazione degli artt. 12 e 15 del RGPD.

Considerate le violazioni accertate, è stato disposto il divieto dell'ulteriore trattamento dei dati estratti dall'*account* di posta elettronica aziendale riferito alla reclamante, fatta salva la loro conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria, per il tempo necessario a tale scopo, tenuto conto dell'art. 160-*bis* del Codice; è stato inoltre ingiunto alla società di conformare il regolamento aziendale per l'utilizzo degli strumenti informatici alla disciplina di protezione dei dati e disposta l'applicazione di una sanzione amministrativa pecuniaria (provv. 21 luglio 2022, n. 255, doc. web n. 9809466).

Inoltre a seguito di una segnalazione di un sindacato, il Garante ha accertato che una regione aveva monitorato i dipendenti che inviavano messaggi a uno specifico sindacato, conservando i metadati della posta elettronica per generiche finalità di sicurezza informatica per 180 giorni, in assenza di idonei presupposti giuridici, violando così i principi di protezione dei dati e delle norme sul controllo a distanza. L'Autorità ha chiarito che la generalizzata raccolta e l'estesa conservazione dei metadati della posta elettronica – che in quanto forma di corrispondenza è tutelata dalla Costituzione – non sono strumentali allo svolgimento della prestazione del dipendente, ai sensi dello Statuto dei lavoratori. In questi casi, infatti, il datore deve avviare le specifiche procedure di garanzia (accordo sindacale o autorizzazione pubblica) previste dalla legge, non potendo i trattamenti di dati personali trovare la propria legittimazione nell'interesse legittimo del titolare o nella cd. teoria dei controlli difensivi, elaborata dalla giurisprudenza. Il trattamento di dati personali posto in essere ha, tra l'altro, consentito al datore di lavoro di entrare in possesso di informazioni relative anche alla sfera privata dei dipendenti, a partire dalle loro opinioni, contatti e fatti non attinenti all'attività lavorativa. Oltre a comminare una sanzione amministrativa pecuniaria, il Garante ha vietato alla regione ogni ulteriore operazione di trattamento dei metadati relativi all'utilizzo della posta elettronica dei lavoratori e disposto la cancellazione di quelli illecitamente raccolti (provv. 1° dicembre 2022, n. 409, doc. web n. 9833530; v. anche *Newsletter* 19 dicembre 2022, doc. web n. 9833616).

Geolocalizzazione

All'esito di un reclamo, con il quale l'interessato ha lamentato il rinvenimento, nel vano motore del proprio veicolo adibito al trasporto di beni, di un dispositivo di geolocalizzazione, l'Autorità ha in primo luogo ribadito che è configurabile un trattamento di dati personali anche qualora il dispositivo completo di funzionalità di geolocalizzazione (tramite sistema Gps) installato sul veicolo aziendale sia associato alla targa del veicolo e non (direttamente) al nome dell'autista, poiché è possibile identificare il guidatore del mezzo anche attraverso l'associazione con altre informazioni (ad es. i documenti relativi ai turni di servizio).

L'attività di geolocalizzazione può essere effettuata da un distinto soggetto che mette a disposizione sia i dispositivi che l'accesso ad un applicativo web che, nel caso di specie, consente la localizzazione mediante sistema Gps e il controllo su mappa della distanza percorsa da ciascun veicolo, il calcolo dei chilometri, del tempo di viaggio e della velocità media di guida.

Il rapporto con il fornitore del servizio deve, tuttavia, essere regolato ai sensi dell'art. 28 del RGPD (responsabile del trattamento).

13

Nel caso di specie la società titolare del trattamento non aveva provveduto a effettuare la designazione del fornitore del servizio di localizzazione, quale responsabile del trattamento, né a impartire allo stesso le dovute istruzioni.

Ciò ha quindi comportato la violazione del richiamato art. 28 del RGPD e anche degli artt. 5, par. 1, lett. *a*) e 6 del RGPD posto che il titolare ha, in tal modo, effettuato una comunicazione a terzi (v. art. 4, n. 10, del RGPD), in assenza di un idoneo presupposto di liceità del trattamento.

Inoltre, in violazione dell'art. 13 del RGPD, non era stata fornita ai collaboratori interessati un'informativa sulle caratteristiche del sistema di localizzazione installato a bordo dei veicoli né era stata effettuata la valutazione di impatto sulla protezione dei dati prevista dall'art. 35 del RGPD. Infine la società aveva effettuato trattamenti di dati dell'interessato anche successivamente all'interruzione del rapporto di lavoro, in assenza di alcuna base giuridica (artt. 5, par. 1, lett. *a*) e 6 del RGPD).

Il Garante ha pertanto disposto l'applicazione di una sanzione amministrativa pecuniaria nei confronti del titolare del trattamento (provv. 15 dicembre 2022, n. 428, doc. web n. 9861249).

Quanto alla società che ha fornito il servizio di localizzazione geografica, nella cui disponibilità tutti i tragitti percorsi rimanevano per un periodo predeterminato, in primo luogo è stato ribadito che l'appartenenza a un gruppo societario la cui capogruppo ha sede legale in un Paese dell'UE non comporta in sé, in assenza di evidenze di trattamenti transfrontalieri (come definiti dall'art. 4, n. 23, lett. *a*) e *b*), del RGPD), l'applicazione delle procedure di cooperazione tra le autorità di protezione dei dati europee, previste dal RGPD.

Nel caso di specie, i trattamenti erano stati effettuati in esecuzione di contratti stipulati dalla società italiana che fornisce il servizio con altra società, avente sede legale in Italia il che escludeva la loro possibile natura transfrontaliera. Né la società italiana risultava essere uno "stabilimento" della società capogruppo.

Si è ritenuto pertanto applicabile l'art. 55 del RGPD che stabilisce la competenza delle autorità di controllo nazionali in relazione ai trattamenti effettuati sul territorio nazionale dal soggetto ivi stabilito, che agisca in qualità di autonomo titolare.

Nel merito, la legittimazione del responsabile del trattamento a trattare i dati degli interessati sulla base della disciplina posta da un contratto o altro atto giuridico che lo vincoli al titolare e "soltanto su istruzione documentata" di quest'ultimo trova ora conferma anche nella pronuncia di Cass., sez. I, civ., ord. 23 luglio 2021, n. 21234 (con riguardo al trattamento di dati personali effettuato in un diverso contesto).

In assenza della dovuta designazione a responsabile, i trattamenti di dati nell'ambito della fornitura del servizio di geolocalizzazione sono risultati effettuati dalla società fornitrice del servizio senza un idoneo presupposto di liceità, in violazione sia dell'art. 28 che degli artt. 5, par. 1, lett. *a*) e 6 del RGPD, (in senso conforme v. precedenti decisioni dell'Autorità, tra cui: provv.ti 17 settembre 2020, nn. 160 e 161, docc. web nn. 9461168 e 9461321 e 11 febbraio 2021, n. 49, doc. web n. 9562852).

Anche nei confronti della società che aveva fornito il servizio di geolocalizzazione è stata pertanto applicata una sanzione amministrativa pecuniaria (provv. 15 dicembre 2022, n. 427, doc. web n. 9856694).

13.2. *Esercizio dei diritti*

Il Garante, nel corso dell'anno di riferimento, nell'esaminare alcuni reclami in materia di esercizio dei diritti, ha ribadito la necessità che, anche nell'ambito del rapporto di lavoro, sia consentito agli interessati l'esercizio effettivo dei diritti

riconosciuti dal RGPD, rammentando tra l'altro, che, 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, informando, altresì, della possibilità di presentare reclamo al Garante o, in alternativa, ricorso giurisdizionale.

Con particolare riferimento al diritto previsto dall'art. 15 del RGPD è stato precisato che il diritto di accesso e il cd. diritto di informativa, seppur correlati, sono diritti differenti, sanciti da distinte disposizioni dell'ordinamento, rispondenti ad esigenze di tutela e garanzia dell'interessato non completamente sovrapponibili.

Diritto di accesso ai dati del lavoratore

Anche nell'ambito del rapporto di lavoro, l'istanza di accesso può riguardare dati personali già in possesso dell'interessato per consentirgli di verificare (anche a "intervalli ragionevoli" di tempo: v. cons. 63 del RGPD) se sia in corso un determinato trattamento e valutarne la liceità e la correttezza. Inoltre il titolare del trattamento è tenuto a soddisfare le richieste dell'interessato con le specifiche modalità e i limiti temporali individuati dall'art. 12 del RGPD, per rendere effettivi i principi di trasparenza e correttezza (v. cons. 58 e 60 del RGPD).

Pertanto, in un caso concreto, la circostanza che in precedenti occasioni fossero state fornite al dipendente informazioni relative ai trattamenti effettuati non poteva giustificare la mancata risposta a una richiesta di esercizio dei diritti peraltro presentata formalmente al datore di lavoro.

In base al RGPD solo se richiesto dall'interessato le informazioni possono essere fornite oralmente (art. 12, par. 1, del RGPD).

Il Garante ha pertanto ritenuto che l'omesso riscontro all'istanza di accesso, presentata dal reclamante, era avvenuto in violazione degli artt. 12, par. 1, 2, 3 e 4, e 15 del RGPD ed ha disposto l'applicazione di una sanzione amministrativa pecuniaria (provv. 15 settembre 2022, n. 305, doc. web n. 9827119).

Tali principi sono stati riaffermati anche in un diverso caso, ribadendo che l'art. 15 del RGPD si pone in rapporto di stretta connessione con l'art. 12 che dispone, a carico del titolare, l'adozione di "misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento".

Accertata pertanto la violazione degli artt. 12 e 15 del RGPD il Garante ha disposto l'applicazione di una sanzione amministrativa pecuniaria (provv. 27 gennaio 2022, n. 19, doc. web n. 9750219).

Distinzione tra informativa e riscontro all'istanza di accesso

Il Garante, in un diverso provvedimento, ha ritenuto che l'obbligo per l'interessato di compilare un modulo predefinito a campi multipli al fine di dare corso alla richiesta di accesso ai sensi dell'art. 15 del RGPD non è conforme in particolare all'obbligo di "agevola[re] l'esercizio dei diritti dell'interessato" previsto dall'art. 12, par. 2, del RGPD, con il quale contrasta la prassi di non considerare istanze eventualmente presentate in forma diversa da quella indicata dal titolare del trattamento.

Inoltre l'Autorità ha chiarito che il diritto di accesso alle informazioni indicate dall'art. 15 del RGPD, in applicazione dei principi di trasparenza e correttezza (art. 5, par. 1, lett. *a*), del RGPD), non può ritenersi soddisfatto per il solo fatto di aver fornito l'informativa di cui agli artt. 13 e 14 del RGPD.

Tutte le informazioni fornite nell'informativa, ai sensi dell'art. 15 del RGPD, devono pertanto essere verificate e declinate alla luce delle concrete operazioni di trattamento effettuate nei confronti del richiedente (in senso conforme anche le *Guidelines 01/2022 on data subject rights - Right of access*, adottate il 18 gennaio 2022 e sottoposte a consultazione pubblica conclusa l'11 marzo 2022).

L'Autorità ha pertanto ravvisato violazione degli artt. 5, par. 1, lett. *a*), 12 e 15 del RGPD, di conseguenza prescritto di soddisfare la richiesta dell'interessato

riguardante l'accesso alle informazioni indicate dall'art. 15, par. 1, lett. *a*) - *g*) e disposto l'applicazione di una sanzione amministrativa pecuniaria.

La società titolare del trattamento ha impugnato la decisione davanti all'Autorità giudiziaria ordinaria.

Con sentenza 6 dicembre 2022, il Tribunale di Milano ha confermato il provvedimento del Garante relativamente alla "contestazione di cui agli artt. 12 e 15 Reg. 679/2016", riducendo l'entità della sanzione pecuniaria e annullato la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione (provv. 16 giugno 2022, n. 225, doc. web n. 9795350).

Diritto di accesso ad attestati di formazione

Con riferimento a un reclamo per il mancato riscontro ad un'istanza di accesso agli attestati di formazione conseguiti durante il rapporto di lavoro, il Garante, dopo avere accertato la violazione degli artt. 12 e 15 del RGPD, ha disposto una sanzione amministrativa pecuniaria nei confronti della società titolare del trattamento.

Nel caso di specie è risultato che il titolare del trattamento, a fronte della presentazione di un'istanza di accesso a seguito della cessazione del rapporto di lavoro, non ha fornito idoneo riscontro.

L'Autorità, richiamando le citate *Guidelines 01/2022 on data subject rights - Right of access*, ha precisato che non grava sugli interessati l'onere di specificare la base giuridica della richiesta di esercizio dei diritti, né l'obbligo di predisporre la richiesta secondo un formato specifico (provv. 1° dicembre 2022, n. 406, doc. web n. 9843805).

Diritto alla cancellazione dei dati

Con riferimento ad un reclamo per il tardivo e inidoneo riscontro ad istanze di cancellazione ex art. 17 del RGPD, la condotta del titolare del trattamento è stata ritenuta in violazione dell'art. 12 con riferimento all'art. 17 del RGPD.

Il titolare, una volta verificata l'identità dell'interessato, non aveva dato seguito all'istanza di cancellazione nei tempi previsti dal RGPD, per un asserito "disguido tecnico" causato dalla "mancata presa in carico dell'adempimento", costringendo l'interessato a sollecitare con una nuova istanza, riscontrata tardivamente, in violazione del termine di 30 giorni dall'art. 12 del RGPD.

Con riferimento, invece, alla mancata cancellazione dei dati riferiti al reclamante (diversi da quelli comunicati ai fini della selezione per un posto di lavoro) attinenti a precedenti rapporti di lavoro intercorrenti con il titolare del trattamento e a rapporti bancari, l'Autorità ha condiviso quanto rappresentato dal titolare del trattamento circa la necessità di conservazione degli stessi, pur rilevando l'assenza dell'indicazione sulla possibilità di proporre reclamo all'autorità di controllo o ricorso giurisdizionale.

In considerazione delle violazioni accertate il Garante ha applicato una sanzione amministrativa pecuniaria (provv. 15 settembre 2022, n. 305, doc. web n. 9815947).

13.3. *Omessa informativa*

Con due provvedimenti i titolari di trattamento nell'ambito del rapporto di lavoro sono stati sanzionati per l'assenza di idonea informativa.

Sistema di videosorveglianza

A seguito della presentazione di una segnalazione è stato accertato che una società, pur avendo conformemente alla procedura di garanzia di cui all'art. 4, l. n. 300/1970, stipulato un accordo con le rappresentanze aziendali in merito al sistema di videosorveglianza attraverso il quale veniva ripresa anche l'attività dei lavoratori, non aveva fornito le informazioni di cui all'art. 13 del RGPD, neanche mediante cartellonistica, né ai dipendenti né ai clienti del locale.

La società si è conformata alla disciplina di protezione dei dati solo a seguito dell'accertamento ispettivo disposto dal Garante.

Precisato che la presa visione da parte dei lavoratori dell'accordo stipulato ai sensi dell'art. 4 della l. 300 del 1970 non è idonea a sostituire l'informativa di cui all'art. 13 del RGPD da fornire anche ai clienti del locale di cui si trattava, è stato ritenuto violato l'art. 13 del RGPD nonché l'art. 5, par. 1, lett. *a*) (principio di correttezza) del RGPD in quanto, nell'ambito del rapporto di lavoro, l'obbligo di informare il dipendente è, altresì, espressione del principio generale di correttezza (provv. 6 ottobre 2022, n. 321, doc. web n. 9827285).

Omessa informativa e trattamento con strumenti tecnologici

Il Garante ha adottato una sanzione amministrativa pecuniaria nei confronti di una società per il trattamento di dati, contenuti nel *personal computer* in uso al reclamante che svolgeva l'attività lavorativa per la società, in assenza di un regolamento o altro specifico documento aziendale.

Per tale ragione sono stati ritenuti violati gli artt. 13 e 12 del RGPD, il quale ultimo, in particolare, dispone che "il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del RGPD" (provv. 10 febbraio 2022, n. 42, doc. web n. 9751137).

13.4. *Trattamenti dei dati biometrici*

Impronte digitali per rilevare le presenze

Il Garante, a seguito di una segnalazione presentata da un sindacato, ha accertato che una società aveva installato un sistema di rilevazione delle presenze dei propri dipendenti basato su tecnologie biometriche.

Il procedimento avviato dall'Autorità è stato aggravato dalla circostanza che il titolare del trattamento non aveva inizialmente fornito riscontro alle richieste di informazioni formulate dall'Autorità ai sensi dell'art. 157 del Codice e ciò ha reso necessario delegare il Nucleo speciale *privacy* e frodi tecnologiche della Guardia di finanza agli accertamenti del caso.

Nel merito è stato in primo luogo ribadito che è configurabile un trattamento di dati biometrici, con conseguente applicazione della specifica disciplina prevista dal RGPD e dal Codice, sia in fase di cd. *enrollment* consistente nella acquisizione delle caratteristiche biometriche – nella specie impronte digitali – dell'interessato (v. punti 6.1 e 6.2 dell'all. A al provv. 12 novembre 2014, n. 513, doc. web n. 3556992), sia nella fase di riconoscimento biometrico, all'atto della rilevazione delle presenze (v. anche punto 6.3 dell'all. A al cit. provv.).

Il trattamento di dati biometrici è di regola vietato in base all'art. 9, par. 1, del RGPD, ammesso per quanto indicato dall'art. 9, par. 2, lett. *b*), del RGPD (v. pure, art. 88, par. 1 e cons. 51-53 del RGPD) ed occorre che sia "in conformità alle misure di garanzia disposte dal Garante" art. 2-*septies*, comma 1, del Codice, in ogni caso nel rispetto dei principi di liceità, correttezza e trasparenza, limitazione delle finalità e minimizzazione (art. 5 del RGPD).

Alla luce delle richiamate disposizioni, il Garante ha ribadito che l'utilizzo del dato biometrico per finalità di ordinaria gestione del rapporto di lavoro non appare conforme ai principi di minimizzazione e proporzionalità del trattamento.

Il trattamento è stato effettuato anche in assenza di un'idonea base giuridica, posto che il consenso del lavoratore non costituisce, di regola, un valido presupposto di liceità per il trattamento dei dati personali in ambito lavorativo, per l'asimmetria tra le parti del rapporto (v., tra gli altri, provv.ti 14 gennaio 2021, n. 16, doc. web n. 9542071; 13 febbraio 2020, n. 35, doc. web n. 9285411; 13 dicembre 2018, n. 500, doc. web n. 9068983; v. altresì artt. 6-7 e cons. 42-43, RGPD; v. anche, in senso conforme, Gruppo Art. 29, linee guida sul consenso ai sensi del RGPD- WP 259 - del 4 maggio 2020, spec. par. 3.1.1; parere 2/2017 sul trattamento dei dati sul

posto di lavoro, WP 249, spec. par. 3.1.1 e 6.2).

È stato infine accertato che l'informativa era del tutto inidonea a rappresentare le caratteristiche essenziali del dispositivo biometrico e che il registro delle operazioni di trattamento predisposto dalla società non indicava i dati biometrici tra i tipi di dati trattati dal titolare, in violazione dell'art. 30, par. 1, lett. *c*), del RGPD.

Il Garante ha pertanto disposto l'applicazione di una sanzione amministrativa pecuniaria nei confronti della società (provv. 10 novembre 2022, n. 369, doc. web n. 9832838).

Specifiche istruttorie sono state inoltre avviate nei confronti di due comuni, per l'installazione di sistemi che consentivano il trattamento dei dati biometrici dei dipendenti per la rilevazione delle presenze al fine di scoraggiare fenomeni di assenteismo. Il Garante ha, anzitutto, chiarito che i trattamenti di dati biometrici, in ambito lavorativo, richiedono un'espressa previsione normativa e specifiche garanzie per i diritti degli interessati. Per tali ragioni in entrambi i casi il Garante ha concluso che in assenza di proporzionate misure legislative e di specifiche garanzie per gli interessati, il trattamento dei dati biometrici per la predetta finalità di rilevazione delle presenze dei dipendenti, non poteva e non può essere effettuato (provv. 15 dicembre 2022, n. 423, doc. web n. 9852800). Né sono state ritenute sufficienti ad escludere la responsabilità del datore di lavoro, le misure tecniche adottate prendendo a riferimento il provvedimento generale prescrittivo in tema di biometria (cfr., provv. 12 novembre 2014, n. 513 doc. web n. 3556992), in assenza dei presupposti di liceità per trattare i dati biometrici dei dipendenti per la specifica finalità considerata (provv. 15 dicembre 2022, n. 422, doc. web n. 9852776).

13.5. *Trattamento del dato relativo allo stato di gravidanza*

Il Garante ha ritenuto illecita la comunicazione effettuata da una società che gestisce un asilo nido alle famiglie dei bambini ivi iscritti concernente lo stato di gravidanza della loro educatrice e la necessità, per la stessa, di assentarsi dal lavoro, in considerazione della qualificazione del ruolo di insegnante come "posizione ad alto rischio".

In particolare risultava violato il diritto dell'interessata di determinare le proprie scelte riguardanti le modalità e i tempi con i quali rendere noto uno stato – avente natura eminentemente privata – a soggetti terzi, estranei al rapporto di lavoro, nell'ambito del quale l'informazione era stata doverosamente resa, peraltro in una fase ancora del tutto iniziale della gravidanza.

Pertanto il trattamento dei dati della reclamante è avvenuto in violazione dei principi di liceità e minimizzazione dei dati (v. art. 5, par. 1, lett. *a*) e *c*), del RGPD), trattandosi di informazioni fornite a terzi non necessarie rispetto alle finalità perseguite e in assenza di un idoneo criterio di legittimazione tra quelli previsti dall'ordinamento (v. art. 6, par. 1, lett. *b*) e *c*), del RGPD).

Il Garante ha disposto l'applicazione di una sanzione amministrativa pecuniaria nei confronti della società (provv. 28 aprile 2022, n. 152, doc. web n. 9776444).

13.6. *Videosorveglianza nel settore privato*

I trattamenti di dati personali nell'ambito del rapporto di lavoro devono svolgersi nel rispetto dei principi generali indicati dall'art. 5 del RGPD, ed in particolare

del principio di liceità, in base al quale il trattamento è lecito se è conforme alle discipline di settore applicabili (art. 5, par. 1, lett. *a*), del RGPD).

Coerentemente con tale impostazione, l'art. 88, del RGPD ha fatto salve le norme nazionali di maggior tutela (norme più specifiche) volte ad assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei lavoratori. Il legislatore nazionale ha approvato, quale disposizione più specifica, l'art. 114 del Codice che tra le condizioni di liceità del trattamento ha stabilito l'osservanza di quanto prescritto dall'art. 4, l. 20 maggio 1970, n. 300.

La violazione delle menzionate disposizioni determina l'illiceità del trattamento e l'applicazione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83, del RGPD, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. *i*), del RGPD), in relazione alla gravità della condotta e alle condizioni economiche dei contravventori.

In tale ambito, nel 2022 l'Autorità ha adottato 19 provvedimenti sanzionatori; in alcuni casi, al pagamento di una sanzione amministrativa si è aggiunta anche la prescrizione di misure correttive al fine di rendere il trattamento conforme alle norme di legge.

In particolare, sono stati emanati provvedimenti sanzionatori per illiceità del trattamento in violazione del principio di trasparenza, dell'obbligo di fornire agli interessati un'idonea informativa (provv.ti 15 settembre 2022, n. 300, doc. web n. 9815745; 28 luglio 2022, n. 273, doc. web n. n. 9812423; 13 gennaio 2022, n. 5, doc. web n. 9745262; 12 maggio 2022, n. 179, doc. web n. 9781966; 28 aprile 2022, n. 168, doc. web n. 9779082; 21 luglio 2022, n. 264, doc. web n. 9810045;), in violazione delle garanzie previste all'art. 4, l. n. 300/1970 richiamato dall'art. 114, d.lgs. n.196/2003 (provv.ti 1° dicembre 2022, n. 407, doc. web n. 9838992; 7 aprile 2022, n. 132, doc. web n. 9823195; 1° dicembre 2022, n. 408, doc. web n. 9838976; 12 maggio 2022, n. 178, doc. web n. 9782434; 7 aprile 2022, n. 121, doc. web n. 9768440; 12 maggio 2022 n. 177, doc. web n. 9788970).

Nel 2022 circa il 60% delle pratiche in materia di videosorveglianza nel settore privato ha riguardato reclami e segnalazioni relativi all'utilizzo di sistemi di videoripresa da parte di persone fisiche per fini esclusivamente personali o domestici.

Al riguardo, mentre l'utilizzo di sistemi di videosorveglianza da parte di persone fisiche nelle aree di diretto interesse (quali quelle inerenti il proprio domicilio e le relative pertinenze) è da ritenersi, in linea di massima, escluso dall'ambito di applicazione materiale delle disposizioni in materia di protezione dati, le linee guida 3/2019 dell'EDPD chiariscono che se la videosorveglianza interessa, anche solo parzialmente, spazi esterni alla sfera privata della persona che effettua il trattamento, questo ricade nell'ambito di applicazione del Regolamento.

Nello stesso senso è la FAQ numero 10, attualmente pubblicata sul sito del Garante tra quelle volte a fornire indicazioni nella materia *de qua* alla luce del RGPD.

In considerazione dell'elevato numero di casi segnalati all'Autorità, in assenza di elementi conclamati di illiceità, l'Ufficio invia al segnalante e al segnalato un riscontro finalizzato a promuovere la consapevolezza riguardo ai limiti che devono essere rispettati da parte di persone fisiche private e agli obblighi imposti dal Regolamento, invitando a verificare che il trattamento sia svolto in conformità a quanto prevede la normativa, confidando sull'adeguamento spontaneo da parte del segnalato.

Nei casi di condotte gravi o violazioni adeguatamente comprovate viene avviata invece un'istruttoria formale, attraverso un accertamento *in loco* prodromico all'eventuale adozione di provvedimenti correttivi.

13

13.7. *La protezione di dati nell'ambito del rapporto di lavoro pubblico. I trattamenti effettuati per finalità di prevenzione dal contagio da Sars-CoV-2*

Nel corso del periodo di riferimento, l'Autorità ha continuato a fornire indicazioni e chiarimenti, ai sensi dell'art. 57, par. 1, lett. *b*) e *d*), del RGPD, agli interessati e ai titolari a vario titolo coinvolti nei trattamenti di dati personali in ambito lavorativo nel quadro dell'emergenza epidemiologica da Sars-CoV-2, avviando campagne di informazione presso il pubblico e adottando specifici documenti di indirizzo volti, in particolare, a prevenire autonome decisioni o iniziative dei datori di lavoro non previste dalla legge, con possibili effetti discriminatori per gli interessati. L'Autorità in molteplici occasioni è stata chiamata a fornire il proprio parere, ai sensi dell'art. 58, par. 3, lett. *b*), del RGPD, sulle disposizioni attuative di un quadro normativo in costante aggiornamento, che ha interessato in modo particolare il settore del lavoro.

13.7.1. La vaccinazione anti Sars-CoV-2 come requisito professionale e le certificazioni verdi per accedere ai luoghi di lavoro

In tale quadro il Garante ha reso in via d'urgenza il proprio parere favorevole sullo schema di d.P.C.M., che ha disciplinato, tra l'altro, le modalità automatizzate di verifica del requisito vaccinale per il personale delle università, delle istituzioni di alta formazione artistica, coreutica e musicale e degli istituti tecnici superiori, nonché i trattamenti di dati personali connessi alle nuove modalità di verifica delle certificazioni verdi Covid-19 nel contesto lavorativo (cfr. 5.1). Le disposizioni hanno tenuto conto delle indicazioni fornite dall'Autorità per assicurare il corretto adempimento degli obblighi di verifica da parte dei datori di lavoro, nonché il rispetto della disciplina di protezione dei dati personali e di quella applicabile al contesto lavorativo (art. 88 del RGPD e 113 del Codice). Le verifiche sono state previste sfruttando sistemi informativi già esistenti e accessibili da parte dei singoli datori di lavoro. In particolare, il Ministero della salute ha reso disponibili ai responsabili delle istituzioni tenuti a effettuare i controlli specifiche funzionalità per la verifica automatizzata della sola informazione di tipo booleano relativa al rispetto dell'obbligo vaccinale (semaforo verde: lavoratore vaccinato o esente; semaforo rosso: lavoratore non vaccinato), e non anche le ulteriori informazioni conservate, o comunque trattate, nell'ambito della piattaforma nazionale *Digital Green Certificate* (DGC). È stato inoltre previsto che le eventuali variazioni dello stato vaccinale del personale dipendente fossero rese note rispetto alla precedente interrogazione per consentire alle università di portare tale circostanza all'attenzione dei verificatori assicurando al contempo la semplificazione del processo di verifica e il trattamento di dati aggiornati.

Nel parere è stato ricordato che i trattamenti effettuati per la verifica del requisito professionale della vaccinazione devono essere tenuti separati da quelli effettuati per la verifica quotidiana del possesso della certificazione verde Covid-19 per l'accesso fisico alle sedi di lavoro, nel rispetto delle condizioni e dei limiti previsti da norme distinte. Quanto alle modalità di verifica del possesso della certificazione verde, le disposizioni attuative sono state aggiornate tenendo conto dell'obbligo introdotto per i lavoratori ultracinquantenni di esibire, per l'accesso ai luoghi di lavoro, dal 15 febbraio 2022, una certificazione verde Covid-19 di avvenuta vaccinazione o guarigione (cfr. art. 4-*quinquies*, d.l. n. 44/2021, introdotto dal d.l. 7 gennaio 2022, n. 1). Al riguardo la verifica del possesso delle diverse tipologie di certificazioni verdi Covid-19 è stata resa possibile senza visibilità delle informazioni che ne hanno determinato l'emissione (vaccinazione, esenzione, guarigione, o tampone negativo) sulla base della data di nascita riportata all'interno della certificazione verde di

ciascuno, semplificando le procedure di verifica e, al contempo, riducendo il rischio di utilizzo improprio o non corretto (provv. 18 febbraio 2022, n. 57, doc. web n. 9746905).

13.7.2. Trattamenti di dati personali nell'ambito di una campagna di screening *anti Covid-19: il ruolo del datore di lavoro*

Su segnalazione di un'organizzazione sindacale è stato adottato un provvedimento sanzionatorio nei confronti del Corpo di polizia locale di un comune per i trattamenti di dati personali effettuati in occasione di una campagna di *screening* anti Covid-19 indirizzata dall'autorità sanitaria competente agli agenti di polizia municipale. Come emerso nel corso dell'istruttoria, il Comando aveva raccolto le adesioni degli agenti, inviato all'azienda sanitaria i loro dati identificativi e di contatto, poi trasmessi alle unità operative a cui appartenevano i lavoratori aderenti, con la data e l'orario in cui ciascun dipendente avrebbe dovuto sottoporsi al test anti-Covid presso l'azienda sanitaria competente.

Il Garante ha al riguardo ricordato che, anche nella situazione emergenziale, i datori di lavoro devono operare solo nell'ambito e nei limiti previsti dalla disciplina applicabile, che costituisce la base giuridica dei relativi trattamenti. In assenza di espresse previsioni normative, non è pertanto consentito al datore di lavoro raccogliere informazioni relative alla sfera privata o alle convinzioni personali dei lavoratori, ivi compresa l'intenzione o meno di aderire ad una campagna di *screening*, in ragione delle disposizioni nazionali che vietano il trattamento di dati non rilevanti rispetto all'attività lavorativa (art. 88 del RGPD e art. 113 del Codice). È stato ricordato che l'autorità sanitaria può raggiungere le categorie di interessati anche tramite i datori di lavoro, coinvolti dal dipartimento di prevenzione locale, per veicolare l'invito di adesione alla campagna tra i propri dipendenti, fermo restando che la titolarità del trattamento resta sempre in capo alla struttura sanitaria che, pertanto, è l'unica legittimata a raccogliere le adesioni e a comunicare i risultati agli interessati. Il datore di lavoro, invece, deve limitarsi a svolgere un ruolo di intermediazione tra la struttura sanitaria e il dipendente, senza procedere alla raccolta di dati personali. Per tali ragioni il Garante ha ritenuto la raccolta e il successivo trattamento dei dati personali dei dipendenti che avevano aderito all'iniziativa di prevenzione privi di base giuridica e in violazione degli artt. 5, par. 1, lett. *a*), 6, 88 del RGPD, nonché artt. 2-*ter* e 113 del Codice (provv. 26 maggio 2022, n. 195, doc. web n. 9788986).

13.7.3. Trattamenti di dati personali effettuati in occasione dell'accertamento del requisito vaccinale per i professionisti sanitari

Un provvedimento sanzionatorio è stato adottato nei confronti di una regione, sulla base di decine di reclami e segnalazioni da parte di interessati, per lo più personale medico e infermieristico impiegato in strutture sanitarie, e sulla base di quesiti formulati da parte di medici competenti operanti presso le aziende sanitarie regionali che avevano trasmesso gli elenchi degli operatori sanitari che non risultavano vaccinati (riportando per ciascun interessato il codice fiscale, cognome, nome, data di nascita, sesso), non solo alle aziende sanitarie territorialmente competenti per l'accertamento della sussistenza del requisito, come espressamente previsto dalla norma di settore, bensì anche ai medici competenti operanti presso le stesse che agivano in qualità di autonomi titolari del trattamento rispetto alla regione. È stata così posta in essere una procedura priva di fondamento giuridico. L'accelerazione del processo di vaccinazione e la sensibilizzazione del personale sanitario avrebbero potuto essere perseguite attraverso campagne di informazione se del caso con l'ausilio dei medici competenti, senza tuttavia ricorrere alla comunicazione di dati personali,

non prevista dalla legge e pertanto in violazione degli artt. 5, par. 1, lett. *a*) e 6, del RGPD e 2-*ter* del Codice (provv. 6 ottobre 2022, n. 320, doc. web n. 9830178).

Il Garante ha poi sanzionato un'azienda sanitaria che, quale datore di lavoro, aveva comunicato a un ordine professionale, cui apparteneva un proprio medico dipendente, i provvedimenti adottati nell'ambito del rapporto di lavoro per la mancanza del requisito vaccinale nonché altre informazioni relative al rapporto di lavoro (mansione svolta dal reclamante; circostanza che lo stesso non potesse essere impiegato ad altre mansioni; possibile sospensione dell'interessato dal servizio senza retribuzione), delle quali l'ordine, in virtù del vigente quadro normativo, non era legittimato a venire a conoscenza. L'ordine, infatti, poteva conoscere, e quindi trattare, ai fini delle dovute annotazioni sull'albo professionale, solo l'informazione relativa all'insussistenza del requisito vaccinale, con conseguente sospensione *ex lege* dell'interessato dall'esercizio della professione medica e non anche l'informazione relativa alla sospensione dal servizio, ipotesi solo eventuale in ragione della possibilità per il professionista di essere adibito a mansioni alternative, sulla base delle valutazioni del datore di lavoro (provv. 24 novembre 2022, n. 384, doc. web n. 9838010).

Con separato provvedimento, il Garante ha, altresì, sanzionato l'ordine professionale, per aver inoltrato la predetta nota dell'azienda sanitaria alle autorità e agli enti di cui all'art. 2, d.P.R. 5 aprile 1950, n. 221, nonché ad altri ordini professionali territoriali, ponendo in essere una comunicazione di dati personali non prevista dalla normativa di settore in materia di accertamento dell'assolvimento dell'obbligo vaccinale (provv. 24 novembre 2022, n. 385, doc. web n. 9839018).

13.8. *Trattamento di dati nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti (cd.* whistleblowing*)*

L'Autorità è tornata ad occuparsi del tema dei trattamenti dei dati personali nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti da parte dei dipendenti e di soggetti terzi, come previsto dalla disciplina nazionale del cd. *whistleblowing* (l. 30 novembre 2017, n. 179 e art. 54-*bis*, d.lgs. 30 marzo 2001, n. 165). In tale quadro, nell'ambito di un ciclo di attività ispettive, avente a oggetto le principali funzionalità di alcuni tra gli applicativi per l'acquisizione e gestione delle segnalazioni di illeciti più diffusamente impiegati dai datori di lavoro pubblici e privati, sono stati effettuati specifici accertamenti nei confronti di una azienda sanitaria ospedaliera (provv. 7 aprile 2022, n. 134, doc. web n. 9768363) e della società fornitrice che gestiva il servizio per conto della stessa (provv. 7 aprile 2022, n. 135, doc. web n. 9768387; *Newsletter* 11 maggio 2022, doc. web n. 9768702).

Nel caso di specie l'accesso all'applicazione web di *whistleblowing*, basata su un *software open source*, avveniva attraverso sistemi che, non essendo stati correttamente configurati, registravano e conservavano i dati di navigazione degli utenti, tanto da consentire l'identificazione di chi la utilizzava, tra cui i potenziali segnalanti. La struttura sanitaria non aveva poi informato preventivamente i lavoratori in merito al trattamento, né effettuato una valutazione di impatto, né aveva inserito tali operazioni nel registro delle attività di trattamento. È infine emersa una scorretta gestione delle credenziali di autenticazione per l'accesso all'applicazione web di *whistleblowing* da parte del Rpct, durante la fase di transizione con il suo successore. Quanto ai profili di responsabilità imputabili alla società informatica che, in qualità di responsabile del trattamento, forniva all'azienda ospedaliera l'applicazione web di *whistleblowing*, è stato rilevato che la stessa si era avvalsa di un fornitore esterno per il servizio di *hosting* dei sistemi che ospitavano l'applicativo, senza dare specifiche

istruzioni sul trattamento dei dati degli interessati e senza darne notizia alla struttura sanitaria. Aveva poi utilizzato il medesimo servizio di *hosting* anche per proprie finalità, ad esempio per la gestione del rapporto di lavoro con i dipendenti o la gestione contabile e amministrativa, anche in questo caso senza regolare il rapporto e l'uso dei dati.

In un'altra istruttoria nei confronti di una società, che fornisce e gestisce per conto di diversi soggetti un applicativo per l'acquisizione e la gestione delle segnalazioni di condotte illecite, sono stati rilevati profili di violazione alla disciplina di protezione dati (provv. 21 luglio 2022, n. 268, doc. web n. 9811271). Essendo emerso che la società non era stata individuata quale responsabile del trattamento né il relativo rapporto disciplinato ai sensi dell'art. 28 del RGPD, il Garante ha altresì adottato provvedimenti sanzionatori anche nei confronti di alcuni clienti della stessa, un comune e un gestore di servizi pubblici (provv.ti 21 luglio 2022, nn. 269, doc. web n. 9813326 e 270, doc. web n. 9811732). Nel caso di specie il comune e il gestore di servizi pubblici, titolari del trattamento, non avevano disciplinato sotto il profilo della protezione dei dati il rapporto con il fornitore, in violazione dell'art. 28 del RGPD mettendo, altresì, a diposizione dello stesso dati personali relativi a segnalazioni di condotte illecite, consentendogli di raccoglierle e conservarle mediante l'applicativo *whistleblowing*, in assenza di idoneo presupposto normativo (in violazione degli artt. 5, par. 1, lett. *a*) e 6 del RGPD e dell'art. 2-*ter* del Codice). Parallelamente, le funzioni svolte dalla società avevano comportato un trattamento dei dati personali, seppur sottoposti a cifratura, dei segnalanti e degli altri interessati indicati nelle segnalazioni, di cui ciascuno dei suoi clienti risultava titolare. Non avendo ricevuto una specifica "istruzione documentata" al riguardo in qualità di responsabile del trattamento e non essendo stati indicati specifici presupposti giuridici per il trattamento dei dati personali da questa effettuata, il Garante ha sanzionato la società per non aver istituito il registro delle attività di trattamento svolte per conto dei propri clienti, titolari del trattamento, in violazione degli artt. 5, par. 1, lett. *a*), e 6 del RGPD e dell'art. 2-*ter* del Codice.

13.9. *Trattamento di dati per finalità di gestione del rapporto di lavoro*

Anche con riguardo alla gestione del rapporto di lavoro il Garante, sulla base di istruttorie avviate a seguito di reclami presentati da dipendenti pubblici o di altri soggetti che prestano la propria attività lavorativa presso soggetti pubblici e enti che perseguono finalità di interesse pubblico, ha accertato l'illiceità di taluni trattamenti.

13.9.1. Trattamento di dati nell'ambito di procedure concorsuali

A seguito della notifica di una violazione di dati personali da parte di una regione, effettuata ai sensi dell'art. 33 del RGPD concernente la pubblicazione di numerosi dati personali riferiti ai partecipanti alle prove preselettive di una procedura concorsuale, il Garante ha accertato che, nella predisposizione dell'applicazione web per la consultazione da parte di ciascun candidato dei propri dati, la società fornitrice, quale responsabile del trattamento per conto della regione, non aveva adottato alcuna misura idonea a garantire che i dati personali di ciascun interessato fossero resi disponibili esclusivamente allo stesso interessato o a soggetti autorizzati. In particolare, chiunque si fosse collegato all'indirizzo web erroneamente messo a disposizione di una candidata avrebbe potuto accedere liberamente ai dati personali dei numerosi interessati partecipanti alla procedura in questione (quali generalità, esiti dettagliati di ciascuna prova e punteggio complessivo). La mancata adozione

di idonee misure aveva quindi determinato una diffusione illecita di dati personali la cui responsabilità era da attribuire alla regione. Il responsabile del trattamento è stato invece ritenuto responsabile della mancata adozione di misure tecniche e organizzative volte ad assicurare la sicurezza del trattamento, che ha creato le premesse dell'incidente di sicurezza e del ricorso ai servizi offerti da una società per i servizi di *hosting*, quale sub responsabile senza previa autorizzazione dalla regione (provv.ti 10 febbraio 2022, nn. 43 e 44, docc. web nn. 9751498 e 9754332).

13.9.2. Pubblicazione e condivisione di dati personali nel registro elettronico delle scuole

Come chiarito tradizionalmente dal Garante, i dati personali dei dipendenti nel contesto lavorativo non possono essere messi a conoscenza di soggetti diversi da coloro che sono parte del rapporto di lavoro e che non siano legittimati, in ragione delle scelte organizzative del titolare del trattamento e delle specifiche mansioni svolte, a trattare i medesimi dati, in qualità di personale autorizzato. Nel periodo di riferimento il Garante ha adottato due provvedimenti sanzionatori nei confronti di due scuole che avevano consentito l'accesso al registro elettronico e ad altri applicativi a personale non autorizzato nonché, in un caso, la diffusione *online* dei dati personali ivi contenuti.

In particolare in un caso era stato reso disponibile nella sezione del registro elettronico riservata ai soli insegnanti, un documento recante l'orario definitivo del personale docente contenente il riferimento alla fruizione dei benefici derivanti dalla l. 5 febbraio 1992, n. 104 da parte della reclamante e di altri docenti, nonché altre informazioni di dettaglio relative a vicende personali e familiari o legate allo specifico rapporto di lavoro di ciascuno (ed es. trasferimento, *part-time*, interdizione maternità, l. n. 104 non grave). Il Garante ha ricordato che il riferimento alla cd. legge 104 consente di ricavare informazioni sullo stato di salute di una persona e che, diversamente, lo stato di gravidanza possa essere considerato dato sulla salute se associata all'informazione relativa all'interdizione dal lavoro delle lavoratrici in stato di gravidanza (cfr. art. 17 comma 2, lett. *a*), d.lgs. n. 151/2001), sicché i dati in parola sono stati resi conoscibili anche per i colleghi della reclamante e non, invece, esclusivamente a vantaggio del solo personale di segreteria autorizzato al trattamento di tali informazioni (provv. 28 aprile 2022, n. 150, doc. web n. 9777200).

In un analogo caso il Garante è intervento in relazione alla pubblicazione, sul sito istituzionale di un istituto scolastico e sul portale utilizzato dall'istituto anche con funzionalità di registro elettronico, di una circolare riguardante le ferie estive dei collaboratori scolastici recante, in allegato, un prospetto che riportava, in corrispondenza del nominativo del reclamante e di altro personale, l'espressa indicazione delle specifiche causali di assenza ivi compreso il riferimento alla fruizione dei benefici derivanti dalla l. 5 febbraio 1992, n. 104. L'istituto – per errore di un collaboratore amministrativo – ha consentito la consultazione ai dati personali dei dipendenti nell'area ad accesso riservato del registro elettronico da parte di colleghi non autorizzati dando luogo a una comunicazione di dati personali e la pubblicazione *online* dei medesimi dati ha altresì comportato la violazione del generale divieto alla diffusione dei dati relativi alla salute di cui all'art 2-*septies*, comma 8, del Codice (provv. 1° settembre 2022, n. 290, doc. web n. 9811361).

13.9.3. Circolazione di informazioni personali nei contesti lavorativi, anche nei sistemi di protocollazione informatica degli atti

Un dipendente di un'azienda sanitaria ha rappresentato di aver chiesto all'amministrazione, datrice di lavoro, nell'ambito di un procedimento riguardante la propria posizione previdenziale, di indirizzare future comunicazioni ad un

proprio indirizzo Pec personale. L'azienda aveva invece inviato una comunicazione anche all'indirizzo di posta elettronica certificata dell'unità organizzativa presso la quale l'interessato prestava servizio in qualità di dirigente, e dunque ad un *account* condiviso cui aveva accesso il personale preposto a tale ufficio. Inoltre, la nota contenente dati del reclamante anche relativi alla sua posizione previdenziale era stata resa visibile, anche mediante protocollo informatico, non solo agli addetti alla protocollazione degli atti ma anche ad altri dipendenti dell'azienda e assegnati alla U.O.S. formazione, diretta dal reclamante. Tali condotte hanno determinato comunicazione di dati personali in favore di personale non autorizzato (provv. 24 marzo 2022, n. 98, doc. web n. 9763051).

Analogamente il Garante ha adottato un provvedimento sanzionatorio nei confronti di un ministero, avendo accertato la messa a disposizione di dati personali di un dipendente, anche relativi alla salute, nonché a condanne penali e reati, a destinatari che non potevano considerarsi autorizzati al trattamento degli stessi (provv. 28 aprile 2022, n. 146, doc. web n. 9776406).

In un altro caso, un comune aveva inviato una nota a un istituto bancario, informando lo stesso non solo dell'avvenuta cessazione del rapporto di lavoro con il reclamante, ma anche di una serie di ulteriori informazioni di carattere personale a questo riferite (quali la proroga del periodo di aspettativa specifica, la ragione della cessazione del rapporto, gli estremi del nuovo datore di lavoro), non giustificate alla luce del quadro normativo che disciplina l'istituto del pignoramento presso terzi e gli obblighi del datore di lavoro, in qualità di terzo pignorato. La medesima nota era stata inviata anche al nuovo datore di lavoro del reclamante, rendendo così noto un debito dell'interessato nei confronti dell'istituto bancario in questione, incluse informazioni di dettaglio relative al pignoramento di quota dello stipendio e al residuo della somma da pagare, nonché informazioni relative alla gestione del precedente rapporto di lavoro con il rischio di esporre il dipendente/reclamante a possibili effetti pregiudizievoli, anche indiretti, nel nuovo contesto lavorativo. Il Garante ha rilevato che in entrambe le circostanze ha avuto luogo una comunicazione di dati personali in assenza di base giuridica (provv. 12 maggio 2022, n. 174, doc. web n. 9781242).

Il Garante ha poi ammonito un comune che aveva inoltrato segnalazioni presentate da alcuni lavoratori, dipendenti di enti accreditati e fornitori di servizi al comune, ai rispettivi datori di lavoro, senza un'effettiva necessità di inoltrare la versione integrale di tali comunicazioni, in cui figuravano anche l'indirizzo di posta elettronica personale del lavoratore mittente e la data/ora di invio del messaggio (provv. 24 novembre 2022, n. 412, doc. web n. 9838947).

Un altro comune è stato ammonito per aver inviato un messaggio di posta elettronica certificata ai partecipanti a una prova concorsuale, con gli indirizzi di posta elettronica degli stessi in chiaro, così rivelando alle due reclamanti gli indirizzi degli altri candidati e a questi ultimi quelli delle due reclamanti, rendendo, inoltre, nota la circostanza che i destinatari – tutti candidati nell'ambito della procedura concorsuale – avessero chiesto un cambio del proprio turno per effettuare una prova preselettiva (provv. 15 dicembre 2022, n. 419, doc. web n. 9843741).

13.10. *Diffusione* online *di dati personali dei lavoratori*

Continuano a essere numerosi i reclami nei confronti di amministrazioni, in merito alla pubblicazione sui siti web istituzionali, in alcuni casi nella sezione "Amministrazione trasparente" o in quella "Albo pretorio", di atti e documenti contenenti dati personali di lavoratori (cfr. par. 4.4).

13

Con riguardo a tali fattispecie, il Garante, nel dichiarare l'illiceità del trattamento, in ragione dell'assenza di un'idonea base giuridica idonea a giustificare la diffusione dei dati personali di lavoratori, ha definito numerosi reclami, di seguito riportati, concernenti la pubblicazione sul sito web istituzionale di:

- un'azienda sanitaria, di un comunicato stampa, contenente dati personali del reclamante e di un altro lavoratore in servizio presso la stessa, relativi a vicende connesse al rapporto di lavoro e a provvedimenti disciplinari adottati a carico degli interessati. Nel motivare la propria decisione, il Garante ha evidenziato che i soggetti pubblici possono diffondere dati personali solo al ricorrere delle condizioni previste dalla normativa in materia di protezione dei dati, a nulla rilevando che i dati siano già stati diffusi altrove, anche dallo stesso interessato, per altre finalità (provv. 13 gennaio 2022, n. 7, doc. web n. 9745807);

- un comune, di una determinazione relativa alla revoca del nullaosta riguardante l'interscambio tra dipendenti di due comuni recante anche l'espressa indicazione del nominativo del reclamante, non direttamente coinvolto nella procedura, la sua qualifica professionale e numerosi riferimenti alle denunce e querele presentate dal reclamante nei confronti di uno dei colleghi destinatario del provvedimento revocato. Il Garante ha ribadito quanto affermato sin dal 2014 nelle linee guida in materia di trattamento di dati personali (provv. 15 maggio 2014, n. 243, doc. web n. 3134436), contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati e cioè che le disposizioni che regolano gli obblighi di pubblicità dell'azione amministrativa per finalità di trasparenza vanno tenute distinte da quelle che regolano le forme di pubblicità per finalità diverse in ragione del diverso regime giuridico applicabile (provv. 10 febbraio 2022, n. 45, doc. web n. 9751549);

- un'agenzia regionale per la tutela dell'ambiente, di una deliberazione avente ad oggetto l'approvazione di uno schema di verbale di conciliazione in sede sindacale, contenente informazioni relative a una vicenda giudiziaria afferente al rapporto di lavoro al tempo in essere tra il reclamante e l'agenzia. In particolare, è stato evidenziato che le informazioni relative ad un procedimento giudiziario a carico di una persona fisica come quelle relative all'apertura di un'indagine o al processo, ed eventualmente alla condanna che ne è risultata, costituiscono dati relativi a condanne penali e reati ai sensi dell'art. 10 del RGPD, anche quando non sia stata effettivamente dimostrata la commissione del reato. Il Garante ha, altresì, ribadito che i soggetti pubblici possono diffondere dati personali solo al ricorrere delle condizioni previste dalla normativa in materia di protezione dei dati, a nulla rilevando che i dati siano già stati diffusi dallo stesso interessato o da terzi per altre finalità (provv. 10 marzo 2022, n. 22, doc. web n. 9761383);

- un comune, di una deliberazione di giunta, con la quale si proponeva la costituzione in giudizio dell'ente in un contenzioso con il reclamante, dipendente del comune, identificabile attraverso l'iniziale del nome e il cognome per esteso, diffondendo, in tal modo, informazioni relative a vicende connesse al rapporto di lavoro al tempo in essere con il reclamante, anche con riguardo a un procedimento disciplinare, a un contenzioso promosso dallo stesso in sede civile e ad altre situazioni afferenti alla sfera privata del reclamante ovvero la circostanza che lo stesso non avesse accettato una posizione lavorativa presso un altro comune (provv. 28 aprile 2022, n. 149, doc. web n. 9777127);

- un ente per la promozione del patrimonio ambientale, di una deliberazione avente ad oggetto l'affidamento di un incarico a uno studio legale in relazione a un contenzioso con il reclamante, ex dipendente dell'ente (provv. 26 maggio 2022, n. 196, doc. web n. 9789541);

- un comune, del *curriculum vitae* di un ex dipendente, con qualifica di dirigente, in cui erano riportati dati quali l'indirizzo di residenza, il numero di cellulare e gli indirizzi di posta elettronica personali, nonostante il rapporto di lavoro fosse già cessato e l'interessato avesse fatto invano istanza di opposizione alla diffusione dei propri dati personali (provv. 26 maggio 2022, n. 198, doc. web n. 9789899);

- un comune, nella sezione Albo pretorio, di una determinazione contenente l'informazione del licenziamento del reclamante, identificato con il proprio numero di matricola. Il Garante ha evidenziato, come già ribadito in numerose decisioni in merito agli obblighi derivanti dall'art. 124, d.lgs. n. 267/2000, che anche alle pubblicazioni nell'Albo pretorio *online* si applicano i principi relativi alla liceità del trattamento e alla minimizzazione dei dati (provv. 15 settembre 2022, n. 299, doc. web n. 9815665);

- un istituto scolastico, della nota con cui veniva comunicata la risoluzione del contratto a tempo indeterminato del reclamante – immesso in ruolo come docente presso l'istituto – con allegati i relativi provvedimenti adottati dall'ufficio scolastico del Ministero dell'istruzione, competente per territorio (provv. 20 ottobre 2022, n. 335, doc. web n. 9828059);

- un comune, nell'Albo pretorio *online* e successivamente anche nell'Albo pretorio storico, di un provvedimento dirigenziale, contenente dati personali del reclamante, il quale, a seguito di trasferimento, aveva comunicato all'ufficio del personale di procedere alle trattenute in busta paga per un prestito contratto in precedenza. Il comune aveva illecitamente pubblicato il provvedimento dirigenziale contenente il nome e cognome del reclamante, l'indicazione della cifra decurtata dallo stipendio, la durata della cessione del quinto, i dati della banca concessionaria corredati dal codice iban (provv. 10 novembre 2022, n. 366, doc. web n. 9834986);

- un'azienda ospedaliera, di due provvedimenti, indicizzati sui motori di ricerca, in cui veniva riportato lo *status* di invalidità del reclamante. Un provvedimento riguardava la rettifica del precedente provvedimento con il quale era stato disposto il collocamento a riposo dell'interessato, mentre l'altro conteneva l'espresso riferimento al verbale di riconoscimento dell'invalidità civile dell'interessato, oltre a informazioni di dettaglio relative a vicende connesse al rapporto di lavoro, quali la richiesta di collocamento a riposo (provv. 1° dicembre 2022, n. 404, doc. web n. 9842783);

- un comune, di un provvedimento dirigenziale, visibile anche in rete, in cui, a seguito di risoluzione del contratto di lavoro del reclamante "per inabilità assoluta e permanente alle mansioni del proprio profilo professionale", veniva riportato, con indicazione in chiaro dei relativi dati anagrafici, anche il giudizio diagnostico (provv. 1° dicembre 2022, n. 405, doc. web n. 9844727);

- un comune, di una determinazione, contenente informazioni riguardanti il rapporto di lavoro del reclamante, identificato con le iniziali del proprio nome e cognome e con il numero di matricola, e ulteriori dati relativi al suo stato di salute (provv. 15 dicembre 2022, n. 420, doc. web n. 9853429);

- un'azienda sanitaria, nella sezione Albo pretorio, di una delibera, con cui, a seguito di impugnazione da parte del reclamante di un provvedimento disciplinare, è stato conferito un incarico a libero professionista per l'assistenza tecnica nel relativo giudizio (provv. 15 dicembre 2022, n. 425, doc. web n. 9857587).

13.10.1. Pubblicazione di graduatorie e atti di procedure concorsuali

Alcuni reclami hanno riguardato la diffusione *online* di dati personali in relazione alla pubblicazione di graduatorie e atti di procedure concorsuali, su cui tradizionalmente il Garante ha fornito specifiche indicazioni alle p.a. in ordine alle cautele da adottare (v. le linee guida in materia di trattamento di dati personali,

contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, cit., spec. II, par. 3.b, nonché le linee guida in materia di trattamento di dati personali, di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, adottate con provv. 14 giugno 2007, n. 161, doc. web n. 1417809).

In un caso, il Garante ha ammonito un ministero per la pubblicazione di una graduatoria di un concorso interno, che, a causa di un errore umano, conteneva una nota, associata al nominativo del reclamante, con la menzione "riserva procedimento penale", diffondendo conseguentemente un dato personale relativo a condanne penali e reati. Il Garante ha evidenziato che le informazioni relative ad un procedimento giudiziario a carico di una persona fisica, come quelle relative all'apertura di un'indagine o al processo, ed eventualmente alla condanna che ne sia risultata costituiscono dati relativi a condanne penali e reati ai sensi dell'art. 10 del RGPD. Il ministero aveva successivamente pubblicato un'altra graduatoria, nella quale compariva l'annotazione "ammesso con riserva", ovvero un'informazione comunque eccedente rispetto alle finalità di trattamento, dalla quale si poteva desumere la potenziale assenza di uno dei requisiti previsti per la partecipazione al concorso oppure una causa di esclusione (provv. 24 marzo 2022, n. 97, doc. web n. 9760883).

Il Garante ha adottato, in un altro caso, un provvedimento sanzionatorio nei confronti di un comune per aver pubblicato le graduatorie degli ammessi con riserva alla prova preselettiva e l'elenco degli ammessi e non ammessi alla successiva prova scritta di una procedura concorsuale. Il Garante ha ribadito che le norme di settore stabiliscono, in generale, la pubblicazione delle sole graduatorie definitive dei vincitori e non anche l'elenco degli ammessi e non ammessi alla selezione o a prove intermedie. È stato, inoltre, evidenziato che il d.lgs. 14 marzo 2013, n. 33, richiamato dal comune, non costituisce un'idonea base giuridica per la diffusione *online* dei dati personali contenuti negli elenchi dei candidati ammessi o non ammessi alle prove selettive in quanto l'art. 19 dello stesso stabilisce che siano pubblicate, per finalità di trasparenza, le sole "graduatorie finali aggiornate con l'eventuale scorrimento degli idonei non vincitori" (provv. 28 aprile 2022, n. 151, doc. web n. 9778996).

13.10.2. Dati personali di lavoratori in banche dati pubbliche

A fronte di tre incidenti informatici, debitamente notificati all'Autorità, che avevano comportato l'accesso non autorizzato ai dati personali – anche relativi alla salute e agli infortuni subiti – di alcuni lavoratori, trattati tramite il servizio *online* denominato Sportello virtuale lavoratori gestito dall'Inail, il Garante ha adottato un provvedimento sanzionatorio nei confronti dell'Istituto. L'istruttoria ha messo in evidenza che all'epoca dei fatti l'Istituto non aveva adottato misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, determinando in tal modo le premesse di accessi non autorizzati a dati personali di terzi anche relativi alla salute. Ai fini della commisurazione della sanzione amministrativa è stata comunque considerata la piena collaborazione offerta dall'Istituto con l'ausilio del proprio Rpd, unitamente al numero esiguo di persone coinvolte nei *data breach* individuati (provv. 28 aprile 2022, n. 147, doc. web n. 9771184; v. anche *Newsletter* 5 maggio 2022, doc. web n. 9774926).

L'Agenzia nazionale per le politiche attive del lavoro (Anpal) ha chiesto al Garante un parere, ai sensi dell'art. 36, par. 4, del RGPD, sullo schema di delibera del Commissario straordinario in materia di trattamento dei dati personali del Programma nazionale per la garanzia occupabilità dei lavoratori (Gol) nell'ambito del Pnrr. Il trattamento dei dati personali dei beneficiari del Programma Gol è

effettuato nell'ambito del sistema informativo unitario delle politiche del lavoro al fine di assicurare il rispetto dei livelli essenziali delle prestazioni e consentire l'attivazione e la gestione dei patti di servizio. I dati personali relativi ai beneficiari sono raccolti esclusivamente presso gli interessati da parte del servizio per il lavoro territorialmente competente utilizzando – ai fini della valutazione del livello di occupabilità e della individuazione della classe di profilazione quantitativa – anche i dati dell'archivio delle comunicazioni obbligatorie dovute dai datori di lavoro. L'Autorità, anche all'esito delle interlocuzioni intercorse con i rappresentanti dell'Agenzia, nell'esprimere il proprio parere favorevole, ha evidenziato come lo schema di delibera recepisce le indicazioni fornite dal Garante volte ad assicurare, in particolare, il rispetto del principio di correttezza e trasparenza nei confronti dei beneficiari e contenga garanzie nell'ambito dei trattamenti automatizzati effettuati a fini di profilazione dei beneficiari, assicurando, in particolare, verifiche periodiche sulla qualità dei dati e l'intervento umano nel processo decisionale finalizzato all'individuazione dei percorsi di politica attiva del lavoro sulla base del livello di occupabilità, nonché il rispetto dei principi di minimizzazione dei dati mediante l'adozione di tecniche di pseudonimizzazione e anonimizzazione nell'ambito dei trattamenti effettuati per lo svolgimento delle funzioni di analisi, monitoraggio e controllo da parte delle istituzioni competenti (provv. 20 ottobre 2022, n. 353, doc. web n. 9827428).

Il Garante ha formulato parere favorevole anche in merito a uno schema di deliberazione della Giunta regionale della Regione Emilia-Romagna, che ha adottato lo "schema di RGPD di attuazione dell'art. 2-*bis* della l.r. 14/2015" in materia di sostegno all'inserimento lavorativo e all'inclusione sociale delle persone in condizione di fragilità e vulnerabilità, che tiene conto delle indicazioni fornite dall'Ufficio nelle interlocuzioni intercorse, considerato che i trattamenti in questione – effettuati anche mediante una specifica applicazione dell'Agenzia per il lavoro dell'Emilia-Romagna, nell'ambito dei servizi del Sistema informativo lavoro (Sil), che è fruibile attraverso il sistema "Portale lavoro per te" – possono comportare rischi elevati per gli interessati (principalmente soggetti vulnerabili), anche in ragione della natura dei dati personali oggetto di trattamento (tra i quali quelli relativi alla salute e alla condizione economica e sociale degli interessati), elaborati, mediante l'attribuzione di un punteggio, ai fini della valutazione della condizione di fragilità, in vista della definizione di programmi personalizzati d'interventi (provv. 21 luglio 2022, n. 253, doc. web n. 9806228).

14 Le attività economiche

14.1. *Trattamento di dati personali in ambito assicurativo*

Ancora nel 2022 sono pervenute all'Autorità numerose istanze, in particolar modo segnalazioni e reclami, riguardanti il settore assicurativo, per lo più definite con note dipartimentali in quanto concernenti tematiche già esaminate in passato dal Garante e sulle quali si è già dato ampio conto nelle Relazioni degli ultimi anni (v. Relazione 2020, p. 179 e Relazione 2021, p. 175).

In una occasione, tuttavia, l'Autorità ha sanzionato una compagnia assicurativa per la violazione dei principi generali di liceità, correttezza, trasparenza e di integrità e riservatezza, di cui all'art. 5, par. 1, lett. *a*) e *f*), del RGPD (provv. 7 luglio 2022, n. 244, doc. web n. 9809201). In particolare, in occasione della liquidazione di una polizza diversa da quella riferita al reclamante, la compagnia assicurativa aveva comunicato a due soggetti terzi (beneficiari della polizza oggetto di liquidazione) informazioni riferite all'interessato, intestatario di un'altra polizza con la compagnia medesima; all'esito del procedimento istruttorio è emerso un errore materiale posto in essere dall'addetto alla liquidazione della pratica e di cui la compagnia ha avuto contezza a distanza di mesi dall'accaduto e solo a seguito della segnalazione effettuata dall'interessato (la cui polizza era stata liquidata in assenza di presupposti). Ai fini della quantificazione della sanzione amministrativa pecuniaria – nel rispetto di quanto disposto dall'art. 83, par. 2, del RGPD – si è tenuto conto, in particolare, del fatto che l'evento si era verificato a causa dell'errore di un dipendente che si era discostato dalle istruzioni impartite dal titolare in ordine ai controlli di completezza e di coerenza nonché del fatto che la compagnia, già precedentemente all'evento, si era dotata di una regolamentazione interna concernente specifici controlli sui processi di liquidazione.

Deve inoltre segnalarsi che l'Autorità, su richiesta formulata da una società assicurativa, ha reso un parere in ordine al ruolo degli istituti di credito che trattano dati personali dei clienti ai fini del collocamento di polizze assicurative (parere 18 maggio 2022, doc. web n. 9781161).

L'Autorità, a seguito di una articolata istruttoria che ha coinvolto anche l'Istituto per la vigilanza sulle assicurazioni (Ivass) e l'Associazione nazionale per le imprese assicuratrici (Ania), esaminata la normativa di settore (in particolare, art. 58, regolamento Ivass 2 agosto 2018, n. 40, come integrato e modificato dal provvedimento Ivass 4 agosto 2020, n. 97) e tenuto anche conto dell'orientamento dall'EDPB sulle figure di titolare e responsabile quali concetti "funzionali" (cfr. linee guida sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del RGPD, adottate il 7 luglio 2021 - parte I, par. 12), ha ritenuto che, nella distribuzione di polizze assicurative, il rapporto che intercorre tra la compagnia assicurativa e la banca intermediaria è quello tipico titolare/responsabile del trattamento.

In particolare, prima di far sottoscrivere al cliente una proposta o un contratto assicurativo la banca ha l'obbligo di acquisire dallo stesso le informazioni utili a valutare le sue richieste ed esigenze sulla base delle indicazioni e dei criteri forniti dalla compagnia assicurativa, senza alcun margine di discrezionalità; si tratta pertanto

di un'attività strumentale alla finalità perseguita dalla compagnia assicurativa (la conclusione del contratto di assicurazione con il cliente) effettuata dalla banca in qualità di responsabile del trattamento.

Nel parere, l'Autorità ha peraltro evidenziato la necessità che il ruolo di responsabile del trattamento rivestito dall'istituto bancario nel collocamento di polizze assicurative sia adeguatamente indicato all'interno delle informative rese agli interessati ai sensi dell'art. 13 del RGPD.

In un altro caso, in cui l'interessato lamentava tra l'altro che i suoi dati personali relativi alla sinistrosità pregressa fossero riportati in modo errato, l'Autorità, a seguito di varie interlocuzioni con la compagnia e con il casellario centrale infortuni (da cui è emerso un errore tecnico di decifratura dei dati del casellario) e dopo aver appurato la pronta rettifica dei dati errati, ha informato Ivass, per le valutazioni di competenza, del rilevato processo di creazione di documenti a partire dalla banca dati del casellario e potenzialmente rappresentanti un'errata situazione infortunistica degli interessati (nota 14 dicembre 2022).

14.2. *Trattamento di dati personali in ambito bancario-finanziario e sistemi di informazioni creditizie*

Il cd. tracciamento delle operazioni bancarie

In diversi casi, i clienti di istituti di credito hanno lamentato accessi indebiti ai loro dati personali (in particolare, informazioni bancarie) da parte di dipendenti degli istituti medesimi per finalità proprie o per la comunicazione a terzi non autorizzati.

Come evidenziato negli anni scorsi (v. Relazioni 2020 e 2021), si tratta di un fenomeno, rispetto al quale l'Autorità è intervenuta già nel 2011 con il provvedimento 12 maggio 2011, n. 192 recante prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (doc. web n.1813953), che ha previsto la necessaria adozione, da parte degli istituti di credito, di sistemi di *alert* idonei a rilevare comportamenti anomali o a rischio relativi alle operazioni di *inquiry* eseguite dal personale sui dati personali della clientela.

Si segnala, in particolare, il provvedimento 28 luglio 2022, n. 272 (doc. web n. 9812423) con il quale l'Autorità ha appurato che un dipendente aveva effettuato accessi alle posizioni contabili della reclamante, non giustificati da esigenze operative, con successivo utilizzo delle stesse nell'ambito di un procedimento giudiziario.

Il Garante, pur avendo accertato che all'epoca dei fatti esaminati, l'istituto di credito non aveva adeguatamente implementato *alert* idonei a rilevare comportamenti anomali o a rischio relativi alle operazioni di *inquiry* eseguite dal personale, ha disposto l'applicazione di una sanzione amministrativa pecuniaria, ma non ha ravvisato i presupposti per ulteriori misure correttive di cui all'art. 58, par. 2, del RGPD, in quanto il titolare aveva nel frattempo ottemperato alle prescrizioni impartitegli con provvedimento correttivo e sanzionatorio n. 270/2021 (v. Relazione 2021, p. 178) per una successiva analoga violazione.

Il Garante ha poi esaminato un reclamo con il quale gli interessati lamentavano accessi indebiti ai propri conti correnti incardinati presso la filiale di una banca; quest'ultima, effettuate le necessarie verifiche, ha comunicato che gli accessi erano stati indebitamente effettuati da un dipendente.

All'esito dell'istruttoria, l'Ufficio, pur ravvisando una sostanziale conformità delle misure adottate dalla banca per il tracciamento degli accessi effettuati dai dipendenti sui dati dei clienti alle disposizioni di cui al provvedimento n. 192/2011 già citato, ha richiamato la banca ad una complessiva valutazione dei sistemi di *alert* per verificare l'eventuale necessità di rafforzare il livello di tutela dei dati personali.

14

Le disposizioni contenute nel citato provvedimento infatti contengono, ad oggi – in ragione del tempo trascorso dalla sua adozione e dello sviluppo dei sistemi tecnologici – i requisiti minimi che le banche sono tenute ad adottare e spetta, comunque, al titolare la concreta individuazione di misure ritenute più idonee, alla luce del generale principio di responsabilizzazione (cd. *accountability*) (artt. 5, par. 2 e 24 e cons. 74 del RGPD) (nota 20 ottobre 2022).

Trattamento dati da parte di un istituto di credito nell'ambito di un addebito RID

In un caso sottoposto all'attenzione dell'Autorità, il reclamante aveva lamentato il trattamento dei propri dati personali da parte di una banca, che, a seguito di una procedura di trasferimento di conto corrente da altra banca – nell'ambito del quale era previsto anche il trasferimento dei mandati di pagamento accesi sul vecchio conto – ha attivato un addebito RID intestando al reclamante, quale debitore, il relativo mandato di pagamento.

Ciò, benché il mandato precedente non fosse intestato al reclamante, bensì alla moglie, cointestataria dello stesso conto corrente.

Nel caso in esame, quindi, poiché i pagamenti attraverso addebito RID, benché relativi a un contratto di finanziamento intestato solo alla moglie del reclamante, erano stati agganciati al codice iban di un conto corrente cointestato, trovava applicazione l'art.1298 c.c.

Tale articolo attribuisce agli intestatari del conto corrente, la qualità di creditori o debitori in solido dei saldi del conto sia nei confronti dei terzi, sia nei rapporti interni (in tal senso, v. anche Cass. civ., sez. 2, ord. 23 febbraio 2021, n. 4838).

L'Autorità ha, tuttavia, rilevato che l'apposizione, sul mandato di pagamento, del termine debitore accanto al nominativo del reclamante – cointestatario del conto corrente su cui poggia il mandato di pagamento, ma comunque non titolare del rapporto di finanziamento sotteso al mandato di pagamento – è idoneo a fornire una rappresentazione non esatta della soggettività giuridica dello stesso reclamante (art. 5, par. 1, lett. *d*), del RGPD).

Per tale motivo la banca è stata richiamata a valutare l'opportunità di adottare misure idonee a garantire l'esattezza dei dati degli interessati, ad esempio, predisponendo dispositivi che consentano l'individuazione dei conti di pagamento solo attraverso l'iban, in grado di identificare, senza ambiguità un unico conto di pagamento (in tal senso, v. regolamento (UE) n. 260/2012 del Parlamento europeo e del Consiglio 14 marzo 2012, che stabilisce i requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro), o indicando sul mandato di pagamento i nominativi di entrambi i titolari del conto corrente eliminando la dicitura debitore (nota 23 maggio 2022).

Accesso ai propri dati e loro cancellazione

Numerose richieste pervenute hanno riguardato l'esercizio dei diritti degli interessati nei confronti di istituti di credito.

Con specifico riguardo al diritto di accesso (regolato dall'art. 15 del RGPD), a conferma del consolidato orientamento dell'Autorità, è stato riaffermato in molteplici circostanze che esso è diverso da quello di ricevere documentazione bancaria (disciplinato dagli articoli 117 e ss., d.lgs. 1° settembre 1993, n. 385 -Testo unico delle leggi in materia bancaria e creditizia, di seguito Tub) e permette agli interessati di conoscere i dati e le informazioni a sé riferite e di ottenere anche l'accesso agli atti e documenti che li contengono, tanto più se, come avviene in ambito bancario, l'accesso documentale è già previsto e disciplinato da altre specifiche normative di settore applicabili (in specie, dall'art. 119 del Tub).

Con provvedimento 6 ottobre 2022, n. 378 (doc. web n. 9831387), il Garante ha ritenuto fondate le doglianze della reclamante che aveva ricevuto riscontro a un'istanza di accesso ai dati personali di propri congiunti deceduti – avanzata ai sensi degli artt. 15 del RGPD e 2-*terdecies* del Codice – oltre il termine di trenta giorni previsto dalla normativa (art. 12, par. 3, del RGPD).

In un altro caso, a conclusione di una complessa e articolata istruttoria, il Garante ha ritenuto illecito il trattamento dei dati personali dell'interessato, sia in ragione del mancato tempestivo riscontro all'istanza di accesso avanzata dallo stesso, sia per l'inidoneità del riscontro medesimo, poiché le informazioni fornite al reclamante erano non esaustive e, soprattutto a causa dell'utilizzo di una terminologia tecnica di difficile comprensione, non consentivano all'interessato, tenuto conto della particolarità e della complessità della vicenda, di individuare, rispetto alle informazioni richieste, il titolare del trattamento (ovvero l'effettivo soggetto cui compete la custodia delle informazioni medesime e, di conseguenza, il riscontro all'esercizio dei diritti) (provv. 20 ottobre 2022, n. 347, doc. web n. 9825689).

In altra circostanza, a seguito di richiesta da parte dell'interessato, di conoscere l'origine dei dati personali a lui riferiti, l'Autorità ha confermato la liceità del comportamento dell'istituto bancario che aveva richiesto all'interessato copia del documento di identità per poter dar seguito alla relativa richiesta, in quanto gli elementi addotti dall'interessato non consentivano un'identificazione certa dello stesso, a causa di omonimie e di un'anomalia riscontrata nell'indirizzo *e-mail* del richiedente (cfr. art. 12, par. 6, del RGPD).

Inoltre, l'Autorità ha confermato la correttezza del trattamento dei dati personali dell'interessato (e.g. nominativo, varie numerazioni telefoniche, etc.) acquisiti dalla banca nell'ambito di un'attività di cessione di rami d'azienda da altro istituto di credito e sulla base del legittimo interesse della cessionaria (v. le linee guida adottate dal Garante il 25 ottobre 2007, doc. web n. 1457247) (nota 9 dicembre 2022).

Alcuni interessati hanno presentato reclami al Garante a seguito di riscontri, a istanze riguardanti, contemporaneamente, la revoca del consenso al trattamento dei propri dati personali e l'esercizio del diritto di cancellazione di questi ultimi dagli archivi gestiti da istituti di credito, con i quali risultavano appena cessati o ancora pendenti specifici rapporti.

Nel ritenere infondati i reclami in questione, l'Autorità ha osservato che, in ambito bancario, assume particolare rilevanza il termine decennale di conservazione dei documenti (art. 119, d.lgs. n. 385/1993 - Tub) e delle scritture contabili (art. 2220 del c.c.), al quale fanno riferimento anche altre disposizioni (art. 2946 c.c. sulla prescrizione ordinaria dei diritti).

In presenza di tali termini – e, più in generale, qualora sussista un obbligo giuridico di conservazione dei dati o documenti – il titolare del trattamento non può dare seguito alle richieste di cancellazione avanzate da un interessato, anche qualora il rapporto contrattuale con quest'ultimo sia concluso.

Quanto alla revoca del consenso, si è evidenziato che, nelle fattispecie prospettate, le basi giuridiche del trattamento dei dati degli interessati sono solo quelle individuate dall'art. 6, par. 1, lett. *b*) e *c*), del RGPD e che non vi era, pertanto, un consenso utilmente revocabile (note 25 novembre e 7 dicembre 2022).

Il fenomeno dei furti d'identità

Nel corso dell'anno si sono intensificate anche le richieste rivolte al Garante in casi riconducibili al fenomeno del cd. furto d'identità, disciplinato dal Titolo V-*bis*, d.lgs. 13 agosto 2010, n. 141 e successive modifiche ed integrazioni, che ha istituito un archivio antifrode presso il Mef (v. parere reso dell'Autorità in data 21 marzo 2013, n. 213, doc. web n. 2462626) e consistente nel carpire o sottrarre fraudolentemente agli interessati dati personali per poi disporre di somme di denaro presenti sui loro conti correnti.

Il Garante ha ricordato che una scheda informativa disponibile sul sito sensibilizza l'utenza ad adottare accorgimenti e cautele volti a prevenire comportamenti fraudolenti e reati (doc. web n. 5779928) e che il 13 aprile 2022 l'Associazione bancaria italiana (Abi) e la Polizia di Stato hanno predisposto e reso disponibile

14

un *vademecum*, facilmente consultabile sul sito dell'Abi e sul portale della Polizia postale, che va ad affiancarsi agli strumenti e alle iniziative già adottate in materia di sicurezza dalla stessa Abi, Istituzioni e singole banche.

Considerato, peraltro, che tutti gli interessati avevano sporto denuncia all'autorità competente per l'accertamento delle fattispecie di reato (artt. 494, 640 e 640-*ter* c.p.), si è fatta riserva di eventuali determinazioni sulla base delle risultanze degli accertamenti in sede giudiziaria (cfr. art. 167, comma 4, del Codice).

In un caso in particolare, notizie di stampa avevano prospettato che l'accesso da parte di ignoti ai conti correnti di clienti di un istituto di credito costituisse un *data breach* ascrivibile a mancanza di sicurezza dei sistemi informativi predisposti dalla banca.

Dall'istruttoria è emersa la riconducibilità della fattispecie al fenomeno del furto d'identità, ma non sono risultate carenze nei sistemi informatici predisposti dalla banca o nelle misure di sicurezza (tecniche e organizzative) di cui quest'ultima si è dotata a protezione dei dati della propria clientela (art. 32 del RGPD).

Pertanto, muovendo dall'insussistenza, nel caso di specie, di un incidente di sicurezza all'origine dei tentativi di frode, si è ritenuto che non sussistesse l'obbligo di attivare le procedure previste dagli artt. 33 e 34 del RGPD (nota 5 agosto 2022).

La comunicazione di dati a terzi

Con provvedimento 26 maggio 2022, n. 202, il Garante ha dichiarato l'illiceità del trattamento effettuato da un primario istituto di credito che aveva comunicato a un terzo non autorizzato i dati relativi a un rapporto bancario intrattenuto con una propria correntista (doc. web n. 9784626).

I dati così acquisiti venivano prodotti in un giudizio pendente dinanzi al tribunale con la dicitura ad uso interno. Il Garante ha ritenuto illecito il comportamento della banca, invitandola a un supplemento di attenzione rispetto al corretto assolvimento delle istruzioni da parte delle persone autorizzate al trattamento dei dati e applicandole una sanzione amministrativa che tenesse conto che lo stesso istituto di credito, già destinatario di un provvedimento analogo, senza un'adeguata riflessione sulle istruzioni fornite al personale riguardo alle richieste di accesso ai dati bancari, si era limitato a richiamare le attività formative genericamente erogate.

In un altro caso un segnalante aveva lamentato l'indebita trasmissione al proprio indirizzo di posta elettronica di comunicazioni riferite a terzi da parte di un istituto di credito.

Al riguardo, richiamando, tra l'altro, le linee guida adottate in data 25 ottobre 2007, relative al trattamento di dati personali della clientela in ambito bancario (doc. web n. 1457247), la banca è stata invitata in particolare a valutare la rispondenza del trattamento effettuato alle disposizioni e ai principi di carattere generale contenuti nel provvedimento sopra menzionato (nota 17 ottobre 2022).

Le successive verifiche effettuate hanno consentito di appurare che l'indirizzo *e-mail* del segnalante risultava associato al nominativo della cliente della banca presso la camera di commercio territorialmente competente e di escludere, pertanto, violazioni ascrivibili alla banca.

I trattamenti di dati effettuati nell'ambito del cd. Sic

Come ogni anno è stato estremamente intenso il flusso di reclami e segnalazioni in materia di trattamenti di dati personali censiti nei sistemi di informazioni creditizie gestiti da soggetti privati (di seguito, Sic).

Alcune istanze hanno riguardato il tema del preavviso da rendere all'interessato al verificarsi di ritardi nel pagamento degli importi pattuiti e prima dell'inserimento dei dati nei Sic; oltre i tempi di conservazione dei dati nei Sic (diversi a seconda che il rapporto censito sia stato stipulato o meno e, in caso positivo che abbia avuto o meno un andamento regolare).

In tutti i casi sottoposti all'esame dell'Autorità sono state richiamate, in particolare, le norme contenute nel codice di condotta – strumento di autoregolamentazione ad adesione volontaria in grado di concorrere alla corretta applicazione della normativa in materia di protezione dei dati personali (art. 40) – approvato dal Garante in via definitiva, con il provvedimento 6 ottobre 2022, n. 324 con il quale è stato anche accreditato il relativo Organismo di monitoraggio (sul quale v. *infra*).

Nella quasi totalità delle fattispecie esaminate, le istanze pervenute all'Autorità (a valle dell'esercizio, da parte degli interessati, dei diritti di rettifica o di cancellazione dei propri dati dai Sic) sono state dichiarate infondate, in assenza di effettive e comprovate violazioni della normativa in materia di protezione dei dati personali.

L'Organismo di monitoraggio e il codice di condotta

Con provvedimento 6 ottobre 2022, n. 324 (doc. web n. 9818201) il Garante ha accreditato l'Organismo di monitoraggio (OdM) dei Sic ed approvato in via definitiva il codice di condotta degli operatori del settore.

Si è in tal modo completato l'*iter* di adozione del codice di condotta già approvato con riserva dal Garante con provvedimento 12 settembre 2019, n. 163 (doc. web n. 9141941), la cui operatività era stata subordinata proprio al completamento della fase di accreditamento dell'OdM, secondo quanto previsto dall'art. 41 del RGPD.

Nello specifico, l'attento esame del regolamento interno sul funzionamento dell'OdM ha evidenziato la conformità dell'Organismo ai requisiti previsti dall'art. 41, par. 2, del RGPD e dal provv. 10 giugno 2020 recante requisiti di accreditamento degli organismi di monitoraggio dei codici di condotta (doc. web n. 9432569, cfr. Relazione 2020, p. 10 e 184).

In particolare, l'OdM deve verificare l'osservanza di regole di condotta da parte degli aderenti e dei gestori dei sistemi di informazione e gestire i reclami degli interessati. Pertanto, ove un interessato ritenesse violata da parte dei gestori dei Sic e dei partecipanti a questi ultimi, la normativa in materia di protezione dei dati e le disposizioni contenute nel codice di condotta, potrà presentare reclamo direttamente all'OdM. Tale reclamo non preclude, comunque, la possibilità di rivolgersi al Garante.

L'Autorità ha effettuato anche l'esame del testo definitivo del codice di condotta suggerendo gli aggiornamenti e le integrazioni rese necessarie in ragione dell'accreditamento dell'OdM.

Con l'approvazione del provvedimento 6 ottobre 2022 da parte del Collegio e la successiva pubblicazione in G.U., il codice di condotta, che fin dalla sua prima approvazione, il 12 settembre 2019, è stato comunque preso in considerazione dagli operatori del settore quale principio di riferimento cui ispirarsi nello svolgimento della propria attività, ha acquistato piena efficacia.

Costituzione di una rete di Rpd

Nel corso dell'anno è stata avviata la costituzione di una rete di Rpd in ambito bancario allo scopo di costituire un canale di collaborazione con le associazioni di categoria (Abi e Federcasse) e i Rpd designati dai singoli istituti di credito delle imprese operanti nel settore bancario.

Per assicurare il pieno successo dell'iniziativa, il Garante ha ritenuto fondamentale la partecipazione al progetto anche della Banca d'Italia.

Si è pertanto svolto un incontro tra la Banca d'Italia in qualità di ente regolatore e l'Autorità, all'esito del quale si è proceduto alla costituzione di un gruppo di lavoro – composto da Rpd rappresentativi dei diversi istituti di credito – funzionale a valutare lo stato di attuazione delle norme del RGPD in materia di Rpd nonché ad individuare le tematiche di maggiore complessità ed interesse con risvolti sul piano della protezione dei dati personali.

14.3. *Imprese*

Nel corso del 2022, come già negli anni passati, sono pervenute numerose istanze in materia di trattamenti di dati nel settore delle attività a carattere economico.

In tale contesto gli interventi del Garante sono stati sia diretti a dare piena attuazione alla normativa di cui al RGPD e al Codice, sia, più specifici in particolare all'esercizio dei diritti previsti dagli artt. 15-22 del RGPD.

Istruttorie in materia di esercizio dei diritti

La maggior parte delle istruttorie ha riguardato il mancato riscontro ad istanze presentate dagli interessati ai sensi degli artt. 15 e ss. del RGPD.

Si segnala, tra gli altri, il provvedimento 5 agosto 2022, n. 285 (doc. web n. 9811300) con cui l'Autorità ha dichiarato l'illiceità del trattamento effettuato da una società di vigilanza che non aveva fornito alcun riscontro all'istanza di esercizio dei diritti, formulata ai sensi dell'art. 15 del RGPD, volta a conoscere principalmente l'origine dei dati.

Nella specie il reclamante aveva rappresentato di aver ricevuto delle fatture elettroniche di pagamento, pur non avendo mai avuto rapporti contrattuali con la società. Nel corso dell'istruttoria, è stato verificato che la società aveva raccolto i dati personali del reclamante, non direttamente dall'interessato, bensì a seguito dell'acquisizione del ramo di azienda di altra società, senza tuttavia rendere edotti i clienti del mutamento della titolarità del trattamento.

Pertanto, l'Autorità ha ribadito che, a seguito della fusione per incorporazione, agli interessati devono essere forniti i necessari aggiornamenti mediante un'informativa che rechi l'indicazione del nuovo titolare del trattamento, al più tardi entro un mese dall'ottenimento del dato, o, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, entro un mese dalla prima comunicazione (art. 14, par. 3, lett. *a*) e *b*), del RGPD).

In un altro provvedimento (10 novembre 2022, n. 370, doc. web n. 9837981), l'Autorità ha applicato una sanzione amministrativa pecuniaria nei confronti di una società per aver fornito un riscontro meramente formale a una istanza di cancellazione dei dati personali formulata ai sensi dell'art. 17 del RGPD.

In particolare, è risultato che la società, tramite una propria dipendente, aveva dato conferma, in due distinte occasioni, della definitiva cancellazione dei dati dell'istante, continuando invece a conservare i dati nei propri archivi.

***App* Mitiga Italia**

Il Garante con decisione 24 marzo 2022, n. 102 (doc. web n. 9762855) ha confermato il provvedimento 3 giugno 2021, n. 224 relativo alla limitazione provvisoria del trattamento dei dati personali (doc. web n. 9592298) posto in essere, per il tramite di un'applicazione mobile (*app* Mitiga Italia), volta a generare un QR *code* attestante il cd. *status Covid-free* degli utenti registrati, al fine di accedere ad eventi, manifestazioni, luoghi aperti al pubblico (cfr. Relazione 2021, p. 146 e s.).

Invero, considerato che il legislatore aveva previsto la limitazione dell'accesso a luoghi pubblici ed eventi come misura di sanità pubblica per il contenimento dei contagi, il connesso trattamento dei dati poteva essere effettuato esclusivamente in virtù di una idonea norma di rango primario (cfr. art. 6, parr. 2 e 3 e art. 9, par. 2, lett. *i*), del RGPD).

Pertanto, tenuto conto del sopra descritto quadro normativo, il trattamento dei dati personali posto in essere dalla società fornitrice dell'*app* è risultato illecito, ai sensi dell'art. 5, par. 1, lett. *a*), del RGPD, in quanto effettuato in assenza di una valida base giuridica.

Piccole e medie imprese

Sono proseguite le attività di interlocuzione e confronto con le associazioni di categoria maggiormente rappresentative delle piccole e medie imprese allo scopo di definire, nei vari settori di riferimento, i possibili ambiti di intervento, anche

per offrire chiarimenti e/o semplificazioni rispetto agli adempimenti previsti dalla normativa di protezione dei dati.

In particolare, in esito ad una prima analisi interna ad un'associazione, è stata ravvisata l'opportunità di avviare un approfondimento rispetto all'esigenza di un codice di condotta (ai sensi dell'art. 40 del RGPD) che regoli specifici trattamenti di dati effettuati, ad esempio nel settore del benessere (nella specie: palestre, acconciatori e centri estetici); trasporti (sia di persone sia di merci) nonché della comunicazione (soprattutto fotografi, stampa e digitale).

Sono proseguiti i lavori concernenti un codice di condotta in ambito nazionale, ai sensi dell'art. 40 del RGPD, per i trattamenti effettuati da imprese operanti nel settore Ict, per garantire la conformità al RGPD.

Progetto di *check-in* biometrico nel settore alberghiero

Nel 2022 una primaria società operante nel settore alberghiero ha presentato al Garante un progetto sperimentale per il *check-in online* con utilizzo di tecniche di riconoscimento facciale (*matching* fra la ripresa del volto e la foto della carta di identità acquisita tramite la telecamera del dispositivo dell'utente); ciò, allo scopo di acquisire un preliminare orientamento dell'Ufficio sul progetto, pur non avendo presentato una formale richiesta di consultazione preventiva ex art. 36 del RGPD.

L'Autorità, già dalle prime interlocuzioni, ha fatto presente che il trattamento di dati biometrici richiede un'attenta valutazione dell'effettiva necessità e proporzionalità del trattamento, in considerazione della estrema invasività e dell'(in)accuratezza dei risultati prodotti da tali trattamenti e dei rischi elevati ad essi connessi.

La sperimentazione, aveva avuto una durata estremamente ridotta, con i clienti di un'unica struttura in Italia, ed un trattamento assai limitato di dati basato sul consenso dei clienti, ai quali era stato sempre garantito in alternativa il *check-in* tradizionale, presso la *reception*.

All'esito della sperimentazione i dati biometrici raccolti erano stati cancellati (comprese le stringhe criptate, contenenti l'esito positivo del *matching*). La società, che aveva avviato la sperimentazione allo scopo di testare l'interesse e gradimento da parte dei clienti verso una modalità innovativa di *check-in* alberghiero, valutate le potenzialità anche dal punto di vista tecnologico, ha sospeso volontariamente la sperimentazione ed ha dichiarato di non avere intenzione di riattivare il progetto (considerati i costi e i modesti risultati ottenuti).

Progetto ARC II

Il Garante è stato coinvolto, in collaborazione con l'Università di Firenze, nella realizzazione del Progetto biennale ARC II, finanziato dalla Commissione europea, dedicato alle PMI di Italia e Croazia, volto ad incrementare la conoscenza degli obblighi derivanti dal RGPD e dal quadro giuridico italiano e croato in materia di protezione dei dati personali, mediante lo svolgimento di molteplici *workshop* durante i quali le PMI potranno ricevere supporto diretto per risolvere specifici problemi relativi alla conformità al RGPD, nonché la predisposizione di materiali ad uso delle piccole e medie imprese.

Esso porterà anche alla creazione di uno strumento digitale che sarà sviluppato in formato *open source*, in modo che tutte le autorità di protezione dei dati possano adattarlo alla propria legislazione e lingua nazionale e che le PMI di tutta l'UE possano usufruirne.

La realizzazione del progetto richiederà anche la collaborazione delle associazioni di categoria per far sì che esso risponda alle reali esigenze del settore con le quali pertanto proseguiranno le interlocuzioni attualmente in corso (cfr. par. 21.6).

14.3.1. Modifiche ai tempi di conservazione di dati relativi a inadempimenti non regolarizzati

Come noto, il Garante si è pronunciato sulla costituzione di una banca dati inter-operatore, denominata S.I.Mo.I.Tel. e contenente informazioni relative alle morosità nel settore della telefonia (provv. 8 ottobre 2015, n. 523, doc. web n. 4349760).

Il Comitato di gestione interaziendale del Si.Mo.I.Tel., costituito dai partecipanti al Sistema, si è rivolto al Garante per valutare la possibilità di allungare i tempi di conservazione dei soli dati negativi relativi a inadempimenti non successivamente regolarizzati a 60 mesi, a far data dal recesso dal contratto, in luogo dei 36 attualmente previsti, per non esporre gli operatori a rilevanti pregiudizi economici. Muovendo dai principi di cui all'art. 5 del RGPD, e in particolare, dal principio generale di *accountability* (artt. 5, par. 2; 24 e 25 del RGPD), si è anzitutto confermato che la base giuridica del trattamento dei dati contenuti nella banca dati deve ora ritenersi quella prevista dall'art. 6, par. 1, lett. *f*), del RGPD.

Tenuto conto, tra l'altro, che già in passato il Garante, in relazione alla conservazione dello stesso tipo di dati contenuti nei sistemi di informazioni creditizie, aveva ritenuto congruo, con il provvedimento adottato il 26 ottobre 2017, n. 438 (doc. web n. 7221677), il termine massimo di 60 mesi dalla data di scadenza del contratto per la cancellazione delle segnalazioni relative a tale tipologia di inadempimenti, ha ritenuto, ai sensi degli artt. 57, par. 1, lett. *v*), del RGPD e 154, comma 1, lett. *f*) e *g*), del Codice, l'estensione in parola conforme al quadro normativo in materia di protezione dati.

Ciò fermi restando gli ulteriori elementi di garanzia a tutela degli interessi, dei diritti e delle libertà fondamentali degli interessati definiti con il provv. 8 ottobre 2015, n. 523, in quanto compatibili con il vigente quadro normativo in materia di protezione dei dati personali (provv. 24 febbraio 2022, n. 71, doc. web n. 9756688).

14.4. *Concessionari di pubblici servizi*

Nel settore dei concessionari di pubblici servizi, l'Autorità ha svolto diverse attività di controllo per verificare la conformità al Regolamento dei trattamenti delle informazioni inerenti alla morosità dei clienti, posti in essere, dalle società di distribuzione di energia nell'ambito delle comunicazioni fornite al Sistema informativo integrato (cfr. testo integrato del Sistema indennitario a carico del cliente finale moroso nei settori dell'energia elettrica e del gas naturale – TISIND di cui all'all. A alla deliberazione di Arera n. 593/2017/R/com).

In tale contesto, è stato adottato il 22 dicembre 2022, il provv. n. 390 (doc. web n. 9832979) nei confronti di un distributore di energia in ragione dell'illecito trattamento dei dati dei clienti con riferimento alle modalità di gestione dei propri processi interni inerenti all'indennizzo CMOR (corrispettivo di morosità) previsto dal Sistema indennitario.

Si tratta di un complesso meccanismo, introdotto da Arera, al fine di contrastare l'emergere di pratiche scorrette di passaggio, da parte del cliente finale, ad altro fornitore energetico, in pendenza di insoluti con il precedente venditore (cd. turismo energetico).

Il predetto sistema, infatti, riconosce – all'atto dello *switching* ad un nuovo fornitore – un indennizzo che consente, al venditore uscente, di recuperare eventuali crediti non riscossi, tramite un articolato meccanismo di riparto di competenze economiche e di trasmissione di flussi di comunicazione – nell'ambito del Sistema indennitario e attraverso il Sistema informativo integrato.

Sono al riguardo emersi una serie di errori tecnici e di processo (inesatta configurazione delle *query* di estrazione dei dati; errata migrazione delle informazioni nel passaggio da una banca dati ad un'altra; impropria identificazione del periodo temporale di valorizzazione dei dati) che hanno comportato la restituzione al Sistema informativo integrato di informazioni inesatte e non aggiornate sulla morosità dei clienti finali, con effetti pregiudizievoli per gli stessi anche inerenti all'impossibilità di effettuare il passaggio ad altro venditore nel libero mercato.

Tutto ciò in violazione del principio di esattezza (art. 5, par. 2, lett. *d*), del RGPD).

È altresì emersa la conservazione dei dati per 10 anni dalla cessazione del contratto per tutte le tipologie di trattamento, senza alcuna correlazione delle stesse a quanto strettamente necessario al conseguimento delle finalità del trattamento dei dati dei clienti afferenti alle pratiche CMOR, in violazione del principio di limitazione della conservazione (art. 5, par. 2, lett. *e*), del RGPD).

Da ultimo, sono state altresì accertate le violazioni degli artt. 5, par. 2 e 24 (*accountability*), – in ragione dell'inadeguatezza delle misure tecniche e organizzative complessivamente adottate dal titolare rispetto alla natura, al contesto, alle finalità e ai rischi del trattamento dedotto in contestazione – nonché degli artt. 12 e 15 del RGPD (inesatto riscontro all'istanza di esercizio dei diritti dell'interessato).

All'esito dell'istruttoria – che ha richiesto anche lo svolgimento di diversi accertamenti ispettivi *in loco* – è stata applicata una sanzione pecuniaria di un milione di euro rapportata alla elevata gravità delle violazioni accertate e alla dimensione economica della società. Si è tenuto conto al riguardo anche dell'elevato numero di soggetti interessati (circa 16 mila clienti) e della delicatezza delle informazioni oggetto di violazione in quanto atte ad evidenziare l'affidabilità in termini di puntualità dei pagamenti dei clienti.

Per quanto concerne i trattamenti di dati personali dei clienti posti in essere da fornitori operanti nel mercato libero dell'energia elettrica e del gas, è proseguita (v. Relazione 2021, p. 184) l'attività di vigilanza e di controllo con riferimento alle pratiche illecite dei cd. contratti non richiesti, ove effettuate per il tramite di trattamenti di dati personali inesatti e non aggiornati; in particolare, mediante lo svolgimento di accertamenti ispettivi *in loco* sulla base dei diversi reclami pervenuti in materia.

L'esame delle segnalazioni, dei reclami e dei quesiti proposti nei confronti di concessionari di pubblici servizi ha altresì interessato, oltre al settore energetico, anche altri concessionari (società di gestione dei servizi idrici, del trasporto pubblico, dei servizi ambientali, dei servizi postali, concessionari stradali, ecc.).

In tale ambito i profili maggiormente contestati hanno riguardato i presupposti di legittimità del trattamento (con specifico riferimento alla acquisizione di copia dei documenti di riconoscimento degli interessati), i solleciti per finalità di recupero credito, il funzionamento dei portali clienti *online* (soprattutto relativamente alle modalità di registrazione agli stessi), le verifiche di affidabilità dei potenziali contraenti.

14.5. *Attività di recupero crediti*

Anche nel 2022 il trattamento di dati personali finalizzato al recupero stragiudiziale dei crediti è stato oggetto di numerose segnalazioni e reclami rivolti al Garante.

In termini generali, l'Autorità, anche al fine di prevenire il rischio del ricorso a modalità lesive della dignità dei debitori, ha svolto, nell'esercizio dei propri poteri di

cui all'art. 57, par. 1, lett. *d*), del RGPD, un'intesa attività volta alla promozione della scrupolosa osservanza sia della disciplina in materia di protezione dei dati personali (di cui al RGPD e alle disposizioni di cui al d.lgs. n. 196/2003), sia dei principi di carattere generale contenuti nel provvedimento del 30 novembre 2005, sulla liceità, correttezza e pertinenza nell'attività di recupero crediti (doc. web n. 1213644).

Il Garante ha invero sottolineato, in diverse occasioni, ai titolari la necessità di adottare misure di vigilanza sull'operato del personale, nonché di programmare periodiche attività formative e di sensibilizzazione dello stesso, e ogni possibile ulteriore iniziativa volta a rafforzare il livello di tutela degli interessati.

Gli stessi sono stati altresì invitati a vigilare sulle attività poste in essere dai soggetti nominati responsabili ai sensi dell'art. 28 del RGPD nonché a tenere in debito conto, all'atto della designazione degli stessi, le concrete modalità operative utilizzate da questi ultimi.

In alcuni casi è risultata la violazione dei principi posti dalla disciplina sulla protezione dei dati personali (art. 5, par. 1, lett. *a*) e *c*), del RGPD) e delle specifiche prescrizioni impartite dal Garante con il provvedimento sopra menzionato, per l'invio di solleciti di pagamento a terzi estranei al rapporto obbligatorio e sono state altresì applicate sanzioni pecuniarie (provv.ti 7 aprile 2022, n. 122, doc. web n. 9771122 e 9 giugno 2022, n. 215, doc. web n. 9794913). Nel secondo caso, nell'applicare la sanzione amministrativa, si è comunque tenuto conto dell'impegno assunto dalla società nel corso del procedimento ad avviare iniziative sia di carattere tecnico sia di carattere organizzativo, volte anche a garantire la vigilanza sull'operato del personale incaricato allo svolgimento delle attività di recupero crediti.

14.6. *Procedure IMI relative a trattamenti di dati in ambito economico-produttivo*

Come noto, la partecipazione al sistema IMI previsto dal regolamento (UE) 1024/2012, per la gestione dei meccanismi di cooperazione e coerenza previsti dal Capo VII del RGPD impegna le autorità di protezione dei dati del See in misura sempre più rilevante in termini di risorse impegnate e di quantità di lavoro svolto.

Nell'ambito economico le procedure IMI riguardano casistiche eterogenee riferite ad una variegata pluralità di titolari e responsabili del trattamento, considerata la granularità del settore di riferimento.

Si conferma nel 2022 la prevalenza delle procedure IMI ai sensi dell'art. 56 del Regolamento volte all'identificazione dell'autorità capofila (*Lead Supervisory Authority*) e delle autorità interessate (*Concerned Supervisory Authority*) che rappresentano circa il 68% delle procedure trattate.

Nel 2022 l'Autorità si è dichiarata interessata, ai sensi dell'art. 4, n. 22, del RGPD, in 58 casi (28%) assumendo invece la posizione di autorità capofila in un numero limitato di casi riguardanti società con stabilimento unico o principale in Italia.

Rimane sostanzialmente stabile, rispetto al 2021, il numero delle procedure IMI di consultazione informale previste dall'art. 60, par. 1, del RGPD, che consente lo scambio, fra l'autorità di controllo capofila e le autorità interessate, di informazioni, valutazioni e documenti relativi alla controversia prima della fase decisoria vera e propria.

A questo proposito, si segnala che, a seguito degli impegni presi a Vienna il 27 e 28 aprile 2022 dalle autorità di protezione dei dati per rafforzare le procedure di cooperazione e il meccanismo dello sportello unico, il Comitato individua su base regolare, secondo alcuni criteri qualitativi e quantitativi (ad es., numero elevato di interessati coinvolti, problemi strutturali o ricorrenti in più Stati membri, casi

che vedono l'interazione fra protezione dei dati e altri ambiti giuridici), alcuni casi transfrontalieri di importanza strategica (cd. *strategic cases*) per i quali la cooperazione è stata potenziata attraverso la creazione di gruppi di lavoro ristretti di autorità di protezione dei dati sotto la guida della capofila. Questo al fine di addivenire, in tempi rapidi, ad una decisione consensuale, prevenendo obiezioni motivate e pertinenti e il ricorso alla procedura di coerenza per la risoluzione delle controversie di cui all'art. 65 del RGPD.

Sono invece lievemente aumentate, rispetto al 2021, le procedure di cooperazione giunte alla fase decisoria nel settore privato. I progetti di decisione caricati sulla piattaforma IMI dalle competenti autorità capofila sono stati complessivamente, condivisi, salva, ove opportuno, la formulazione di commenti o richieste di chiarimenti.

Si segnala altresì che nel corso dell'anno sono stati adottate dal Garante, in qualità di autorità competente, alcune decisioni emesse all'esito del procedimento di cooperazione.

Si è conclusa la procedura di cooperazione avente ad oggetto il reclamo proposto da un cittadino tedesco volto a segnalare una possibile violazione dell'art. 32 del RGPD da parte di una società con sede in Italia operante nel settore dell'abbigliamento ed accessori sportivi (il titolare gli avrebbe inviato, nella *e-mail* di conferma della registrazione al proprio sito web, la sua *password* in chiaro). Il Garante, in qualità di capofila, preso atto del rafforzamento delle misure di sicurezza da parte del titolare, ha deciso la chiusura del procedimento, pur invitando il titolare del trattamento ad una scrupolosa e continua verifica degli *standard* di sicurezza utilizzati. Il provvedimento finale adottato da parte dell'Autorità italiana ai sensi dell'art. 60, par. 7 è stato notificato al titolare.

In via di conclusione è, inoltre, la procedura di cooperazione avente ad oggetto il reclamo proposto da un cittadino austriaco nei confronti di una piccola società con sede in Italia operante nel settore editoriale e di sviluppo di siti web e volto ad ottenere la cancellazione dei dati dell'interessato. Il Garante, mediante la procedura IMI art. 61 (assistenza reciproca volontaria), ha trasmesso la documentazione ricevuta dal titolare italiano all'Autorità austriaca condividendo con quest'ultima la propria valutazione sul caso. Successivamente, il Garante, in qualità di autorità di controllo capofila, ha proposto, attraverso la procedura IMI art. 60 (consultazione informale), di definire amichevolmente la controversia, senza l'adozione di misure correttive/sanzionatorie. Nel caso concreto, infatti, si è ritenuto che ricorressero i presupposti per un *amicable settlement* previsti dalle linee guida del Comitato 6/2022 sull'attuazione pratica delle composizioni amichevoli, e in particolare: esercizio di un diritto (cancellazione) e corrispondente obbligo adempiuto da parte del titolare, anche grazie all'intervento dell'Autorità; numero limitato di interessati coinvolti e di dati trattati; natura non sistematica della violazione ed effetti lievi della stessa; soddisfacimento dell'interessato. La posizione del Garante è stata condivisa dall'autorità interessata, dopo aver debitamente consultato l'interessato a riguardo (che non ha sollevato ulteriori rilievi); il progetto di decisione è stato condiviso dal Garante, quale capofila, con le altre autorità interessate che non hanno sollevato obiezioni; pertanto è prossima l'adozione del provvedimento finale.

Per quanto riguarda l'assistenza reciproca fra le autorità di controllo ex art. 61 del RGPD, sempre con riferimento all'ambito economico, si conferma l'utilizzo della relativa procedura IMI allo scopo di ottenere informazioni sulle normative nazionali in tema di protezione dei dati o su questioni relative all'applicazione di particolari disposizioni del Regolamento: ad esempio, in materia di normativa anti-riciclaggio; prevenzione di truffa informatica; *usage-based insurance* - cd. *black box* in

ambito assicurativo; videosorveglianza; concessionari; esercizio dei diritti (prassi di compagnie aeree che impongono il pagamento di una *fee* per correggere il nome del passeggero in caso di errore nella prenotazione in violazione dell'art. 16 del RGPD).

Di particolare rilievo, la richiesta della Autorità di protezione dei dati francese in merito all'installazione di sistemi di videosorveglianza nelle stanze private dei residenti nelle case di riposo e dei pazienti di strutture sanitarie, nonché nei dormitori degli asili nido. Per quanto concerne gli istituti scolastici pubblici e privati, il Garante ha richiamato il provvedimento generale sulla videosorveglianza dell'8 aprile 2010 i cui principi possono ritenersi compatibili con il nuovo quadro giuridico vigente (doc. web n. 1712680).

In un altro caso, l'Autorità di protezione dei dati irlandese ha chiesto assistenza agli Stati membri per chiarire la base giuridica del trattamento dei dati di consumo e del tempo di utilizzo dello *smart meter* (ovvero dati di intervallo semiorari) da parte del Gestore del servizio di distribuzione allo scopo di fornire i dati di misurazione del consumo disponibili all'utente finale tramite un portale web. In particolare, è stato chiesto se sia possibile interpretare l'obbligo previsto dall'art. 20 della direttiva 2019/944 – che impone al Gestore di fornire i dati sui consumi dei clienti – come condizione di liceità per la raccolta sistematica da parte dello stesso DSO dei dati sul tempo di utilizzo senza il consenso del cliente.

Nel riscontro fornito il Garante ha rappresentato che l'attuazione delle direttive 2019/944/UE e 2012/27/UE è stata adempiuta attraverso l'istituzione, da parte dell'Arera (cfr. delibera 25 giugno 2019, n. 270/2019/R/com previo parere del Garante 20 giugno 2019, n. 131, doc. web n. 9123551), del Portale dei consumi attraverso il quale è possibile per il cliente finale, previa autenticazione tramite Spid, avere accesso ai dati relativi alle forniture di energia elettrica e gas naturale di cui è titolare, ivi inclusi i propri dati storici di consumo ed i relativi dati tecnici e contrattuali (cfr. art. 5 dell'all. A, delibera Arera n. 270/2019/R/com).

Anche nel 2022 sono stati presentati al Garante reclami ai sensi degli art. 143 e ss. del Codice nei confronti di società con sede in altro Stato membro per i quali si è reso necessario trasmettere la relativa documentazione alla competente autorità capofila. Tra questi, è stato condiviso con la competente autorità, un reclamo presentato da un interessato italiano nei confronti di una società tedesca per presunta violazione del diritto di accesso; altri reclami hanno avuto ad oggetto la richiesta di cancellazione dei dati da *account* aperto su una importante piattaforma con sede principale nel Lussemburgo.

15 Altri trattamenti in ambito privato

15.1. *Trattamento di dati personali nell'ambito del condominio*

Anche nel 2022 si è registrato un significativo afflusso di istanze relative all'ambito condominiale, in prevalenza relative ad argomenti già esaminati e definiti in passato dal Garante e trattati più volte anche in occasione di precedenti Relazioni.

Nel rispondere a istanze, quesiti e richieste di parere l'Ufficio ha pertanto fatto riferimento agli atti già adottati in materia (provv. generale del Garante 18 maggio 2006), rappresentando che anche nel novellato quadro giuridico possono formare oggetto di lecito trattamento da parte della compagine condominiale unitariamente considerata (con l'ausilio, di regola, dell'amministratore nell'eventuale veste di responsabile del trattamento) i soli dati pertinenti e non eccedenti la finalità di amministrazione e gestione del condominio, non quelli (quali numero di telefono o indirizzi *e-mail*) in sé non funzionali alla determinazione dei diritti o degli oneri relativi al bene comune.

Quanto alla comunicazione di informazioni relative ai singoli condòmini a soggetti esterni alla compagine condominiale in assenza di altra idonea base giuridica è necessario il consenso degli interessati.

Nel definire alcune istanze, è stato precisato che l'utilizzo cumulativo e in chiaro degli indirizzi di posta elettronica degli interessati senza la previa adozione di idonei accorgimenti – quali, ad esempio, la funzione ccn – non risulta conforme ai princìpi in materia di protezione dati (tra le altre, note 10 e 20 gennaio, 31 maggio, 7 e 18 ottobre 2022).

All'esito di un'istruttoria avviata a seguito di una segnalazione, l'Autorità ha ammonito uno studio professionale che si occupa di gestioni condominiali per l'omesso riscontro alla richiesta di informazioni formulata dall'Ufficio ai sensi dell'art. 157, d.lgs. n. 196/2003, in relazione alla installazione di una telecamera volta alla ripresa di aree comuni (provv. 7 aprile 2022, n. 120, doc. web n. 9774621). In altri casi sono state fornite informazioni richiamando le regole contenute nel provvedimento generale del Garante in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680) e nel *vademecum* "Il condominio e la *privacy*" del 10 ottobre 2013 (doc. web n. 2680240), nonché le disposizioni introdotte con la legge 11 dicembre 2012, n. 220.

Per quanto riguarda la possibilità di accedere ai dati del registro dell'anagrafe condominiale è stata richiamata la disciplina civilistica (art. 1129, comma 2, c.c.), la cui applicazione spetta al titolare del trattamento nel rispetto del principio di minimizzazione dei dati (art. 5, par. 1, lett. *c*), del RGPD) (nota 27 giugno 2022).

Circa la pubblicazione in bacheca condominiale di dati personali concernenti i singoli condomini pur in assenza di comprovate criticità, nei casi esaminati, è stato raccomandato agli amministratori di condominio di adottare idonee misure atte a evitare l'indebita conoscibilità di dati relativi ai condòmini e di pubblicare, se del caso, solo avvisi di carattere generale, ovvero privi di dati riferiti a soggetti identificati o identificabili.

15.2. *Trattamenti di dati da parte di associazioni e fondazioni*

Nel settore associativo, i profili maggiormente oggetto di contestazione hanno riguardato i presupposti di legittimità del trattamento, con specifico riferimento alla circolazione e diffusione dei dati personali degli associati.

Con riferimento alla divulgazione dei dati personali degli iscritti, l'Autorità ha esaminato un reclamo con cui si lamentava la pubblicazione, sul sito web di una federazione, degli esiti di una prova d'esame, con l'indicazione del giudizio di inidoneità riportato accanto al nome e cognome del reclamante, senza l'utilizzo di modalità che garantissero la conoscibilità di tale informazione esclusivamente ai soggetti interessati.

Nel corso dell'istruttoria, non si sono ravvisati profili di criticità, poiché il d.lgs. 14 marzo 2013, n. 33 e s.m.i. ha disciplinato in maniera organica i casi di pubblicità per finalità di trasparenza sui siti web istituzionali, annoverando tra i soggetti obbligati anche le associazioni e gli enti di diritto privato indicati all'art. 2-*bis*, comma 2. Sono state in proposito richiamate anche le linee guida 15 maggio 2014 (doc. web n. 3134436), sul trattamento di dati personali, contenuti anche in atti e documenti amministrativi, per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati (nota 28 novembre 2022).

Sempre in materia di trasparenza, un reclamo lamentava che una fondazione, ente lirico non a scopo di lucro, aveva pubblicato sul sito web tre determinazioni commissariali contenenti informazioni relative allo stato di salute della reclamante, nonché informazioni idonee a rivelare la pendenza di una procedura disciplinare nei confronti dell'interessata.

Il trattamento è risultato non conforme ai principi di liceità, correttezza e trasparenza, nonché di minimizzazione dei dati, in violazione degli artt. 5, par. 1, lett. *a*) e *c*), in assenza di una idonea base normativa (art. 6, par. 1, del RGPD) e in violazione del divieto di diffusione di dati sulla salute (art. 2-*septies*, comma 8, del Codice, cfr. anche art. 9, par. 4, del RGPD).

Con provvedimento 20 ottobre 2022, n. 346 (doc. web n. 9828987) l'Autorità ha quindi applicato una sanzione amministrativa.

Ancora, è stata riscontrata una richiesta dell'Associazione nazionale magistrati di chiarimenti con specifico riguardo a:

- la possibilità di pubblicare, su una rivista liberamente accessibile *online*, i nominativi e gli esiti dei procedimenti disciplinari endoassociativi;
- la possibilità di pubblicare integralmente, nella sezione del sito fruibile dai soli associati tutti gli atti dei procedimenti disciplinari relativi agli iscritti;
- i limiti temporali per la conservazione e pubblicazione dei predetti dati.

Nel richiamare i princìpi di cui all'art. 5 del RGPD (tra cui quello di responsabilizzazione), l'Autorità, con nota 20 ottobre 2022, ha ricordato che l'attività di pubblicazione sul web impatta significativamente sui diritti e sulle libertà fondamentali degli interessati, vieppiù se la natura dei dati trattati è tale da determinare interferenze non marginali nel contesto relazionale e professionale delle persone coinvolte (in tal senso, già provv. 2 luglio 2020, n. 124, doc. web n. 9445567).

È stata richiamata altresì in particolare l'esigenza di verificare se le operazioni di trattamento siano sorrette da adeguati presupposti giustificativi (consenso degli interessati; obbligo di legge; legittimo interesse del titolare del trattamento o di terzi; ecc.) e di rappresentare chiaramente e puntualmente agli interessati gli scopi perseguiti attraverso la divulgazione. In questo quadro, l'Autorità per la mancanza di un legittimo interesse dell'associazione alla conoscibilità generalizzata dei dati degli iscritti sottoposti a procedimento disciplinare, nonché del consenso degli

interessati, ha ritenuto, con riferimento al primo quesito, che non sussistessero ragioni specifiche che potessero giustificare la pubblicazione delle informazioni su una rivista *online* liberamente accessibile; ciò, tenuto anche conto che la stessa iscrizione all'Associazione non costituisce, di per sé, un dato di dominio pubblico.

Con riguardo al secondo quesito, l'Autorità ha ritenuto che la pubblicazione integrale, anche all'interno di una sezione riservata del sito, di tutti gli atti e documenti relativi ai procedimenti disciplinari degli associati costituisse un trattamento eccedente e sproporzionato, non in linea con il principio di finalità e di minimizzazione dei dati (art. 5, par. 1, lett. *b*) e *c*); ciò, non solo perché tale conoscenza non avrebbe apportato agli associati alcun contributo aggiuntivo in termini di chiarezza, ma anche perché i medesimi atti e documenti potrebbero contenere informazioni molto delicate e riguardare soggetti anche diversi dagli aderenti.

Per quanto attiene, infine, al terzo quesito, è stata confermata la necessità che, in ossequio al principio di limitazione della conservazione dei dati (art. 5, par. 1, lett. *e*), del RGPD, cit.), debba essere individuato un limite temporale alla pubblicazione dei suddetti dati, da stabilire in funzione delle specifiche finalità perseguite.

Riguardo la diffusione via web di dati giudiziari, il Garante ha adottato un provvedimento nei confronti di una federazione sportiva che aveva pubblicato, sul sito internet, un provvedimento disciplinare adottato da un tribunale federale e contenente dati personali relativi a condanne penali e a reati (provv. 20 ottobre 2022, n. 340, doc. web n. 9831323).

Al riguardo, nel rammentare che il trattamento di informazioni idonee a rivelare condanne penali e reati è protetto da un quadro di garanzie particolarmente stringenti (art. 5, par. 1, lett. *a*) e art. 10, del RGPD; art. 2-*octies*, del Codice), non è stata ravvisata la sussistenza nell'ordinamento sportivo di una base giuridica idonea a consentire la diffusione *online* dei dati giudiziari inerenti al reclamante né in ordine alle finalità di pubblicità delle decisioni previste dal diritto sportivo (art. 5, par. 1, lett. *b*) e *c*), del RGPD), né relativamente all'individuazione di garanzie specifiche per i diritti e le libertà degli interessati (art. 10 del RGPD e art. 2-*octies*, comma 1, del Codice). È stata quindi dichiarata l'illiceità del trattamento posto in essere dalla federazione, applicando una sanzione pecuniaria.

Alcune istanze hanno poi riguardato, più in generale, la circolazione endoassociativa dei dati personali degli iscritti.

Nella maggior parte dei casi, non sono stati rinvenuti elementi sufficienti a comprovare un'effettiva violazione della disciplina applicabile, e sono state richiamate indicazioni di carattere generale, salvo eventuali specifiche istruzioni.

Emblematico, in tal senso, è il riscontro fornito ad un interessato che lamentava l'indebita circolazione, all'interno della compagine associativa, di un'informazione concernente il mancato pagamento della propria quota associativa.

In proposito, l'Ufficio ha precisato che le informazioni personali riferite al reclamante, già membro del Collegio dei probiviri, erano state oggetto di lecita condivisione poiché il pagamento di detta quota, in base alle disposizioni statutarie dell'associazione, costituiva condizione necessaria per ricoprire la carica di socio, a sua volta requisito indispensabile per lo svolgimento delle funzioni di probiviro (nota 6 ottobre 2022).

In qualche limitata circostanza, peraltro, si è ritenuto opportuno scrivere anche ai titolari, per invitarli a valutare l'eventuale adozione di adeguate misure atte a garantire un compiuto rispetto della disciplina in materia di protezione dei dati personali.

In un caso, invece, la comunicazione, a tutti gli associati, di informazioni concernenti il provvedimento di esclusione adottato dall'organo sociale nei confronti

15

di un socio è stata ritenuta illecita (provv. 30 giugno 2022, n. 239, doc. web n. 9803345).

Nella fattispecie è emerso, in particolare, che in base al regolamento relativo ai "provvedimenti disciplinari", l'inibizione temporanea o definitiva a ricoprire cariche o incarichi nell'associazione e la radiazione debbono essere pubblicate "sull'organo ufficiale dell'associazione (sito e rivista) […] una volta divenuti definitivi, per mancato ricorso al Collegio dei probiviri o a seguito di decisione di quest'ultimo".

Nel caso di specie, tuttavia, la pubblicazione in questione aveva riguardato un provvedimento non ancora definitivo e – peraltro – successivamente annullato dal Collegio dei probiviri, che ha riconosciuto la fondatezza del ricorso proposto dall'associato.

Peraltro, anche successivamente al suo annullamento il provvedimento è rimasto accessibile per un certo lasso temporale sulla piattaforma *cloud* alla quale accedono tutti i soci, contribuendo a rendere agli stessi una rappresentazione non più pertinente dell'interessato.

Per quanto attiene al tema dell'esercizio dei diritti, l'Autorità è intervenuta nei confronti di una fondazione che non aveva provveduto a fornire riscontro a un'istanza concernente dati di soggetti deceduti (provv. 15 dicembre 2022, n. 426, doc. web n. 9855586).

In considerazione del dolore provocato dalla perdurante ricezione di corrispondenza indirizzata alla defunta madre, la reclamante aveva rappresentato di aver inviato plurime richieste di cancellazione dei dati personali dagli archivi della fondazione, ma di non aver mai ottenuto riscontro. A seguito dell'invito ad aderire formulato dall'Ufficio la fondazione ha dichiarato di aver cancellato i dati personali della *de cuius* scusandosi per il mancato tempestivo riscontro cagionato da un disguido interno.

Nel confermare che la fondazione non aveva fornito riscontro nel termine indicato dall'art. 12, par. 3, del RGPD, l'Autorità ha dichiarato che il disguido non poteva escludere la responsabilità, posto che il carattere colposo della violazione non rileva sul piano dell'accertamento dell'infrazione, ma su quello dell'irrogazione dell'eventuale sanzione amministrativa, di cui costituisce uno degli elementi di valutazione e quantificazione (art. 83, par. 2, lett. *b*), del RGPD). È stato ribadito, inoltre, che il titolare del trattamento è tenuto ad adottare misure appropriate anche (e proprio) al fine di agevolare gli interessati nell'esercizio dei propri diritti in materia di protezione dei dati personali (art. 12, parr. 1 e 2, del RGPD).

Sulla base di tali motivazioni, l'Autorità ha ammonito la fondazione per non aver fornito tempestivo riscontro all'istanza di cancellazione dei dati.

Per quanto attiene, infine, ai tempi di permanenza dei *curricula* e dei certificati del casellario giudiziale dei candidati alle elezioni pubblicati sui siti web di partiti e movimenti politici ai sensi della legge n. 3/2019, l'Autorità ha continuato, anche nel 2022, a seguire e approfondire tale delicata problematica.

Come già rappresentato lo scorso anno (cfr. Relazione 2021, p. 191), è infatti emersa la necessità di individuare congrui termini entro cui provvedere, in assenza di indicazioni normative specifiche, alla rimozione dei predetti documenti dai siti web di partiti e movimenti politici; ciò, anche alla luce dell'esigenza, manifestata dalla Commissione di garanzia degli statuti e per la trasparenza e il controllo dei rendiconti dei partiti politici, di esercitare i propri poteri sanzionatori nei confronti dei soggetti inadempienti entro il termine quinquennale previsto dalla legge n. 689/1981.

Per contemperare i contrapposti interessi l'Autorità ha preso contatto con la menzionata Commissione di garanzia. Il confronto, che ha portato allo scambio di alcune prime, significative riflessioni, è tuttora in corso.

16 Intelligenza artificiale e diritto alla protezione dei dati personali

Le tematiche connesse alla vasta e ancora non normativamente definita nozione di "intelligenza artificiale" (di seguito IA) e alle sue multiformi applicazioni sociali hanno continuato ad essere al centro dell'attenzione dell'Autorità (cfr. par. 23.1.1).

Proposta di regolamento UE sull'IA

Spazio crescente nel dibattito pubblico e tra gli operatori giuridici assume il processo di formazione del quadro regolatorio volto a disciplinare nell'UE le applicazioni sociali dell'IA: a questo proposito, a seguito della proposta di regolamento presentata dalla Commissione europea il 21 aprile 2021 – sulla quale si era incentrato il parere congiunto, reso il 18 giugno 2021, dall'EDPB e dall'EDPS (profili ai quali si è fatto cenno nella Relazione 2021, p. 194) –, deve registrarsi l'avvenuta adozione, il 6 dicembre 2022, dell'orientamento generale sulla stessa da parte del Consiglio dell'UE (in https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/it/pdf). Entro la stessa cornice, il Cepd con lo *Statement on enforcement cooperation* del 28 aprile 2022, ha sottolineato la necessità di un'integrazione organica sia delle norme del RGPD, sia delle autorità di protezione dati nell'architettura normativa che si viene delineando a livello europeo per il mercato digitale (*Data Act, Digital Markets Act, Digital Services Act*, regolamento sull'intelligenza artificiale, *Data Governance Act*), invocando una chiara distribuzione di competenze fra tutti i soggetti regolatori, tale da assicurare una cooperazione efficace (doc. web n. 9765521).

CAI

Parimenti rilevanti, nella formazione della cornice regolatoria sovranazionale, sono gli sviluppi presso il Consiglio d'Europa: in questo ambito, conclusisi i lavori dell'*Ad hoc Committee on Artificial Intelligence* (CAHAI) con l'adozione di un documento finale all'esito della riunione del 30 novembre-2 dicembre 2021 (più ampie informazioni in https://www.coe.int/en/web/artificial-intelligence/cahai), nel 2022 hanno preso l'avvio i lavori del Comitato sull'intelligenza artificiale (*Committee on Artificial Intelligence* - CAI), con l'obiettivo di predisporre un testo di Convenzione internazionale in materia di IA aperto alla ratifica anche da parte di Stati diversi dalle Parti contraenti (analogamente a quanto già accaduto in passato con la Convenzione 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere o con la Convenzione sulla criminalità informatica 185/2001). Oltre all'*Inaugural Meeting* organizzato dal Consiglio d'Europa e dalla Presidenza italiana del Comitato dei ministri del Consiglio d'Europa, tenutosi a Roma il 4 aprile 2022, i lavori – incentrati sul cd. *Zero draft* della *[Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law,* predisposto come base di lavoro dal *Chair* – del CAI con il supporto del Segretariato del Consiglio d'Europa, cui prende parte nell'ambito della delegazione italiana anche un rappresentante dell'Autorità, sono continuati nei giorni 21-23 settembre e proseguiranno nel corso del 2023 (cfr. https://www.coe.int/en/web/artificial-intelligence/cai) (v. par. 21.3).

G7 DPA *Roundtable*

Considerata la (crescente) rilevanza transnazionale del tema, anzitutto nella menzionata prospettiva regolatoria, i profili dell'IA hanno formato oggetto di trattazione in diversi fora di approfondimento: così il Garante ha fatto espresso riferimento alla necessità del "rifiuto di un uso indiscriminato dell'IA applicata ai dati personali che porti a forme di sorveglianza massiva con l'evidente scopo di controllare e manipolare i comportamenti degli individui a partire dai dati personali, raccolti, analizzati e incrociati in grandi quantità, varietà e velocità" nel corso della

Roundtable of G7 Data Protection and Privacy Authorities tenutasi l'8 settembre 2022 sul tema "*Promoting data free flow with trust and knowledge sharing about the prospects for international data spaces*" (cfr. doc. web n. 9803414) (cfr. par. 21.4).

Audizione sull'IA

Il Presidente del Garante si è soffermato sulle preoccupazioni correlate ai possibili impieghi dell'IA che riecheggiano nella discussione internazionale e negli studi in materia, in occasione dell'audizione informale tenutasi il 9 marzo 2022 avanti alle Commissioni IX e X riunite della Camera dei deputati a margine della proposta di regolamento (UE) sull'intelligenza artificiale e con la Memoria presentata in tale circostanza (cfr. doc. web n. 9751565), evidenziando che i trattamenti di dati personali effettuati mediante l'IA (o che contribuiscono al suo "allenamento") si pongono come ulteriore (naturale) oggetto della (più tradizionale) attività dell'Autorità in relazione agli sviluppi delle ICTs e continueranno a caratterizzarne l'azione in futuro. Anche a questo ambito – nella misura in cui i sistemi di IA siano correlati all'effettuazione di operazioni di trattamento di dati personali – si ritiene debbano estendersi le attribuzioni facenti capo alle autorità di protezione dei dati, in linea peraltro con la previsione contenuta nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea, tanto nelle funzioni di controllo, quanto nei compiti ulteriori indicati all'art. 57, par. 1, lett. *i*), ma anche *m*) e *n*) oltre che *b*) e *d*), del RGPD.

GPA-AIWG

Gli effetti dell'IA sul diritto alla protezione dei dati e sui diritti fondamentali hanno formato oggetto di approfondimenti, cui l'Autorità ha contribuito anche entro la cerchia della *Global privacy assembly* (GPA). Ciò è avvenuto, in particolare nell'ambito del GPA *Working Group on Ethics and Data Protection in AI* (AIWG), anzitutto contribuendo alla predisposizione del *Technical report* dedicato al *Risk management* nel contesto dell'IA (cfr. *Risks for Rights and Freedoms of Individuals Posed by Artificial Intelligence Systems - Proposal for a General Risk Management Framework, AIWG Action Point n. 6*, in https://globalprivacyassembly.org, documento presentato in occasione della *Closed session* della 44ª Conferenza GPA tenutasi ad Istanbul il 27 ottobre 2022) e, quindi, in occasione dell'*Internet governance forum* - IGF 2022 *Open Forum Session* (30 novembre 2022). Inoltre, sempre nell'ambito delle attività dell'AIWG, è stata altresì predisposta la risposta ad un questionario in materia di "*AI in Employment*" in vista di una comune elaborazione sul tema in programma per il 2023.

ECHW

L'esperienza applicativa relativa al RGPD rispetto ai primi casi di interazione con l'IA nell'esperienza italiana ha poi formato oggetto di trattazione con altre autorità nazionali di protezione dei dati personali nell'ambito dell'*European Case Handling Workshop* (ECHW) tenutosi a Tbilisi (Georgia) tra il 18-19 novembre 2022.

CEN/CENELEC

Nell'ambito delle interazioni con i diversi attori che si occupano delle tematiche legate all'IA, il contributo dell'Ufficio è stato anche indirizzato ad alcuni tavoli di lavoro istituiti presso il CEN/CENELEC JTC 21, in particolare dedicati ai profili della individuazione e gestione dei rischi connessi all'IA (AI *risk catalogue* e *risk management*) nonché al tema della cd. *data quality*.

L'attività provvedimentale

Nell'ambito dell'attività provvedimentale del Garante, per quanto ancora entro limiti circoscritti, hanno formato oggetto di considerazione alcune applicazioni dei sistemi di IA: ciò è accaduto nell'esame di una valutazione d'impatto predisposta dalla Banca d'Italia per una più efficace trattazione dei reclami alla stessa pervenuti (cfr. provv. 24 febbraio 2022, n. 78, doc. web n. 9751895); anche nel contesto sanitario, con riguardo alla riforma del Fse e all'istituzione dell'Ecosistema dei dati sanitari (Eds), si è prefigurato uno spazio per l'applicazione dell'IA (cfr. provv.ti 22 agosto 2022, nn. 294, doc. web n. 9802729 e 295, doc. web n. 9802752, cfr. par. 5.2.1). E, ancora, con riguardo al tema del trattamento dei dati biometrici, riferimenti all'IA si rinvengono nell'ordinanza-ingiunzione adottata nei confronti

di Clearview AI (provv. 10 febbraio 2022, n. 50, doc. web n. 9751362, sul quale informazioni più puntuali possono essere rinvenute nel par. 12.5).

Infine, con provvedimento 30 luglio 2022, n. 276 (doc. web n. 9808839) un esame approfondito è stato riservato all'impiego dell'IA alla luce di quanto rappresentato nella valutazione di impatto sulla protezione dati relativa al trattamento "Analizzare rischi e fenomeni evasivi/elusivi tramite l'utilizzo dei dati contenuti nell'Archivio dei rapporti finanziari e l'incrocio degli stessi con le altre banche dati di cui dispone l'Agenzia delle entrate" – art. 1, comma 684, l. 27 dicembre 2019, n. 160 (v. già al riguardo il parere 22 dicembre 2021, n. 453, doc. web n. 9738520, cfr. par. 4.1.2). In particolare, per i profili di diretto interesse rispetto all'applicazione di tecniche di IA, si è richiesto alle Amministrazioni interessate (Agenzia delle entrate e Guardia di finanza) di adottare misure idonee ad assicurare: la registrazione del grado di coinvolgimento umano nel processo decisionale; la comprensione, da parte degli operatori alle quali è affidato l'intervento umano, delle capacità e dei limiti del processo decisionale automatizzato, monitorandone debitamente il funzionamento, in modo che i segnali di anomalie, disfunzioni e prestazioni inattese possano essere individuati e affrontati quanto prima; la consapevolezza degli operatori della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'*output* prodotto da un processo decisionale automatizzato utilizzato per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; la corretta interpretazione dell'*output* del processo decisionale automatizzato, tenendo conto in particolare delle caratteristiche del sistema e degli strumenti e dei metodi di interpretazione disponibili; la possibilità per gli operatori di decidere, in qualsiasi situazione particolare, di non usare il processo decisionale automatizzato o altrimenti di ignorare, annullare o ribaltare l'*output* dello stesso.

Cini

Entro la cornice di riferimento dell'accordo quadro di durata triennale formalizzato il 17 gennaio 2022 con il Consorzio interuniversitario nazionale per l'informatica – Cini (al quale si è fatto cenno nella Relazione 2021, p. 195), prime interlocuzioni sono intervenute con il "Lab Nazionale IA". Nello stesso contesto iniziative ulteriori hanno trovato nel frattempo concreta attuazione: in particolare, sulla base di un'apposita convenzione esecutiva con il Lab Nazionale "Informatica e scuola" in relazione alla iniziativa "Programma il futuro", personale dell'Ufficio ha tenuto un primo ciclo di *webinar* mirati al mondo della scuola che, seguendo il corso dell'anno scolastico, troverà completamento con un secondo ciclo di *webinar*, dedicati a profili di interesse dei minori rispetto alle nuove tecnologie, nella prima parte del 2023. Tutti i *webinar* sinora realizzati (arricchiti da materiali di primo riferimento) sono accessibili all'indirizzo https://programmailfuturo.it/notizie/*webinar*. Ad accompagnare questa attività, con il concorso del Lab Nazionale "Informatica e società", è stato altresì concordato lo svolgimento, nel 2023, di un ciclo di seminari presso il Garante su vari profili connessi allo sviluppo delle ICTs: si tratta di un'iniziativa finalizzata a consolidare le competenze tecnologiche presso l'Autorità e ad aumentare la consapevolezza di quanti in essa operano circa le implicazioni sociali degli sviluppi tecnologici emergenti.

LeADS

È proseguita, infine, la cooperazione nell'ambito del Progetto di ricerca denominato *Legality Attentive Data Scientist* (LeADS), finanziato dall'UE nell'ambito del programma Horizon 2020 – *Research and Innovation Framework* e coordinato dal prof. Giovanni Comandé (Scuola superiore Sant'Anna di Pisa), alle cui attività l'Autorità partecipa in qualità di *partner*; l'iniziativa, che vede inoltre 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 imprese

16

(piccole, medie e grandi), mira a formare esperti in *data science* e diritto in grado di operare nel settore dell'intelligenza artificiale; all'interno di questa cornice l'Autorità ospiterà presso la propria sede, a partire dal 2023, quattro dottorandi di ricerca afferenti al Consorzio universitario.

17 Violazione dei dati personali

Dal 1° gennaio al 31 dicembre 2022 sono state notificate all'Autorità n. 1.351 violazioni dei dati personali ai sensi dell'art. 33 del RGPD o dell'art. 26 del d.lgs. n. 51/2018, da parte di soggetti pubblici (31,2% dei casi) e privati (68,8% dei casi). Alcune sono state notificate per fasi (come previsto dall'art. 33, par. 4, del RGPD e dall'art. 26, comma 1, d.lgs. n. 51/2018) con l'invio, in un primo momento, di una notifica preliminare e, successivamente, di una o più notifiche integrative.

In particolare, nel settore pubblico, le violazioni dei dati personali hanno riguardato soprattutto comuni, istituti scolastici e strutture sanitarie; nel settore privato, sono stati invece coinvolti sia piccole e medie imprese e professionisti, che grandi società del settore delle telecomunicazioni, energetico, bancario e dei servizi.

I fenomeni più frequentemente riscontrati sono stati la diffusione di *malware* di tipo *ransomware*, che ha compromesso la disponibilità dei dati all'interno dei sistemi *server*, delle postazioni di lavoro e dei *database* di numerose organizzazioni pubbliche e private, e che, in molti casi, ha anche inciso sulla riservatezza delle informazioni trattate; l'accesso non autorizzato o illecito ai dati personali trattati all'interno di sistemi informativi complessi; la diffusione accidentale di dati personali a causa di erronea configurazione o utilizzo dei sistemi *software* di gestione della posta elettronica.

L'attività istruttoria svolta a seguito della notifica delle violazione dei dati personali ha avuto come duplice obiettivo quello di esaminare l'adeguatezza delle misure adottate dal titolare del trattamento (o che lo stesso intendeva adottare) per porre rimedio alla violazione dei dati personali o per attenuarne i possibili effetti negativi nei confronti degli interessati, nonché di valutare la necessità di comunicare la violazione agli interessati coinvolti, fornendo indicazioni specifiche sulle misure da adottare per proteggersi da eventuali conseguenze pregiudizievoli.

Con riferimento ad alcune violazioni dei dati personali rispetto alle quali i titolari del trattamento avevano ritenuto di non dover informare gli interessati coinvolti, l'Autorità, dopo aver valutato la probabilità che le violazioni presentassero un rischio elevato, ha ingiunto ai titolari di provvedervi senza ritardo.

Nei casi in cui è emersa una possibile inadeguatezza delle misure di sicurezza adottate dal titolare o dal responsabile, sono stati acquisiti gli elementi necessari a individuare le lacune organizzative e tecniche che hanno determinato, o hanno contribuito a determinare, le violazioni dei dati personali notificate. Tale attività di approfondimento ha portato all'adozione di alcuni provvedimenti collegiali di tipo correttivo e, nei casi più gravi, sanzionatorio.

18 Il trasferimento dei dati personali all'estero

Nel 2022 l'attività del Garante nel settore del trasferimento dei dati all'estero è stata prevalentemente caratterizzata dalla definizione delle istruttorie avviate a seguito della presentazione di alcuni reclami nei confronti di diversi gestori di siti web, relativi alla legittimità dei trasferimenti dei dati personali degli utenti verso gli USA, posti in essere in conseguenza dell'utilizzo, tramite i loro siti internet, di Google Analytics.

L'Autorità, all'esito di una complessa indagine effettuata di concerto con le altre autorità di controllo europee, nell'ambito della *task force* specificamente incaricata di coordinare l'esame di 101 reclami presentati nei confronti di diversi titolari del trattamento stabiliti negli Stati membri del See (cfr. Relazione 2021, p. 199), ha adottato tre provvedimenti (9 giugno 2022, n. 224, doc. web n. 9782890; 7 luglio 2022, n. 243, doc. web n. 9806053 e 21 luglio 2022, n. 254, doc. web n. 9808698) rilevando che l'utilizzo di Google Analytics, da parte dei gestori dei siti web, in qualità di titolari del trattamento, comporta il trasferimento dei dati personali dei visitatori dei suddetti siti verso Google LLC con sede negli Stati Uniti.

È emerso che i gestori dei siti web che utilizzano Google Analytics raccolgono, mediante *cookie*, l'indirizzo Ip del dispositivo dell'utente, nonché le informazioni sulle interazioni degli utenti con i predetti siti, le singole pagine visitate e i servizi proposti.

In particolare, è stato accertato che tali informazioni sono state oggetto di trasferimento verso gli USA e che le garanzie di cui alle clausole contrattuali tipo sottoscritte dai titolari in tale contesto non sono risultate adeguate. Il Garante ha altresì constatato, anche alla luce delle indicazioni fornite dal Cepd nella raccomandazione 1/2020 del 18 giugno 2021, che le misure supplementari adottate da Google non garantivano un livello adeguato di protezione dei dati, stante la possibilità, per le autorità e agenzie di *intelligence* statunitensi, di accedere ai dati personali degli utenti.

Pertanto, nel dichiarare l'illiceità dei suddetti trasferimenti ai sensi degli artt. 44 e 46 del RGPD, il Garante ha ammonito i gestori dei siti web destinatari degli accertamenti, ingiungendo agli stessi di conformarsi al RGPD, entro novanta giorni dalla data di notifica dei provvedimenti; ciò adottando misure supplementari adeguate, pena la sospensione dei flussi di dati effettuati, per il tramite di Google Analytics, verso gli Stati Uniti.

L'Autorità ha quindi richiamato l'attenzione di tutti i gestori italiani di siti web, pubblici e privati, sull'illiceità dei trasferimenti effettuati verso gli USA qualora gli stessi utilizzino Google Analytics sulla base delle misure tecniche e organizzative allo stato messe a disposizione da Google, invitando al contempo i titolari del trattamento a verificare la conformità degli strumenti di web *analytics* utilizzati sui propri siti internet con la normativa in materia di protezione dei dati personali (v. comunicato stampa 23 giugno 2022, doc. web n. 9782874).

Nel corso dell'anno è inoltre proseguita l'attività di collaborazione del Garante nell'ambito della menzionata *task force* con specifico riferimento alle istruttorie aventi ad oggetto la liceità dei trasferimenti dei dati personali verso gli USA, posti in essere da alcuni gestori di siti web, mediante l'utilizzo di Facebook Pixel. In tale

contesto, maggiori elementi in merito alle caratteristiche dei servizi resi da Meta Platforms sono stati acquisiti tramite un'attività di coordinamento e di scambio di informazioni tra le varie autorità di controllo nazionali partecipanti.

Da ultimo, con riguardo all'istanza in ordine all'approvazione di Bcr ai sensi dell'art. 47 del RGPD presentata da un gruppo multinazionale d'impresa, *leader* nel settore delle infrastrutture digitali, l'Autorità in qualità di Bcr *lead* della relativa procedura europea di cooperazione (cfr. Relazione 2020, p. 198), ha condiviso, con le autorità *co-reviewer* e le altre autorità di controllo interessate, lo schema consolidato di decisione predisposto dal Gruppo.

19 L'attività ispettiva

19.1. *L'attività ispettiva dopo l'emergenza pandemica*

L'anno 2022 ha segnato, anche per quello che concerne l'attività ispettiva, il superamento della fase emergenziale e la ripresa, in condizioni di "quasi" normalità, delle attività di accertamento *in loco*.

È stato così possibile riprendere quell'indispensabile presenza sul territorio che, al di là delle caratteristiche del singolo intervento, contribuisce a dare concretezza ed effettività al dettato normativo e svolge una significativa funzione di deterrenza, con il correlato positivo effetto di "moltiplicatore di legalità".

I dati statistici confermano queste asserzioni, come dimostrato dal numero globale di interventi *in loco* effettuati nell'anno: 140, a fronte dei soli 49 realizzati nell'anno 2021, quando il persistente stato di emergenza indotto dalla pandemia aveva obbligato l'Autorità (specie nel primo semestre) a ridurre drasticamente gli interventi sul territorio.

Dei 140 accertamenti svolti *in loco* nel corso dell'anno, 45 sono stati effettuati direttamente dal personale in servizio presso l'Ufficio, i rimanenti 95 sono stati invece delegati al Nucleo speciale *privacy* e frodi tecnologiche della Guardia di finanza.

Le attività ispettive hanno riguardato, come sempre, un variegato campo di trattamenti di dati personali, passando da situazioni molto puntuali e limitate (coinvolgenti quindi un ristretto numero di interessati) ad accertamenti di maggior impatto (talora collegati a violazioni di dati personali che avevano interessato un elevato numero di soggetti) caratterizzati anche da una rilevante complessità tecnologica.

Del resto ormai quasi tutte le ispezioni richiedono uno sforzo organizzativo trasversale che coinvolge una pluralità di competenze. Ai funzionari ispettivi in senso proprio (rivestenti, tra l'altro, il ruolo di ufficiale di polizia giudiziaria) si affiancano necessariamente sia i funzionari dello specifico dipartimento giuridico coinvolto negli accertamenti (di regola assegnatari del fascicolo istruttorio relativo alla vicenda in esame) sia gli ingegneri informatici del dipartimento tecnologico, il cui ausilio è sempre più determinante.

Tutte le attività svolte, sia quelle nate da autonome iniziative dell'Ufficio sia quelle più strettamente connesse alle istruttorie già in corso relative a reclami e segnalazioni, si sono ovviamente inserite nel solco delle due delibere (provv.ti 22 dicembre 2021, n. 452, doc. web n. 9737049 e 21 luglio 2022, n. 277, doc. web n. 9809072) con le quali il Collegio ha fissato, ai sensi dell'art. 4 del reg. n. 1/2019 del Garante, le linee della programmazione semestrale delle attività ispettive.

Fra gli ambiti più significativi possiamo ricordare le attività di trattamento dei dati a fini di *marketing* e profilazione (con un'attenzione specifica ai soggetti operanti mediante pratiche di *telemarketing*, nonché alle imprese utilizzatrici di carte di fidelizzazione), le verifiche sull'impiego della tecnologia *cloud* in ambito pubblico, le ispezioni volte a controllare l'effettiva implementazione da parte dei gestori di siti web delle disposizioni contenute nelle cd. linee guida sui *cookie* pubblicate dal Garante il 10 giugno 2021, n. 231 (doc. web n. 9677876).

Allo scopo di corrispondere agli obblighi comunitari in materia, sono poi state

effettuate le verifiche periodiche relative ai trattamenti dei dati personali nell'ambito del sistema VIS (*Visa Information System*), che è un sistema informatizzato di condivisione dei dati relativi ai visti d'ingresso nello spazio Schengen. Come da protocolli comunitari, i controlli hanno riguardato sia le strutture centrali del sistema (presso i Ministeri degli affari esteri e dell'interno a Roma ed il Centro elaborazione dati della Polizia di Stato di Napoli), sia alcuni uffici decentrati sul territorio (in particolare gli uffici della Polizia di frontiera presso l'aeroporto di Fiumicino e lo scalo marittimo di Civitavecchia).

Una serie (più consueta) di accertamenti ha infine riguardato il tema, sempre oggetto di vivace contenzioso, del trattamento dati tramite sistemi di videosorveglianza. Ciò, con particolare riguardo ai casi in cui il titolare sia un'impresa e le telecamere riprendano, oltre a clienti, fornitori e terzi estranei, anche lavoratori dipendenti.

19.2. *La collaborazione con la Guardia di finanza*

I dati statistici citati nel precedente paragrafo, hanno già evidenziato il rilevante apporto fornito all'attività ispettiva dal Nucleo speciale *privacy* e frodi tecnologiche della Guardia di finanza.

Lo sforzo effettuato nel 2022 è stato quello di coinvolgere maggiormente il Nucleo nelle attività svolte dall'Ufficio, attraverso la partecipazione diretta di ispettori del Nucleo a controlli (solitamente complessi e articolati) curati direttamente dai dipartimenti giuridici.

L'obiettivo è quello di poter delegare un sempre maggior numero di interventi complessi agli ispettori della Guardia di finanza, moltiplicando così, in termini sia quantitativi che qualitativi, la presenza dell'Autorità sul territorio.

Le ispezioni congiunte (funzionari dell'Ufficio più ispettori del Nucleo), precedute da incontri preparatori presso la sede dell'Autorità e seguite da un'attività di accurato esame congiunto dei verbali di operazioni compiute e del materiale acquisito, hanno rafforzato il livello di competenze dei militari che non sono permanentemente distaccati presso l'Ufficio e hanno permesso di progettare cicli ispettivi più ampi del passato, delegando *in toto* al Nucleo, dopo le prime attività svolte insieme, i controlli successivi.

Negli ultimi mesi dell'anno questo *format* operativo ha poi trovato un'esplicazione particolare nei controlli relativi alle citate linee guida sui *cookie*. In questo caso, concretizzando una modalità operativa già prevista nel Protocollo d'intesa con la Guardia di finanza, sono stati effettuati una serie di accertamenti *online*, cioè un'attività ispettiva realizzata da remoto, che per la sua intrinseca agilità di esecuzione, permette, quando la tipologia dei controlli da effettuare lo consente, un maggior numero di interventi, moltiplicando così la possibilità per il Garante di effettuare accertamenti su ampie platee di titolari del trattamento, contribuendo ad assicurare, di conseguenza, un maggior grado di effettività alla normativa di settore ed alle linee interpretative dell'Autorità.

20 Il contenzioso giurisdizionale

20.1. *Considerazioni generali*

In applicazione del quadro normativo vigente, tutte le controversie che riguardano l'applicazione della disciplina in materia di protezione dei dati personali devono essere comunicate al Garante, anche se non sono relative all'impugnazione di provvedimenti dell'Autorità (artt. 152 del Codice e 10, comma 9, d.lgs. n. 150/2011, come modificato dall'art. 17, d.lgs. n. 101/2018).

In relazione a tale incombente informativo, si registra, nel decorso anno, un leggero aumento rispetto al passato: a fronte dei 56 nel 2020 e dei 58 del 2021, nel 2022 è stata comunicata all'Autorità la pendenza di 70 opposizioni.

Permane, invece, non sempre puntualmente adempiuto l'altro obbligo, a carico delle cancellerie, di trasmettere al Garante copia dei provvedimenti emessi dall'Autorità giudiziaria in materia di protezione dati e di criminalità informatica (art. 154, comma 6, del Codice).

Salvo quanto si dirà al par. 20.3, tali obblighi di comunicazione consentono all'Autorità di monitorare l'evoluzione della giurisprudenza in materia di protezione dei dati personali ed eventualmente di segnalare al Parlamento e al Governo gli interventi normativi ritenuti necessari per la tutela dei diritti degli interessati.

20.2. *Le opposizioni ai provvedimenti del Garante e le decisioni giudiziali di maggior rilievo*

L'anno 2022 ha registrato un leggero incremento nella proposizione delle opposizioni a provvedimenti dell'Autorità: 123 a fronte dei 115 del 2021.

Nell'anno di riferimento, inoltre, l'Autorità ha avuto notizia di 113 decisioni dell'Autorità giudiziaria relative a opposizioni a provvedimenti del Garante (di cui 40 relative a cartelle di pagamento).

Di seguito si dà conto delle sentenze di maggior rilievo.

Trattamento di dati da parte di soggetti pubblici

La Corte costituzionale ha respinto il ricorso per conflitto di attribuzione promosso da una provincia autonoma sorto a seguito del provvedimento del Garante 18 giugno 2021, n. 244 (doc. web n. 9671917) che ha stabilito come la disciplina della certificazione verde (*green pass*), in quanto implicante un trattamento dei dati personali ai sensi del RGPD, possa essere recata solo da una uniforme disciplina statale, con gestione per mezzo della Piattaforma nazionale-DGC ed ha imposto alla provincia autonoma la limitazione definitiva dei trattamenti relativi all'utilizzo del *green pass*, eseguiti in forza di ordinanze del presidente della giunta provinciale. In particolare, la provincia sosteneva che non spetterebbe al Garante affermare che la regolamentazione del *green pass* competa alla sola normativa statale. La Consulta ha invece ritenuto corretto il provvedimento del Garante, rilevando tra l'altro che "la limitazione delle competenze regionali o provinciali che ne dovesse conseguire troverebbe fondamento e giustificazione direttamente nel diritto dell'Unione europea, nella misura in cui il provvedimento del Garante sia stato adottato in presenza dei presupposti e nel rispetto dei limiti stabiliti dal Regolamento n. 2016/679/UE"

(Corte costituzionale n. 164/2022).

Il Tribunale di Milano, con sentenza n. 4135/2022, ha rigettato il ricorso presentato da un ente sanitario contro il provvedimento del Garante 13 maggio 2021, n. 268 (doc. web n. 9685332) riguardante l'implementazione di un servizio, tramite web, che consentiva di conoscere se un cittadino dell'area metropolitana di riferimento fosse o fosse stato positivo al Covid-19, semplicemente inserendo il codice fiscale e il numero di telefono mobile del cittadino. In particolare, se il soggetto era o era stato positivo, il sito rivelava che era già presente un *account* per tale soggetto (consigliando l'accesso tramite le credenziali *e-mail* e *password*); in caso contrario, proponeva allo stesso la registrazione al servizio; ciò rivelava indirettamente ma con certezza lo stato di positività attuale o passato al Covid-19. L'ente ha impugnato il provvedimento del Garante per una pluralità di motivi di carattere sostanziale e procedurale, giungendo a negare che il Garante fosse legittimato ad irrogare sanzioni amministrative pecuniarie nei confronti di soggetti pubblici. Il Tribunale ha respinto tutte le argomentazioni del ricorrente, riconoscendo la correttezza del procedimento e del provvedimento del Garante con particolare riferimento all'inadeguatezza dello standard di sicurezza del sistema, alla mancanza di adeguata informativa ed alla omessa effettuazione di una valutazione di impatto. Il Tribunale ha pure escluso che l'emergenza pandemica allora in atto potesse consentire di escludere la responsabilità dell'ente per la sussistenza dello stato di necessità o di forza maggiore. La sentenza è stata impugnata davanti alla Corte di cassazione ed il relativo giudizio è ancora in corso.

Con sentenza 5 ottobre 2022, n. 14423, il Tribunale di Roma ha respinto il ricorso di un'amministrazione statale sanzionata dal Garante (provv. 29 ottobre 2020, n. 205, doc. web n. 9493020) per aver comunicato dati errati riferiti ad un provvedimento di sicurezza adottato nei confronti di un cittadino e, pur consapevole dell'errore, aver provveduto alla rettifica di tali dati con grave ritardo, violando gli artt. 3, comma 1, lett. *a*) e *d*), 4, comma 3, e 12, comma 1, d.lgs. n. 51/2018. Il Tribunale ha respinto il ricorso, rigettando in particolare il motivo della tenuità del fatto addebitato con conseguente illegittimità della sanzione, dal momento che era provata la violazione del trattamento dei dati dell'interessato e la lesione del diritto di costui alla correttezza delle informazioni circa i propri dati personali, alla quale l'amministrazione interessata non aveva tempestivamente rimediato.

Con sentenza 17 ottobre 2022, il Tribunale di Roma ha respinto il ricorso da parte di un'amministrazione statale avverso l'ordinanza-ingiunzione 11 febbraio 2021, n. 54 (doc. web n. 9556625), con cui il Garante le aveva inflitto una sanzione pecuniaria di euro 75.000,00 per la violazione degli artt. 5, par. 1, lett. *a*), *b*) e *c*); 6, par. 1, lett. *c*) ed *e*), par. 2 e par. 3, lett. *b*); 37, par. 1 e par. 7 del RGPD. Il Tribunale ha ritenuto fondata l'eccezione di improcedibilità, sollevata dal Garante in giudizio con il patrocinio di un avvocato del libero foro, in quanto il ricorso del Mise era stato notificato al Garante oltre il termine di cui all'art. 10 del d.lgs. n. 150/2011.

Il Tribunale ha rappresentato che la suddetta disposizione "prescrive, al comma 6, che il ricorso-decreto sia notificato entro il termine «perentorio» fissato dal giudice. Trattasi pertanto di un termine imposto a pena di decadenza. Non può condividersi l'argomentazione difensiva principale dell'Avvocatura, secondo la quale la perentorietà del termine sarebbe nella specie da escludersi perché non espressamente indicata nel decreto di fissazione dell'udienza di comparizione. Invero, il carattere perentorio del termine è direttamente previsto dalla legge (che la parte ha l'onere di conoscere ed osservare) e pertanto non abbisogna di alcuna esplicita conferma – o, meglio, ripetizione – nel singolo provvedimento giudiziario. Del resto, non è ipotizzabile che un termine definito perentorio dalla legge possa essere "degradato" a termine

20

ordinatorio dal giudice, neppure per sua esplicita volontà manifestata espressamente in un provvedimento, ed *a fortiori* per effetto della mera omissione, di per sé non inequivocabilmente significativa, di una precisazione peraltro superflua, trattandosi semplicemente di dare attuazione ad un preciso precetto normativo [...] e di trarne le inevitabili conseguenze". Nella specie, quindi, è stata ritenuta maturata la decadenza in danno della parte ricorrente e il ricorso è stato dichiarato improcedibile.

Con sentenza 21 ottobre 2022, il Tribunale di Roma ha accolto parzialmente il ricorso proposto dal Ministero dell'interno avverso il provvedimento del Garante 10 giugno 2021 n. 289 (doc. web n. 9701975) – con cui l'Autorità aveva ordinato al Ministero il pagamento di una sanzione di euro 75.000,00 per la divulgazione dei video contenenti le aggressioni avverso un pensionato di Manduria, deceduto a seguito delle violenze subite da parte di un gruppo di giovani del suo territorio, sui profili *social* della questura competente e della Polizia di Stato (per la violazione degli artt. 3, comma 1, lett. *a*) e *c*) e 5, d.lgs. n. 51/2018) – riducendo la medesima sanzione a euro 50.000,00. In particolare il Tribunale ha ritenuto che la pubblicazione dei video, peraltro rimossi dopo circa un mese su indicazione del resistente, sia avvenuta in violazione della dignità della vittima, tenuto conto dell'omessa alterazione della parte audio come risulta nel provvedimento del Garante e dall'ascolto dei video depositati in atti dalle parti, nonostante la richiesta in tal senso da parte della Procura della Repubblica.

Con sentenza 11 novembre 2022, n. 33257, la Corte di cassazione ha accolto il ricorso proposto nell'interesse di questa Autorità con rinvio al Tribunale di Firenze. Con ordinanza-ingiunzione, l'Autorità aveva ordinato ad un'unione comunale il pagamento di euro 10.000,00 ai sensi dell'art. 162, comma 2, d.lgs. n. 196/2003, assumendo che l'ente aveva illegittimamente pubblicato sul proprio sito web la graduatoria pacchetto scuola 2010-2013 per l'ammissione a sussidi scolastici per famiglie indigenti, con i dati personali dei soggetti non ammessi al beneficio e informazioni non pertinenti riguardanti gli assegnatari, quali la residenza dell'alunno e del genitore, la tipologia di scuola e di classe frequentata e il valore Isee di ciascun beneficiario. Il Tribunale di Firenze aveva accolto integralmente l'opposizione dell'unione comunale, osservando che, nel procedere alla pubblicazione della graduatoria, l'unione comunale si era adeguata alle indicazioni contenute nell'atto dirigenziale provinciale n. 3175/2012, diffondendo informazioni strettamente funzionali a garantire la trasparenza dell'azione amministrativa ai sensi del d.lgs. n. 33/2013, in conformità alle linee guida adottate dal Garante con provvedimento 15 maggio 2014 (doc. web n. 3134436).

Secondo la Cassazione, l'amministrazione, in ossequio al disposto degli artt. 3 e 11, comma 1, lett. *d*), del Codice, allora vigenti, doveva comunque attenersi al principio imperativo ed inderogabile della minimizzazione e necessità della diffusione, privilegiando, se del caso, la pubblicazione di dati anonimi e osservando modalità che permettessero di identificare l'interessato solo in caso di necessità. In definitiva, secondo la Suprema Corte, la diffusione di dati diversi da quelli espressamente previsti dal d.P.R. n. 118/2000, non beneficiava di fondamento normativo ai sensi dell'art. 19, comma terzo, del Codice. Le disposizioni del d.lgs. n. 33/2013 non erano in vigore al momento della violazione e non contemplavano – in ogni caso – la facoltà di pubblicare tutti i dati personali dei soggetti interessati dalla procedura di assegnazione dei benefici (inclusi coloro che non avevano ottenuto alcuna sovvenzione). Infatti, "in ogni ipotesi in cui l'amministrazione proceda alla pubblicazione di dati, informazioni e documenti che comporti un trattamento di dati personali, devono essere opportunamente contemperate le esigenze di pubblicità e trasparenza con i diritti e con la dignità dell'interessato, con particolare riferimento

alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (art. 2, d.lgs. 196/2003)". La Suprema Corte ha ricordato, infine, con quale principio costante nella sua giurisprudenza che l'art. 3, l. n. 689/1981 pone una presunzione di colpa a carico dell'autore del fatto vietato, gravando sul trasgressore l'onere di provare di aver agito senza colpa (Cass. nn. 13610/2007; 20219/2019 e 11777/2020).

L'esimente della non colpevolezza può configurarsi, al pari di quanto avviene per la responsabilità penale in materia di contravvenzioni, solo quando detta violazione appaia inevitabile, occorrendo a tal fine, da un lato, la sussistenza di elementi positivi, estranei all'autore dell'infrazione, idonei ad ingenerare la convinzione della liceità della condotta e, dall'altro, che l'autore dell'infrazione abbia fatto il possibile per osservare la legge, onde nessun rimprovero possa essergli mosso, neppure sotto il profilo della negligenza omissiva (Cass. nn. 19759/2015, 33441/2019 e 24081/2019). L'essersi l'unione comunale conformata ad un provvedimento dirigenziale provinciale concernente aspetti non riguardanti la pubblicazione dei dati personali, pur essendo necessario che la pubblicazione fosse consentita da una previsione di legge e non da un atto meramente amministrativo, non poteva condurre ad escludere la colpa e la responsabilità dell'amministrazione, non risultando che l'unione dei comuni si fosse resa parte diligente in modo da ricevere un affidabile riscontro della liceità della pubblicazione, facendo il possibile per evitare le violazioni contestate. Per tali ragioni, sono stati accolti entrambi i motivi di ricorso proposti dal Garante.

Trattamento di dati in materia di mobilità

È stato respinto il ricorso avverso il provvedimento con il quale il Garante aveva comminato una sanzione pecuniaria ad una società per aver trattato dati personali degli utenti (raccolti attraverso una determinata tipologia di parcometri), senza essere stata previamente nominata quale sub-responsabile per il trattamento e senza avere adottato i prescritti registri di trattamento, indispensabili per valutare la conformità dei trattamenti alla normativa in materia di protezione dati (provv. 22 luglio 2021, n. 292, doc. web n. 9698558). Il Tribunale di Roma con sentenza 23 giugno 2022, n. 10214, ha in particolare deciso che l'esistenza di obblighi contrattuali di natura privatistica tra l'opponente e la sua committenza non può giustificare un trattamento effettuato senza il rispetto delle prescrizioni regolamentari, ed inoltre, la circostanza che in una fase successiva si sia dato luogo alla formalizzazione della nomina non vale a sanare i trattamenti effettuati in precedenza. Il Tribunale ha altresì chiarito che il numero di targa dei veicoli costituisce, in una percentuale statisticamente preponderante, un dato personale idoneo a risalire alla persona dell'utilizzatore del parcometro, consentendone dunque la profilazione, onde il trattamento non può dirsi irrilevante sotto questo profilo. Quanto alla violazione relativa alla omessa tenuta dei registri delle attività di trattamento di cui all'art. 30 del RGPD, il Giudice ha ritenuto che sussistono i requisiti di obbligatorietà della relativa istituzione (requisiti che la norma declina in via alternativa e non cumulativa) posto che la raccolta dei dati in questione, non occasionale e relativa ad una mole notevole di informazioni, implica un rischio effettivo per il diritto alla riservatezza degli interessati (le cui abitudini ed i cui spostamenti sono suscettibili di profilazione attraverso la raccolta dei numeri di targa dei veicoli in sosta).

Con sentenza 15 novembre 2022, il Tribunale di Roma ha rigettato il ricorso presentato da un'azienda municipalizzata contro un'ordinanza-ingiunzione di euro 400.000,00 comminata per plurime violazioni della disciplina *privacy*, in ragione della illecita condotta della società nella realizzazione di alcuni parcometri in un comune (cd. parcometri evoluti) che prevedevano l'inserimento della targa del veicolo, in modo da evitare al conducente di dover esporre il tagliando o lo scontrino di pagamento sul cruscotto del veicolo (provv. 22 luglio 2021, n. 293, doc. web

n. 9698597). Il Tribunale ha accolto integralmente gli argomenti difensivi del Garante, confermando la sanzione comminata e disponendo la rifusione, da parte del soccombente, delle spese di giudizio sostenute dal Garante.

Divulgazione di dati sulla salute nell'ambito di una ricerca scientifica

Con sentenza 15 dicembre 2022, n. 2246, il Tribunale di Verona ha respinto il ricorso con il quale un medico, dipendente dell'azienda sanitaria scaligera, aveva richiesto l'annullamento di un provvedimento di ordinanza-ingiunzione con il quale l'Autorità aveva sanzionato il professionista per la violazione degli artt. 5, par. 1, lett. *a*) e *c*), 6 e 9 del RGPD, per aver pubblicato, nell'ambito di un convegno, dati personali e immagini diagnostiche e fotografiche non anonimizzate relative a un paziente, senza il consenso informato dell'interessato e senza l'autorizzazione del titolare del trattamento.

Il Tribunale ha confermato la piena legittimità del provvedimento del Garante, osservando che il ricorrente avrebbe dovuto alternativamente mascherare le informazioni relative al paziente in modo da non renderlo identificabile o acquisire un apposito consenso per il trattamento dei propri dati sensibili in occasione del convegno.

Nella sentenza si osserva in particolare che, con riferimento alla pseudonimizzazione dei dati, erroneamente richiamata dal medico ricorrente al fine di giustificare il trattamento posto in essere, e visto l'art 4 del RGPD, "la data di nascita dell'interessato, nonché le iniziali del nome e del cognome, le numerose immagini ritraenti parti del corpo e le peculiari cicatrici dovute agli interventi subiti, sono tutte informazioni che consentono l'identificazione del paziente senza l'ausilio di informazioni aggiuntive".

I dati sensibili relativi all'interessato sono stati inoltre utilizzati da una persona fisica, in occasione della partecipazione del medico – a titolo personale – ad un convegno a carattere scientifico, per cui è emerso "un utilizzo dei dati ulteriore, non compreso nell'autorizzazione rilasciata inizialmente per iscritto dal paziente. Anche ad ammettere che il consenso sia stato validamente prestato in forma scritta od orale, lo stesso sarebbe stato rilasciato dal paziente all'azienda sanitaria e non potrebbe intendersi esteso anche al trattamento di dati posto in essere dal singolo medico per fini personali". In conclusione a giudizio del Tribunale veneto il mero carattere scientifico dell'evento non basta di per sé a far cadere ogni garanzia in materia di protezione di dati personali e l'utilizzo di dati sensibili relativi a un paziente per ragioni di studio e ricerca deve avvenire pur sempre nel rispetto delle garanzie di cui all'art. 89 del RGPD al fine di assicurare il rispetto del principio della minimizzazione dei dati.

Telefonia

La Corte di cassazione ha accolto il ricorso presentato da una società telefonica sulla incompetenza del Garante a pronunciarsi sul diniego del fornitore di una rete pubblica a comunicare i dati relativi alle utenze intestate al proprio assistito, richiesti per esigenze difensive in sede penale con le modalità previste dall'art. 391-*quater* c.p.p. (richiamato dall'art. 132 del previgente Codice). In particolare, la Corte ha annullato il provvedimento del Garante 14 maggio 2020, n. 85 (doc. web n. 9442587), ritenendo che a fronte della richiesta presentata nel corso delle indagini difensive prevista dall'art. 391-*quater* c.p.p. sono esperibili solo i rimedi ivi richiamati (Cass. n. 21314/2022). La decisione tuttavia non è destinata a produrre effetti per il futuro, riguardando una disposizione del Codice non più vigente.

Trattamento dati in ambito associazionistico

Con sentenza 15 giugno 2022, il Tribunale di Roma ha respinto il ricorso presentato da un'associazione contro il provvedimento del Garante 29 aprile 2021, n. 165 (doc. web n. 9672215) che aveva sanzionato l'ente per avere comunicato tramite *newsletter* a tutti gli associati (oltre mille), dati personali relativi ad un associato in assenza del consenso dell'interessato o di altro legittimo presupposto (art.

6, par. 1, RGPD), nonché in violazione dei principi generali di liceità, correttezza e minimizzazione nel trattamento dei dati rispetto alle finalità perseguite (art. 5, par. 1, lett. *a*) e *c*), del RGPD). Il ricorrente aveva invocato le disposizioni statutarie in materia di trasparenza delle attività degli organi dell'associazione. Il Tribunale, accogliendo le tesi difensive del Garante, ha respinto l'argomento, poiché le finalità di trasparenza potevano ben essere perseguite senza la comunicazione ai circa mille associati, attraverso una *newsletter*, del nominativo del socio.

Con ordinanza n. 34658/2022, la Suprema Corte ha accolto il ricorso del Garante avverso la sentenza del Tribunale di Milano n. 5566/2020 che aveva annullato il provvedimento 26 ottobre 2017, n. 445 (doc. web n. 7323489), con il quale l'Autorità aveva accolto parzialmente il ricorso proposto dall'interessato, ordinando a Google di rimuovere entro venti giorni gli Url oggetto di richiesta anche dalle versioni extraeuropee del motore di ricerca.

La sentenza, nel ribadire i contenuti del diritto all'oblio, inteso come correlato al diritto alla riservatezza nella misura in cui tutela "la pretesa di non veder ulteriormente divulgate notizie, già legittimamente pubblicate, ma ormai superate dal tempo, che ha dissolto l'interesse pubblico alla circolazione dell'informazione", afferma la tutela dell'individuo e della propria identità personale digitale, estendendo la portata territoriale dell'ordine di deindicizzazione oltre i confini europei e accogliendo pienamente le ragioni eccepite dalla difesa del Garante.

Con l'importante pronuncia il Giudice, nel ribadire che "Il diritto all'oblio si correla al diritto alla riservatezza e in questa prospettiva protegge l'interessato nella pretesa; ovvero al diritto all'identità personale, e in questa prospettiva protegge l'esigenza di contestualizzazione e aggiornamento delle informazioni; ovvero, ancora, al diritto alla protezione dei dati personali dell'interessato", ha cassato senza rinvio la decisione del Tribunale di primo grado, che secondo la Suprema Corte non aveva interpretato correttamente il diritto dell'Unione europea.

La Corte, infatti, nel commentare la sentenza della Corte di giustizia, Grande Sezione, 13 maggio 2014, C-131/12, nota come Google Spain o caso Costeja, ha sancito l'ammissibilità di un ordine di deindicizzazione o rimozione extraterritoriale nei confronti del gestore del motore di ricerca (*global delisting o global removal*). La citata sentenza, infatti, ad avviso del giudice, è chiara nello statuire che "Il diritto dell'Unione non impone agli Stati membri di far sì che la persona interessata che si avvalga del diritto alla deindicizzazione possa ottenere il risultato di incidere su tutte le versioni, anche extraeuropee, del motore di ricerca. E tuttavia il diritto dell'Unione neppure vieta agli Stati membri di consentire questo risultato".

L'obiezione mossa dalla società resistente, inerente alla questione di un riconoscimento di una decisione del nostro ordinamento in un diverso ordinamento giuridico, non inciderebbe sulla ammissibilità astratta dell'ordine ma, eventualmente, sulla sua effettiva possibilità di esecuzione e sul riconoscimento della decisione italiana in altri ordinamenti "Secondo questa Corte, non vi è dubbio che il diritto alla protezione dei propri dati personali e il suo fondamento costituzionale non tollerino limitazioni territoriali all'esplicazione della sfera di protezione, tanto più che nella specie tale diritto si sovrappone e si accompagna ai diritti all'identità, alla riservatezza e alla contestualizzazione delle informazioni".

Viene pertanto confermata la difesa del Garante, laddove spiega che "questo ragionamento confonde due piani ben distinti: da un lato, quello della potenziale portata extraterritoriale delle norme e dei provvedimenti nazionali; dall'altro, quello del loro riconoscimento da parte degli Stati esteri nell'esercizio della loro sovranità. Tale sovranità non è certamente compromessa dalla efficacia extraterritoriale del provvedimento del Garante, restando impregiudicata la possibilità per lo Stato

straniero di non riconoscere il provvedimento o della decisione giurisdizionale che lo ha ritenuto legittimo".

Altra casistica

Con ordinanza 17 gennaio 2022, n. 1263, la Suprema Corte ha respinto il ricorso del Garante avverso la sentenza del Tribunale di Palermo n. 3563/2019, che aveva annullato l'ordinanza-ingiunzione di euro 192.000,00 (doc. web n. 4858951) irrogata ad un CTU (per le violazioni di cui agli artt. 161, 162, comma 2-*bis*, e 164-*bis*, comma 2, del Codice, all'epoca vigenti), ritenendo che questi avesse svolto i trattamenti oggetto di sanzione "per ragioni di giustizia" e valutando l'impianto istruttorio su cui si è retta l'accusa mossa nei confronti del CTU affetto da "congenita debolezza", sicché la decisione di merito da parte del Tribunale era insindacabile nel giudizio di legittimità dinnanzi alla Suprema Corte.

Con sentenza 29 aprile 2022, n. 9542, il Tribunale di Milano non ha ritenuto fondata la decisione del Garante (nota 11 settembre 2019) di improcedibilità di un reclamo per litispendenza (in relazione all'avvenuta presentazione di una querela in sede penale) in relazione alla dedotta violazione dell'art. 2-*octies* del Codice da parte di una banca, che poi è stata giudicata effettivamente sussistente, riformando parzialmente il provvedimento opposto, ed ha invece condiviso la decisione del Garante in relazione alla dedotta violazione degli artt. 6 e 7 del RGPD, rigettando la domanda del ricorrente.

20.3. *Il contributo del Garante nei giudizi in materia di protezione dati*

Come si è visto al paragrafo 20.1, l'Autorità giudiziaria deve comunicare al Garante la pendenza di una controversia, trasmettendo copia degli atti introduttivi (art. 10, comma 9, d.lgs. 1° settembre 2011, n. 150, come modificato dall'art. 17, d.lgs. 10 agosto 2018, n. 101). Tale comunicazione consente all'Autorità, "nei casi in cui non sia parte in giudizio", di "presentare osservazioni, da rendere per iscritto o in udienza, sulla controversia in corso con riferimento ai profili relativi alla protezione dei dati personali".

Conformemente agli indirizzi giurisprudenziali e al parere espresso dall'Avvocatura generale dello Stato, il Garante, nei giudizi diversi da quelli direttamente attinenti a pronunce dell'Autorità, limita, in generale, il proprio contributo ai soli casi in cui sorga, o possa sorgere in prosieguo, la necessità di difendere o comunque far valere particolari questioni di diritto.

In 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 sull'evoluzione delle vicende processuali e di ricevere comunicazione in merito agli esiti.

Al riguardo si consideri che la notifica al Garante dei ricorsi in materia di protezione dei dati personali che non riguardano provvedimenti dell'Autorità amplia la casistica di possibile intervento, anche in relazione a questioni di legittimità costituzionale o di compatibilità europea di leggi, anche con riferimento alla CDFUE, nonché alle norme di adeguamento al RGPD, in relazione a disposizioni la cui difesa per conto della Presidenza del Consiglio dei ministri è affidata all'avvocatura erariale. La legittimazione attiva dell'Autorità nei giudizi in cui non è parte ed al potere di intervento al fine di sostenere principi rilevanti nell'applicazione della disciplina in materia di protezione dei dati personali, sembrerebbero potersi desumere anche dall'art. 154-*ter* del Codice, nella parte in cui ora riconosce al Garante la legittimazione ad agire nei confronti del titolare o del responsabile del trattamento *tout court*, senza alcuna qualificazione, "in caso di violazione delle disposizioni in

materia di protezione dei dati personali", quindi anche nei confronti dell'autorità pubblica.

Il medesimo art. 154-*ter* del Codice, peraltro, 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.

21 Le relazioni comunitarie e internazionali

Il 2022 è stato contrassegnato a livello dell'Unione europea da un'intensa attività riguardante le proposte normative relative alla regolamentazione dello spazio digitale. Con riferimento, in particolare, al pacchetto sui servizi digitali e all'euro digitale, il Cepd ha sottolineato con vari documenti (pareri, dichiarazioni, lettere), l'importanza che l'adozione di nuovi strumenti e strategie digitali sia sempre accompagnata da misure idonee a tutelare i diritti fondamentali delle persone.

È proseguita l'attività volta a chiarire l'applicazione e l'interpretazione delle norme del RGPD a beneficio dei titolari e responsabili del trattamento, rafforzando la tutela dei diritti degli interessati.

Il Comitato ha inoltre approfondito la riflessione sulle questioni rilevanti emerse nei primi anni di applicazione dei meccanismi di cooperazione tra le autorità europee introdotti dal RGPD, potenziando la strategia di cooperazione tra autorità.

La drammatica situazione bellica in Ucraina ha avuto importanti ripercussioni soprattutto nell'ambito del Consiglio d'Europa, culminate nella decisione del Comitato dei ministri del 16 marzo 2022 a seguito della quale la Federazione russa ha cessato di essere membro del Consiglio d'Europa. La crisi ucraina ha influito anche sui lavori dei diversi comitati che operano a Strasburgo, tra cui il Comitato consultivo della Convenzione 108. Ciononostante, accanto all'impegno rivolto ad apportare gli aggiustamenti procedurali a seguito dell'uscita della Federazione russa dal Consiglio d'Europa (v. *infra*), è proseguita l'attività del Comitato consultivo, specie con riferimento all'interpretazione e all'applicazione della Convenzione 108 e della sua versione modernizzata nei diversi settori in merito alla quale il Garante ha continuato a svolgere un ruolo particolarmente attivo.

Per altro verso, il progressivo venire meno delle restrizioni imposte per contenere la diffusione da Covid-19 ha consentito un ritorno a riunioni in presenza in relazione ai diversi tavoli cui il Garante partecipa a livello europeo e internazionale. Tali riunioni si sono spesso abbinate ad incontri ibridi o interamente da remoto, ormai entrati nella prassi della cooperazione tra le autorità, che hanno anche quest'anno facilitato una più rapida adozione di un rilevante numero di documenti ed iniziative.

21.1. *La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dei dati*

Nel corso dell'anno si sono svolte 15 riunioni plenarie delle quali tre in presenza e 162 riunioni dei sottogruppi e delle *task force* che si occupano dell'applicazione del Regolamento e della direttiva *law enforcement* nei diversi settori.

È proseguita l'attività del Comitato volta ad armonizzare e chiarire l'interpretazione delle norme-chiave del RGPD attraverso l'elaborazione di specifiche linee guida.

Linee guida sul diritto di accesso

Sono state adottate dal Cepd il 18 gennaio 2022 le linee guida sul diritto di accesso, che analizzano puntualmente le previsioni dell'art. 15 del RGPD, soffermandosi, in particolare, sul contenuto di tale diritto, sulle diverse modalità con cui il titolare può dare riscontro alle richieste dell'interessato, sul rapporto tra il diritto di accedere ai dati e di ottenere copia ai sensi dell'art. 15, par. 3, sul formato

della richiesta di accesso e sulla nozione di richiesta manifestamente infondata o eccessiva prevista dall'art. 12, par. 5. Una volta adottate, le linee guida sono state sottoposte a consultazione pubblica conclusasi l'11 marzo 2022 e l'adozione finale, dopo la revisione del *Board* alla luce dei contributi pervenuti, è prevista per il 2023.

Linee guida in materia di legittimo interesse

Il *Board* ha avviato la stesura di linee guida in materia di legittimo interesse (del titolare o di terzi, cfr. art. 6, par. 1, lett. *f*), del RGPD) per aggiornare il parere 6/2014 del Gruppo Art. 29, alla luce delle novità regolamentari.

Linee guida sul trattamento dei dati relativi ai minori

È altresì proseguita la discussione sull'interpretazione delle previsioni normative del RGPD in materia di minori ai fini della predisposizione di specifiche linee guida, volte ad offrire un quadro di riferimento generale affinché il trattamento dei dati relativi ai minori tenga conto delle loro specifiche vulnerabilità e del principio del superiore interesse dei minori *(best interest of the child)* che permea l'intero complesso del diritto minorile nei Paesi europei e a livello internazionale.

Meccanismo di cooperazione e coerenza – Dichiarazione di Vienna sulla cooperazione

Il 28 e 29 aprile 2022 i vertici di tutte le autorità di protezione dei dati nello Spazio economico europeo (See) si sono riuniti a Vienna per potenziare la cooperazione prevista dal RGPD, nell'ambito del meccanismo di "sportello unico" (OSS) di cui all'art. 60 del RGPD. La dichiarazione finale contempla l'individuazione di casi strategici e il rafforzamento dello scambio di informazioni preliminari alla definizione di singoli casi, nonchè la creazione di strumenti comuni quali un modello per la presentazione dei reclami. Un documento più specifico indica i criteri sostanziali per l'individuazione dei casi strategici unitamente alla procedura per il riconoscimento della natura prioritaria. I menzionati criteri attengono a problematiche ricorrenti o di natura strutturale, all'intersezione con altri ambiti legislativi, al numero elevato di interessati (potenzialmente) coinvolti, all'elevata rischiosità dei trattamenti.

Con lettera indirizzata alla Commissione europea si sono evidenziati alcuni profili procedurali che potrebbero beneficiare di un'ulteriore armonizzazione di rango legislativo a livello UE, al fine di ovviare alle differenze nelle procedure e nelle pratiche amministrative dei diversi Stati membri di possibile impatto negativo sulla cooperazione transfrontaliera. Il Comitato ha in particolare segnalato la necessità di armonizzare la posizione delle parti nel procedimento e segnatamente il diritto del reclamante di stare in giudizio, l'esercizio del diritto di accesso difensivo nel procedimento nonché la definizione di termini univoci per le procedure OSS.

Linee guida sull'applicazione dell'art. 60 del RGPD

Le linee guida 2/2022 elaborate dal Comitato sull'applicazione dell'art. 60 del RGPD, muovono dalla premessa secondo cui lo "sportello unico" configura un processo decisionale consensuale, fondato su uno scambio ampio di informazioni nell'ottica della leale cooperazione che la stessa Corte di giustizia ha evidenziato quale chiave di volta dell'intero sistema (nella causa C-645/19); individuano l'obbligo per l'autorità capofila di presentare un progetto di decisione alle altre autorità interessate e chiariscono le procedure che conducono all'adozione della decisione finale. Da segnalare la "guida rapida" in appendice, che presenta in forma sintetica e tabellare le principali raccomandazioni e indicazioni (buone prassi) sviluppate nel testo delle linee guida.

Linee guida sull'attuazione pratica delle composizioni amichevoli

Le linee guida 6/2022 sull'attuazione pratica delle composizioni amichevoli esaminano, in primo luogo, la composizione amichevole in quanto tale, alla luce dei diversi approcci nazionali, e della sua *ratio* quale meccanismo efficiente e veloce di risoluzione dei reclami, anche attraverso l'indicazione delle casistiche di riferimento nel settore della protezione dei dati ovvero i reclami relativi ai diritti degli interessati, di non particolare complessità, di massima risolvibili attraverso l'intervento dell'autorità di controllo con soddisfazione documentata del reclamante e dimostrazione dell'avvenuta ottemperanza da parte del titolare. In secondo

luogo, analizzano il ricorso a tale strumento nelle procedure di "sportello unico" evidenziando, in particolare, la necessità per l'autorità capofila che tenti una composizione amichevole di rispettare tutti i requisiti applicabili a tali procedure (compresa la necessità di sottoporre alle altre autorità interessate un progetto di decisione a chiusura del procedimento, secondo quanto delineato nelle linee guida relative all'art. 60 di cui sopra). Il documento contiene una *checklist* finale per guidare le autorità nell'individuazione corretta dei presupposti per procedere a una composizione amichevole in presenza di reclami degli interessati, anche in rapporto a trattamenti transfrontalieri.

Cooperazione fra autorità di controllo del See e autorità omologhe di Paesi terzi

Si è provveduto ad elaborare il pacchetto di strumenti (*toolbox*) in vista delle attività di cooperazione internazionale di cui all'art. 50 del RGPD. Si tratta di una serie di clausole-modello da utilizzare per disciplinare, in primo luogo, i trasferimenti di dati personali funzionali ad accordi amministrativi di cooperazione sottoscritti direttamente tra autorità di protezione dei dati del See e autorità omologhe di Paesi terzi (ai sensi dell'art. 46, par. 3, lett. *b*), del RGPD). Le clausole in oggetto possono servire, tuttavia, anche per disciplinare gli aspetti di protezione dati nel quadro di accordi internazionali negoziati dalla Commissione europea con Paesi terzi in materia di *enforcement* (ai sensi dell'art. 46, par. 2, lett. *a*), del RGPD). Il documento ricorda che, nel primo caso, le garanzie e le tutele discendono dagli ordinamenti applicabili, mentre nel secondo caso, dovrebbero trovare fondamento nello stesso accordo internazionale. Nella sostanza tuttavia tali garanzie e tutele sono identiche: diritti degli interessati, periodo di conservazione dei dati, qualità e proporzionalità dei dati, sicurezza e riservatezza, regole sui trasferimenti ulteriori di dati sia fra autorità all'interno dello stesso Paese terzo sia verso autorità di altri Paesi terzi (questi ultimi consentiti solo con l'accordo dell'autorità See e per le stesse finalità di cooperazione), riservatezza e segreto professionale (qualora si verifichi la necessità di prevedere clausole in merito), garanzia di mezzi di ricorso giudiziali per gli interessati nel See in caso di violazioni delle norme.

Decisioni vincolanti ex art. 65 del RGPD

Cinque sono state le decisioni vincolanti adottate dal Comitato nel 2022 nell'ambito della procedura di coerenza prevista dall'art. 65 del RGPD al fine di risolvere contrasti tra l'autorità capofila e le autorità interessate. Sulla natura e gli effetti delle decisioni vincolanti, il 7 dicembre 2022, il Tribunale della UE, con ordinanza, ha dichiarato irricevibile il ricorso T709/21 proposto, ai sensi dell'art. 263 TFUE, da WhatsApp Ireland Ltd per chiedere l'annullamento della decisione vincolante 1/2021 del Comitato del 28 luglio 2021 (v. Relazione 2021, p. 216), sottolineando che la decisione del Comitato non modifica di per sé la situazione giuridica della società ricorrente, configurandosi solo quale atto preparatorio o intermedio di un procedimento che deve concludersi con l'adozione, da parte di un'autorità nazionale di controllo, di una decisione definitiva di cui la società è destinataria e nei confronti della quale il RGPD prevede già una tutela giurisdizionale effettiva. L'ordinanza è stata impugnata dalla società dinanzi alla Corte GUE (caso C-97/23 P).

La prima decisione vincolante adottata nel 2022 (decisione 1/2022) ha riguardato la controversia fra l'Autorità francese (Cnil) e l'Autorità polacca rispetto al progetto di decisione in un procedimento avviato nei confronti di Accor (multinazionale operante nel settore alberghiero, con stabilimento principale in Francia) a seguito di alcuni reclami presentati per la ricezione di comunicazioni indesiderate. Il Comitato ha dato indicazioni alla Cnil di rivedere l'importo della sanzione pecuniaria alla luce degli ulteriori fattori richiamati nelle obiezioni sollevate dall'Autorità polacca e accolte dall'EDPB (quali la necessità di tenere conto del fatturato 2021, a prescindere dalle difficoltà finanziarie del settore di riferimento; il basso livello di dissuasività

della sanzione proposta originariamente nonché ulteriori elementi quali il numero elevato di interessati coinvolti in UE).

Le successive decisioni, adottate nella seconda parte del 2022, hanno riguardato quattro progetti di decisione predisposti dall'Autorità irlandese, in qualità di autorità capofila in merito alla liceità dei trattamenti dei dati effettuati dalla società Meta Platforms Ireland Limited in relazione a servizi Facebook e Instagram e dalla società Whatsapp Ireland Limited in relazione al servizio Whatsapp. In tutte le decisioni il Comitato, accogliendo diverse obiezioni ha indicato all'Autorità irlandese di tenere conto di ulteriori violazioni individuate dalle altre autorità interessate, anche per la commisurazione delle sanzioni comminate (cfr. par. 12.6).

Azione coordinata sull'utilizzo del *cloud* da parte dei soggetti pubblici

Per intensificare la cooperazione volta a garantire l'applicazione e l'attuazione coerente del RGPD, il Comitato ha adottato, il 20 ottobre 2020, un piano (CEF, *Coordinated Enforcement Framework*) volto a fornire un coordinamento per le azioni di *enforcement* che le autorità, su base volontaria, decidono di avviare su uno specifico tema comune di anno in anno (v. Relazione 2020, p. 224).

La prima azione, con la partecipazione di ventidue autorità avviata a febbraio 2022, ha riguardato un centinaio di soggetti pubblici che operano in vari settori (sanità, fisco, istruzione), incluse le Istituzioni europee, le centrali di committenza e i fornitori di servizi Ict della pubblica amministrazione centrale e locale.

L'iniziativa si è sviluppata sulla base di un questionario comune utilizzato da tutte le autorità per raccogliere informazioni comparabili, ed è volta alla predisposizione di *report* nazionali per presentare gli esiti delle attività svolte dalle singole autorità a livello nazionale, redatti sulla base di un modello comune per garantirne una certa omogeneità, e di un *report* comune del Comitato per raccogliere informazioni statistiche su numero e tipologia degli *stakeholder* coinvolti nonchè illustrare i principali aspetti problematici riscontrati nel corso delle attività. Il *report* è atteso per i primi mesi del 2023.

Linee guida sul calcolo delle sanzioni amministrative

Nella riunione del 12 maggio il Cepd ha adottato le nuove linee guida sul calcolo delle sanzioni amministrative, armonizzando la metodologia utilizzata dalle autorità per la protezione dei dati, da articolare in cinque fasi in conformità all'art. 83 del RGPD.

In primo luogo, occorre determinare se un comportamento sanzionabile comporti una o più infrazioni, in quanto infrazioni concomitanti possono condurre a calcoli diversi della sanzione.

Un passo successivo consiste nel considerare tre fattori: 1) il massimo legale applicabile della sanzione; 2) la natura, la gravità e la durata della violazione, nonché le categorie di dati personali e il numero di interessati; 3) il fatturato della società, al fine di garantire una sanzione effettiva, proporzionata e dissuasiva. Questi elementi conducono a un punto di partenza per la determinazione dell'importo della sanzione, dal quale le autorità di controllo possono discostarsene qualora le circostanze lo richiedano.

La fase successiva consiste nell'individuare le circostanze aggravanti e attenuanti legate al comportamento del titolare/responsabile del trattamento.

Dopo la qualificazione di tutti gli elementi pertinenti, occorre individuare il massimo legale della sanzione i cui importi sono stabiliti dall'art. 83, parr. da 4 a 6, del RGPD.

Infine, occorre analizzare se l'importo definitivo soddisfa i requisiti di efficacia, proporzionalità e dissuasione. L'importo finale, di conseguenza, può ancora essere adeguato alle circostanze del caso specifico.

Una volta adottate, le linee guida sono state sottoposte a consultazione pubblica per un periodo di 6 settimane.

Linee guida sul trasferimento dei dati: codici di condotta e certificazioni

Sono state adottate dal Comitato le linee guida che forniscono indicazioni in ordine a finalità, contenuto e requisiti di due nuovi strumenti di trasferimento dei dati introdotti dal Regolamento: codici di condotta (artt. 40, par. 3 e 46, par. 2, lett. *e*), del RGPD) e certificazioni (artt. 42, par. 2 e 46, par. 2, lett. *f*), del RGPD).

Dopo una prima adozione il 7 luglio 2021, le linee guida 4/2021 sui codici di condotta come strumenti per il trasferimento dei dati all'estero sono state approvate con modifiche, il 22 febbraio 2022, alla luce dei contributi pervenuti nella consultazione pubblica.

Al documento originale (v. Relazione 2021, p. 219) sono stati aggiunti una sintesi introduttiva e alcuni diagrammi di flusso relativi alla procedura per l'adozione dei codici e al ruolo dei diversi attori in essa coinvolti. Come chiariscono le linee guida, una volta approvati dall'autorità di controllo competente e ottenuto il riconoscimento della loro validità generale all'interno dell'Unione ai sensi dell'art. 40, par. 9, del RGPD, ai codici possono aderire i titolari o i responsabili del trattamento, non soggetti al RGPD, situati in Paesi terzi (importatori). Essi possono essere utilizzati inoltre, senza necessità di adesione, dai titolari/responsabili del trattamento soggetti al RGPD (vale a dire gli esportatori) per adempiere agli obblighi posti dal Capo V del RGPD in caso di trasferimenti verso tali importatori.

Nel nuovo testo delle linee guida ulteriori chiarimenti sono forniti anche sulle condizioni per il subappalto delle attività dell'organismo di monitoraggio a soggetti che siano stabiliti fuori dell'Unione europea.

Le linee guida 7/2022 sulle certificazioni come strumenti di trasferimento dei dati all'estero, adottate il 30 giugno 2022, sono state sottoposte a consultazione pubblica; l'approvazione definitiva è prevista nei primi mesi del 2023.

Considerato che l'EDPB ha già adottato linee guida sulle certificazioni e l'accreditamento degli organismi di certificazione ai sensi del RGPD, le menzionate linee guida 7/2022, composte da quattro parti e da un allegato, si concentrano sugli aspetti specifici della certificazione come strumento per i trasferimenti.

La prima parte concerne lo scopo delle linee guida, gli attori coinvolti e il loro ruolo (in particolare, l'importatore nel Paese terzo che riceve una certificazione e l'esportatore che se ne avvale), l'ambito, l'oggetto e il processo di adozione della certificazione come strumento per i trasferimenti.

La seconda parte fornisce indicazioni in ordine ai requisiti di accreditamento degli organismi di certificazione. In particolare, tenuto conto che requisiti contenuti nelle linee guida 4/2018 del Comitato e nell'ISO 17065 sono sufficientemente generali da coprire anche quelli necessari per l'accreditamento degli organismi di certificazione che rilasciano certificazioni come strumento per i trasferimenti, le linee guida 7/2022 si limitano a fornire pochi, ulteriori dettagli.

La terza parte precisa i criteri di certificazione specifici da includere nel meccanismo di certificazione ovvero la valutazione della legislazione dei Paesi terzi, gli obblighi generali degli esportatori e degli importatori, le norme in materia di trasferimenti successivi, i diritti dei terzi beneficiari e i mezzi di tutela esercitabili, le misure da adottare per le situazioni in cui la legislazione e le prassi nazionali impediscono il rispetto degli impegni assunti dall'importatore nell'ambito della certificazione e nei casi di richieste di accesso ai dati da parte delle autorità di Paesi terzi.

La quarta parte attiene agli impegni vincolanti e azionabili richiesti all'importatore.

Un allegato alle linee guida contiene alcuni esempi di misure supplementari in linea con quelle elencate nell'all. II alle raccomandazioni 1/2020 relative all'utilizzo di una certificazione come strumento per i trasferimenti.

Nel corso del 2022 il Comitato ha lavorato sulla revisione delle linee guida 5/2021 sottoposte a consultazione pubblica fino a gennaio 2022, concernenti l'interazione tra l'ambito di applicazione territoriale del RGPD (art. 3) e le disposizioni sui trasferimenti internazionali di cui al Capo V. Sessantadue sono stati i contributi ricevuti da parte di organizzazioni non governative, studiosi, società, quattordici dei quali stabiliti in Paesi terzi. Il Comitato ha inteso fornire maggiori chiarimenti in merito ai casi in cui, pur in assenza di un trasferimento dei dati ad altro soggetto fuori dall'Unione europea, il titolare del trattamento o il responsabile che tratti i dati al di fuori del See deve adottare importanti misure di tutela: è stato in particolare chiarito che i titolari e/o i responsabili del trattamento i cui trattamenti sono soggetti al RGPD sono responsabili delle loro attività di trattamento, indipendentemente dal luogo in cui hanno luogo e che il trattamento in Paesi terzi può comportare rischi maggiori (anche in relazione a un accesso sproporzionato ai dati da parte di soggetti pubblici di tali Paesi) che devono essere identificati e affrontati affinché il trattamento sia lecito ai sensi del RGPD. Il nuovo testo delle linee guida è atteso per i primi mesi del 2023.

Linee guida sull'*interplay* tra articolo 3 e capo V del RGPD

Per quanto riguarda le regole vincolanti di impresa (*Binding corporate rules*, di seguito Bcr), per il trasferimento dei dati all'interno di un gruppo imprenditoriale o di un gruppo di imprese che svolgono un'attività economica comune, sono state adottate, il 17 novembre 2022, le raccomandazioni 1/2022 sulle Bcr per titolari del trattamento, che sostituiscono il documento di lavoro WP 256, rev. 01 (v. Relazione 2017, p. 167) in particolare, ampliando le garanzie previste, anche alla luce di quelle introdotte nelle nuove clausole contrattuali standard, con riferimento alle richieste di accesso da parte di autorità pubbliche di Paesi terzi. Una sezione iniziale contiene anche il modello per presentare la richiesta di approvazione delle Bcr all'autorità capofila. Il documento è stato sottoposto a consultazione pubblica e l'approvazione definitiva dovrebbe aversi entro il 2023.

Bcr e raccomandazioni 1/2022

Sempre in tema di regole vincolanti d'impresa, nel 2022 sono state diciannove (come nel 2021) le Bcr approvate, dalle competenti autorità di protezione dei dati (cd. *Bcr Lead* individuate sulla scorta dei criteri indicati nel WP 263 rev. 01: v. Relazione 2018, p. 190), previo parere del Comitato. Tredici pareri riguardano Bcr per titolari e sei Bcr per responsabili. Con i pareri, così come con le conseguenti decisioni di approvazione delle Bcr, il Comitato accerta che le garanzie in esse contenute offrano un livello adeguato di tutela alla luce degli elementi richiesti dall'art. 47 del RGPD, ma è necessario che ciascuna impresa appartenente al gruppo interessato verifichi di poter rispettare le garanzie ivi previste tenuto conto delle specificità di ciascun trasferimento e del Paese terzo in cui è stabilita la società del gruppo che agisce in qualità di importatore. Ove infatti il quadro normativo applicabile non consenta all'importatore di rispettare gli impegni assunti con l'adesione alle Bcr, l'esportatore dovrà – come nel caso di ogni altro tipo di strumento per il trasferimento – porre in essere misure supplementari che gli consentano di rispettare tali impegni (v., al riguardo, *supra*, le raccomandazioni 1/2020) o astenersi dal trasferire i dati.

A fine 2022, il Comitato ha iniziato a lavorare sul parere relativo al progetto di decisione sull'adeguatezza del "Quadro sulla *privacy* dei dati UE-USA" (EU-US *Data Protection Framework*, di seguito anche DPF UE-USA), presentato dalla Commissione europea il 13 dicembre 2022. Il nuovo quadro transatlantico per la tutela dei dati trasferiti negli USA era stato preannunciato il 25 marzo 2022, sulla base di un accordo politico di principio tra la Commissione e gli Stati Uniti ed era stato accolto con favore nella dichiarazione 1/2022 con la quale, tuttavia, il Comitato richiamava l'attenzione sulla necessità di adottare misure idonee a superare le obiezioni sollevate dalla CGUE nella decisione Schrems II del luglio 2020 in

Il nuovo *Data Protection Framework* UE-USA

merito alle (non adeguate) garanzie previste dal precedente accordo EU-US *Privacy Shield* (v. Relazione 2020, p. 226).

Il DPF UE-USA è un sistema di autocertificazione attraverso il quale le organizzazioni statunitensi aderenti si impegnano a rispettare una serie di principi sulla *privacy* – i cd. *Data Privacy Framework* UE-USA *Principles* (all. I al progetto di decisione) – emanati dal Dipartimento del commercio degli Stati Uniti. Una volta adottato (sentito cioè il Comitato e portata a termine la procedura di cui all'art. 5 del regolamento (UE) 182/2011 che prevede il via libera da parte di un comitato composto da rappresentanti degli Stati membri dell'UE e fermo restando il diritto di controllo del Parlamento europeo), la decisione di adeguatezza consentirà alle imprese statunitensi aderenti di ricevere dati personali dall'Unione europea senza la necessità di garanzie ulteriori (cfr. art. 45 del RGPD).

La nuova decisione di adeguatezza si basa su un'analisi, da un lato, delle norme relative alle garanzie di protezione dei dati che devono essere rispettate dagli importatori che aderiscono al sistema di autocertificazione DPF UE-USA e, dall'altro, delle limitazioni e garanzie in materia di accesso ai dati personali trasferiti dall'UE da parte delle autorità pubbliche statunitensi, in particolare per finalità di *law enforcement* e di sicurezza nazionale. Novità di maggior peso sono individuabili proprio in ordine a siffatte limitazioni e garanzie, considerate le modifiche introdotte dall'*Executive Order* (EO) n. 14086 adottato dal Presidente Biden, il 7 ottobre 2022, e funzionali a "Migliorare le salvaguardie per l'attività di *signal intelligence* statunitense". L'EO è volto a rispondere alle due principali obiezioni della CGUE avanzate nel caso Schrems II (ossia, possibilità di accesso indiscriminato ai dati trasferiti dall'UE e mancanza di una tutela giurisdizionale effettiva per gli interessati in tali casi) attraverso l'introduzione di nuove garanzie, l'imposizione di limitazioni all'accesso da parte delle agenzie di *intelligence* statunitensi ai dati trasferiti dall'UE e l'istituzione di un meccanismo di ricorso, con caratteristiche di indipendenza e imparzialità, per gestire e risolvere i reclami di individui i cui dati siano stati trasferiti in USA dall'UE, anche mediante la creazione di un "Tribunale di revisione della protezione dati". Il parere del Comitato è atteso nei primi mesi del 2023.

Requisiti per l'accreditamento degli organismi di monitoraggio di codici di condotta

Anche nel 2022 il Comitato ha garantito un approccio uniforme tra le autorità di protezione dei dati nella definizione ed applicazione dei requisiti di accreditamento per gli organismi di monitoraggio dei codici di condotta. Il RGPD non fissa un unico insieme di requisiti per l'accreditamento di tali organismi, bensì demanda all'autorità di controllo competente la redazione dei requisiti per l'accreditamento degli organismi di monitoraggio sulla base dell'art. 41, par. 2, del RGPD. Questi ultimi sono quindi adottati da ciascuna autorità di controllo competente in linea con il parere espresso dal Cepd, in ottemperanza al meccanismo di coerenza. Nel corso del 2022, il Comitato si è espresso in particolare sui progetti dei requisiti di accreditamento presentati dall'Autorità di controllo bulgara (parere 14/2022), lussemburghese (parere 15/2022) e slovena (parere 16/2022)

Requisiti per l'accreditamento degli organismi di certificazione

Altrettanto importante è stata l'attività del Cepd volta ad assicurare la coerenza nell'applicazione del RGPD con riferimento alla definizione dei requisiti aggiuntivi di accreditamento degli organismi di certificazione da parte delle autorità di controllo competenti ai sensi dell'art. 43, par. 3, del RGPD (cfr. le linee guida del Cepd 4/2018 sull'accreditamento degli organismi di certificazione). Nel 2022 il Comitato ha reso il parere previsto dall'art. 64, par. 1, lett. *c*), del RGPD in ordine ai progetti di requisiti aggiuntivi per l'accreditamento degli organismi di certificazione predisposti dalle Autorità di controllo della Polonia (parere 11/2022), della Francia (parere 12/2022) e della Bulgaria (parere 13/2022).

Secondo il RGPD, lo scopo principale dei meccanismi di certificazione della protezione dei dati è quello di aiutare i titolari e i responsabili che ottengano tale certificazione a dimostrare la conformità del trattamento al RGPD. In tale ambito il 1° febbraio 2022, il Cepd ha adottato per la prima volta un parere sui criteri per uno schema di certificazione della protezione dei dati a livello nazionale (parere 1/2022 sul GDPR-CARPA, meccanismo di certificazione sviluppato dall'Autorità di controllo del Lussemburgo). Lo schema, applicabile sia ai titolari che ai responsabili del trattamento, è volto a dimostrare la conformità delle attività di trattamento coperte dalla certificazione al complesso delle regole e dei principi RGPD e comprende criteri relativi alla *governance* della protezione dei dati. Il parere del Comitato, reso ai sensi dell'art. 64 del RGPD, mira a garantire la coerenza e la corretta applicazione dei criteri di certificazione tra le diverse autorità di controllo nel See. A tal fine, il Cepd ha indicato una serie di modifiche al progetto di criteri di certificazione ritenute necessarie per assicurare un'applicazione coerente del RGPD. A seguito dell'approvazione dei criteri da parte dell'Autorità di controllo lussemburghese, aziende, autorità pubbliche, associazioni e altre organizzazioni con sede in Lussemburgo hanno la possibilità di dimostrare che le loro attività di trattamento dei dati sono conformi al RGPD.

Primi meccanismi di certificazione della protezione dati a livello nazionale

Il 13 settembre 2022 il Cepd ha reso un altro parere, in conformità al meccanismo di coerenza, sui criteri di un secondo sistema di certificazione a livello nazionale: il meccanismo di certificazione *European Privacy Seal* (EuroPriSe) rivolto ai responsabili del trattamento e presentato al Comitato dall'Autorità di protezione dei dati tedesca del Nord Reno Westfalia (parere 25/2022). Al fine di soddisfare i requisiti imposti dall'art. 42 del RGPD e la coerente applicazione dei criteri di certificazione nel See, il Cepd ha individuato nel parere specifiche modifiche da apportare.

Dopo che l'Autorità lussemburghese e quella del Nord Reno Westfalia avranno approvato, secondo le rispettive competenze, i criteri di certificazione nazionali sopra indicati, i relativi schemi saranno aggiunti al registro dei meccanismi di certificazione e dei sigilli di protezione dei dati del Comitato in conformità all'art. 42(8) del RGPD.

Il 10 ottobre con parere 28/2022 reso ai sensi dell'art. 64(2) del RGPD, il Cepd si è pronunciato sui criteri di certificazione *Europrivacy* presentati dall'Autorità di controllo del Lussemburgo come certificazione comune europea. Il meccanismo di certificazione *Europrivacy* è il primo sigillo europeo per la protezione dei dati (*European Data Protection Seal*) approvato dal Comitato con validità in tutti gli Stati membri dell'UE. Esso si rivolge a un'ampia gamma di operazioni di trattamento in vari settori eseguite sia da titolari che da responsabili del trattamento, consentendo a questi ultimi, anche in Paesi diversi, di dimostrare di aver raggiunto lo stesso livello di conformità al RGPD per operazioni di trattamento simili. Lo schema include altresì criteri specifici che lo rendono in parte modulabile e applicabile a taluni specifici trattamenti o settori di attività.

Il primo sigillo europeo per la protezione dei dati

È proseguita l'attività del Comitato anche con riferimento all'applicazione dei principi di protezione dei dati nel settore finanziario, attraverso uno specifico sottogruppo (*Financial Matters*) il cui coordinamento è affidato al Garante.

Affari finanziari

Uno dei punti cardine del lavoro del *Board* in materia finanziaria ha riguardato l'euro digitale.

La discussione, avviata lo scorso anno (v. Relazione 2021, p. 225) è proseguita anche attraverso l'interlocuzione con rappresentanti della Banca centrale europea (Bce).

Il Cepd ha fornito il suo contributo (adottato dalla plenaria il 14 giugno 2022) alla consultazione pubblica su alcune scelte strategiche che la Commissione europea potrebbe effettuare in materia di euro digitale, mentre nella dichiarazione del 10

ottobre 2022 ha messo in evidenza che un livello elevato di tutela della vita privata e protezione dei dati, adeguato alle aspettative espresse dai cittadini, è fondamentale per garantire la fiducia degli europei nell'euro digitale. Per tali ragioni è essenziale che fin dalla progettazione la nuova moneta digitale risponda ad adeguati parametri che mettano al riparo i cittadini da forme di controllo e sorveglianza. La dichiarazione sviluppa alcune raccomandazioni chiave quali: a) la necessità di evitare la convalida delle transazioni da parte di terze parti e di ridurne il monitoraggio; b) la necessità di fissare una soglia nell'ammontare delle transazioni al di sotto delle quali la transazione non dovrebbe essere tracciata, rispecchiando il rischio ridotto che tali movimenti comportano in termini di lotta al riciclaggio e al finanziamento del terrorismo; c) la necessità che a livello UE sia predisposto uno strumento normativo specifico che disciplini in modo preciso i profili di protezione dati (rispetto al quale il Cepd ha già manifestato la propria disponibilità a fornire un proprio parere); d) l'opportunità di favorire un dibattito pubblico sui vantaggi e sui rischi dell'euro digitale traendo beneficio dai contributi forniti dalla società civile e dal mondo accademico.

Antiriciclaggio e lotta al finanziamento del terrorismo

Un'altra tematica che ha continuato ad impegnare il Comitato è stata quella della lotta al riciclaggio e al finanziamento del terrorismo (AML/CFT) oggetto di uno specifico piano di azione della Commissione europea (7 maggio 2020) e di un pacchetto di quattro proposte legislative pubblicate dalla Commissione il 20 luglio 2021.

In continuità con il lavoro precedente (v. Relazione 2021, p. 225), il Cepd, il 12 maggio 2022, ha adottato la lettera alla Commissione, al Parlamento e al Consiglio al fine di fornire indicazioni specifiche sui diversi punti deboli delle proposte e sulle modifiche necessarie a garantirne la coerenza con i principi del RGPD. Muovendo dal presupposto che il rispetto dei principi di minimizzazione, necessità e proporzionalità è dovuto in base alle norme del Regolamento per tutelare i diritti delle persone e contribuisce all'efficienza dei sistemi AML/CFT, la lettera suggerisce specifiche modifiche alle proposte normative, in particolare con riferimento ai trattamenti delle categorie speciali di dati e di quelli giudiziari, rispettivamente previsti dagli artt. 9 e 10 del RGPD. Si sofferma inoltre sulla opportunità di introdurre specifiche norme per garantire che le fonti utilizzate dai soggetti tenuti ad adempiere agli obblighi di antiriciclaggio e lotta al finanziamento del terrorismo siano accurate e affidabili e che i soggetti obbligati siano tenuti a documentarne la valutazione dell'affidabilità e dell'accuratezza.

Foreign Account Tax Compliance Act

Sempre in ambito finanziario è proseguita l'attività riguardo agli scambi automatizzati tra Stati a fini fiscali, in particolare con riferimento agli accordi intergovernativi che implementano la normativa statunitense antievasione fiscale FATCA (*Foreign Account. Tax Compliance Act*). In base all'art. 70 RGPD, che affida al Cepd il compito di garantire un'applicazione coerente del Regolamento, e considerata l'esistenza di aspetti di protezione dei dati comuni ai diversi Stati membri relativi all'applicazione di FATCA, le autorità di protezione dati UE hanno lavorato insieme per individuare le questioni che potrebbero essere indirizzate alle rispettive autorità nazionali competenti per verificare la coerenza dei rispettivi accordi intergovernativi con i principi del Regolamento, come ricordato nelle due lettere adottate dal Comitato in data 4 novembre 2022 rivolte, rispettivamente, all'europarlamentare Sophie in't Veld e all'Associazione dei cd. *Accidental Americans*.

Il Comitato ha altresì rivisto alcuni documenti precedentemente adottati per assicurarne la coerenza con linee guida precedentemente adottate e con il RGDP.

Linee guida sulla violazione dei dati (*data breach*)

Le linee guida sulla violazione dei dati (*data breach*) – adottate nel febbraio 2018 dal Gruppo Art. 29 – sono state riviste e convertite in linee guida del Cepd (linee guida 9/2022, adottate il 10 ottobre 2022). Esse chiariscono in particolare che il meccanismo di cooperazione e coerenza del RGPD si applica solo ai titolari del trattamento con uno o più stabilimenti nell'UE mentre, se la società non ha

uno stabilimento nell'UE, la semplice presenza di un rappresentante in uno Stato membro non è sufficiente per beneficiare dello "sportello unico". In caso di *data breach*, i titolari del trattamento che non hanno una sede nell'UE dovranno quindi confrontarsi con le autorità di controllo locali dello Stato membro in cui operano, tramite i rispettivi rappresentanti locali.

Linee guida per l'individuazione dell'autorità capofila

È stato altresì rivisto il testo delle linee guida per l'individuazione dell'autorità capofila al fine di assicurare piena coerenza con le più recenti linee guida del Comitato su titolare e responsabile adottate nella loro versione definitiva il 7 luglio 2021. La nuova versione delle linee guida 8/2022, adottata il 10 ottobre 2022, ha chiarito che il potere decisionale dei contitolari del trattamento non comprende la determinazione dell'autorità di controllo competente ai sensi degli artt. 55 e 56 RGPD o la capacità di tali autorità di esercitare i propri compiti e poteri come descritto negli artt. 57 e 58 e che lo stabilimento principale di un titolare del trattamento non può essere considerato lo stabilimento principale del contitolare del trattamento. Pertanto, i contitolari del trattamento non possono designare (tra gli stabilimenti in cui vengono prese le decisioni sulle finalità e sui mezzi del trattamento) uno stabilimento principale comune per entrambi i contitolari.

La versione emendata è stata sottoposta a consultazione pubblica conclusasi il 21 dicembre 2022 alla quale seguirà la pubblicazione della versione definitiva alla luce dei contributi ricevuti.

Linee guida sui *dark patterns* nelle piattaforme *social media*

Le linee guida 3/2022, adottate dal Comitato il 14 marzo 2022, offrono raccomandazioni pratiche ai progettisti e agli utenti delle piattaforme di *social media* per valutare ed evitare i cosiddetti *dark patterns* (modelli oscuri), tecniche sleali che inducono gli utenti a compiere azioni indesiderate e ad assumere decisioni potenzialmente dannose in merito al trattamento dei loro dati personali. Il documento contiene una lista non esaustiva di pratiche volte ad influenzare il comportamento degli utenti ostacolandone la capacità di proteggere efficacemente i propri dati personali e richiede che i titolari responsabilmente verifichino la conformità con il regolamento di ciascuna pratica implicante il trattamento dei dati relativi agli utenti.

Il documento, strutturato sulla falsariga del "ciclo di vita" di un *account* utente di *social media*, presenta altresì le migliori pratiche per i diversi casi d'uso fornendo raccomandazioni specifiche per la progettazione di interfacce utente che facilitino l'efficace attuazione del RGPD.

Parere su proposta di regolamento per prevenire e combattere gli abusi sessuali sui minori

Il 28 luglio 2022 è stato adottato il parere congiunto del Cepd e del Gepd sulla proposta di regolamento del Parlamento europeo e del Consiglio recante norme per prevenire e combattere gli abusi sessuali sui minori. La proposta impone specifici obblighi ai fornitori di servizi di *hosting* o di comunicazione interpersonale (e altri servizi) per quanto riguarda l'individuazione, la segnalazione, la rimozione e il blocco di materiale pedopornografico *online* noto e nuovo, nonché l'adescamento di minori. Prevede inoltre l'istituzione di una nuova agenzia decentralizzata dell'UE e di una rete di autorità nazionali di coordinamento per le questioni relative agli abusi sessuali sui minori incaricate dell'attuazione della proposta. Nel parere viene sottolineato che la proposta solleva diverse importanti preoccupazioni in materia di protezione dati e vengono pertanto invitati i co-legislatori in particolare, a garantire che i previsti obblighi di rilevamento di materiale pedopornografico *online* noto e nuovo, nonché dell'adescamento di minori soddisfino i principi di necessità e di proporzionalità e non determinino l'indebolimento o il degrado della crittografia.

Parere sullo Spazio europeo dei dati sanitari

Il 12 luglio 2022 è stato adottato il parere congiunto 03/2022 Cepd/Gepd sulla proposta della Commissione europea per lo Spazio europeo dei dati sanitari (EHDS), tesa a favorire l'istituzione di un'unione sanitaria europea ed a consentire all'UE di sfruttare appieno il potenziale offerto dallo scambio, uso e riutilizzo sicuro e protetto

21

dei dati sanitari elettronici. Il parere 3/2022 accoglie con favore lo sforzo di rafforzare i diritti delle persone rispetto ai propri dati sanitari elettronici ed esorta il Parlamento europeo e il Consiglio a garantire la coerenza delle nuove regole con il RGPD, per evitare il rischio di incertezze giuridiche, specie in relazione ai diritti degli interessati rispetto all'uso primario dei dati e al rischio di opacità in merito alla distinzione tra il diritto alla salute e alla ricerca e quello alla protezione dei dati personali. Con riguardo all'uso secondario dei dati sanitari elettronici sottolinea che i dati sanitari generati dalle *app* per il benessere e da altre applicazioni digitali per la salute (che producono un'enorme quantità di dati non sempre della stessa qualità di quelli generati ad esempio dai dispositivi medici) dovrebbero essere esclusi dall'ambito di applicazione della proposta e raccomanda di circoscrivere meglio le finalità perseguibili in tale ambito, ammettendo solo quelle che presentano un collegamento sufficiente con la salute pubblica e la sicurezza sociale. Il parere riconosce che l'infrastruttura per lo scambio di dati sanitari elettronici prevista nella proposta EHDS non è in alcun modo diretta a creare una banca dati centralizzata di dati sanitari in UE, mirando, invece, a facilitare lo scambio di tali dati da banche dati decentralizzate. A causa della grande quantità di dati sanitari elettronici che verrebbero trattati, della loro natura sensibile, del rischio di accessi illeciti da parte di autorità governative in Paesi terzi e della necessità di garantire l'esercizio di una supervisione efficace da parte delle autorità di protezione dei dati, il Parlamento europeo e il Consiglio vengono invitati ad integrare la proposta con l'obbligo di conservazione dei dati sanitari elettronici in UE, fatti salvi ulteriori trasferimenti in conformità al Capo V del RGPD.

Parere sulla proroga delle misure in materia di certificati Covid-19

Con il parere congiunto 1/2022 adottato il 12 marzo 2022, il Cepd e il Gepd si sono pronunciati sulle due proposte di regolamento della Commissione europea che modificano rispettivamente il reg. (UE) 2021/953 relativo a un quadro per il rilascio, la verifica e l'accettazione di certificati Covid-19 di vaccinazione, test e guarigione interoperabili e il reg. (UE) 2021/954 relativo a un quadro per il rilascio, la verifica e l'accettazione dei certificati Covid-19 di vaccinazione, test e recupero interoperabili per quanto riguarda i cittadini di Paesi terzi che soggiornano o risiedono legalmente nei territori degli Stati membri.

Le proposte mirano a prorogare di 12 mesi l'applicazione del reg. 2021/953 sul certificato Covid digitale UE e a prolungare allo stesso tempo il potere della Commissione di adottare atti delegati ai sensi dello stesso regolamento. Tali proposte, in particolare, ampliano la definizione di test Sars-CoV-2 per includere i test immunologici eseguiti in laboratorio e non solo i test antigenici rapidi; chiariscono che i certificati di vaccinazione devono contenere il numero di dosi somministrate, indipendentemente dallo Stato membro in cui sono state somministrate, per garantire dati accurati; includono i certificati di vaccinazione rilasciati per un vaccino Covid-19 in fase di sperimentazione clinica tra i certificati che possono essere accettati dagli Stati membri; correggono un erroneo rimando all'art. 13(2) del reg. (UE) 2021/953. Il parere sottolinea l'assenza di una adeguata valutazione di impatto volta a dimostrare chiaramente la necessità e la proporzionalità delle misure adottate e sottolinea la necessità di una periodica valutazione in merito a quali misure rimangano efficaci, necessarie e proporzionate rispetto alla finalità di contenimento della pandemia, per garantire la piena applicazione dell'art. 5 del RGPD.

Parere sulla proposta di regolamento relativa all'accesso e uso equo dei dati

Il 4 maggio 2022 il Cepd e il Gepd hanno reso un parere congiunto (02/2022) sulla proposta di regolamento recante norme armonizzate in materia di accesso e uso equo dei dati (cd. *Data Act*). La proposta, pilastro fondamentale della strategia europea dei dati, si propone di creare un quadro unitario di regole per facilitare l'accesso e l'utilizzo dei dati da parte di consumatori e imprese, in particolare quelli (personali e non) derivanti dall'utilizzo di oggetti connessi (internet delle cose) e dei servizi ad

essi correlati, quali i dispositivi medici impiantabili e gli assistenti vocali virtuali. Il *Data Act* mira altresì a rafforzare il diritto alla portabilità dei dati estendendolo ai dati non personali e agli utenti di un dispositivo connesso o servizio correlato, siano essi persone fisiche o giuridiche, in qualità di proprietari, affittuari o noleggiatori degli stessi. Al contempo, la proposta introduce l'obbligo, in capo ai produttori/fornitori di tali prodotti e servizi, di rendere accessibili agli utenti i dati derivanti dai prodotti e servizi in questione, nonché trasferirli a terzi, su richiesta degli utenti, per l'offerta di ulteriori servizi (compresi quelli di intermediazione dei dati previsti dal cd. *Data Governance Act*, ma con l'esclusione dei *gatekeepers* ai sensi del cd. *Data Markets Act*). Il *Data Act* introduce inoltre la possibilità per gli enti del settore pubblico, istituzioni, agenzie o organismi dell'UE di accedere e utilizzare i dati detenuti dal settore privato, in determinate situazioni di eccezionale necessità, per lo svolgimento di compiti di interesse pubblico. Ed infine, detta una serie di condizioni e misure per facilitare il passaggio tra diversi servizi *cloud*, prevenire il trasferimento illegale di dati (non personali) al di fuori dell'UE e incentivare lo sviluppo di standard di interoperabilità dei dati.

Nel parere congiunto il Cepd e il Gepd accolgono con favore gli sforzi compiuti per garantire che il *Data Act* non incida sull'attuale quadro normativo di protezione dei dati. Allo stesso tempo, poiché esso si applicherebbe anche a dati personali altamente sensibili, come quelli sulla salute o i dati biometrici, raccomandano, tra l'altro, di prevedere limitazioni o restrizioni all'uso dei dati generati dall'uso di un prodotto o servizio da parte di soggetti diversi dagli interessati, in particolare laddove i dati in questione possano consentire di trarre conclusioni precise riguardanti la vita privata degli stessi o comportino altrimenti rischi elevati per i diritti e le libertà degli interessati. Chiare limitazioni andrebbero introdotte anche per quanto riguarda l'uso dei dati a fini di *marketing* diretto o pubblicità; monitoraggio dei dipendenti; calcolo o modifica di premi assicurativi; *credit scoring*. Inoltre, i prodotti dovrebbero essere progettati in maniera da offrire agli interessati la possibilità di utilizzare i dispositivi in modo anonimo o nel modo meno intrusivo possibile per la vita privata e dovrebbero essere previste ulteriori limitazioni all'uso dei dati per proteggere interessati vulnerabili, in particolare i minori.

Circa la legittimità, la necessità e la proporzionalità dell'obbligo per il settore privato di mettere i dati a disposizione degli enti del settore pubblico degli Stati membri e delle istituzioni, agenzie e organismi dell'UE in caso di "necessità eccezionale" il documento sottolinea che qualsiasi limitazione del diritto alla protezione dei dati personali richiede una base giuridica adeguatamente accessibile e prevedibile la quale dovrebbe definire la portata e le modalità di esercizio delle prerogative esercitabili dagli enti pubblici ed essere accompagnata da garanzie volte a tutelare gli interessati da interferenze arbitrarie. Di conseguenza, il Cepd e il Gepd esortano il Parlamento europeo e il Consiglio a definire in modo più stringente le ipotesi di emergenza o di "necessità eccezionale" e ad individuare in modo più rigoroso gli enti del settore pubblico nazionale e le agenzie e gli organismi dell'UE legittimati a richiedere i dati al settore privato.

Il parere accoglie invece con favore la designazione delle autorità di controllo per la protezione dei dati come autorità competenti responsabili per il monitoraggio dell'applicazione del *Data Act* e chiede altresì al Parlamento europeo e al Consiglio di designare le medesime come autorità di coordinamento competenti.

Linee guida sul riconoscimento facciale nel settore delle attività di polizia e giudiziarie

Nelle linee guida 5/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di polizia e giudiziarie adottate il 12 maggio 2022 il Comitato rinnova la richiesta di vietare la tecnologia di riconoscimento facciale in determinate circostanze in considerazione dei seri rischi per i diritti e le libertà individuali posti dal trattamento di dati biometrici che tale tecnologia comporta. Il Cepd ritiene, in

particolare, che andrebbero vietati: l'identificazione biometrica a distanza di individui in spazi accessibili al pubblico; i sistemi di riconoscimento facciale che classificano gli individui su base biometrica in gruppi con riferimento all'etnia, al genere, nonché all'orientamento politico o sessuale o ad altri motivi di discriminazione; il riconoscimento facciale o tecnologie simili per dedurre le emozioni di una persona; il trattamento di dati personali per attività di polizia e giudiziarie fondato su banche dati contenenti raccolte su larga scala di dati personali (ad es. ottenute attraverso tecniche di web *scraping* di fotografie e immagini facciali accessibili *online*). Le linee guida sono accompagnate da tre allegati che intendono rispettivamente: aiutare a classificare la gravità dell'interferenza con i diritti fondamentali prodotta dai sistemi basati sull'uso di tali tecnologie in diversi ambiti; aiutare le autorità di contrasto a gestire un sistema di tecnologie di riconoscimento facciale garantendo il rispetto dei diritti fondamentali e dei principi di protezione dati; fornire indicazioni pratiche anche sugli aspetti rilevanti da considerare in relazione ad alcuni potenziali scenari e casi concreti di applicazione delle tecniche di riconoscimento facciale.

Secondo Protocollo addizionale alla Convenzione di Budapest

Il 22 febbraio 2022 il Cepd ha adottato un parere richiesto dalla Commissione per le libertà civili, la giustizia e gli affari interni (LIBE) del Parlamento europeo in merito al secondo Protocollo aggiuntivo alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest), anche alla luce delle due proposte di decisioni del Consiglio dell'UE, avanzate dalla Commissione europea, che autorizzano gli Stati membri a firmare e ratificare il Protocollo. Il Protocollo mira a rafforzare la cooperazione transfrontaliera e detta regole relative all'esibizione di prove elettroniche nell'ambito di indagini o procedimenti penali. Il Cepd ricorda al riguardo che il livello di protezione dei dati personali trasferiti in Paesi terzi sulla base delle regole di cooperazione previste dal Protocollo deve essere sostanzialmente equivalente al livello di protezione dei dati nell'UE. Il Comitato fa inoltre riferimento al parere reso dal Gepd il 20 gennaio 2022 ai sensi del reg. (UE) 2018/1725 sulle due proposte della Commissione e ne evidenzia alcuni punti cruciali. In particolare il Cepd accoglie con favore le salvaguardie, incluse nel Protocollo, relative alla protezione dei dati personali e al controllo della sua attuazione, ma si rammarica, tra l'altro, che questo non assicuri, come regola generale, che le informazioni alle persone che esercitano il diritto di accesso ai dati personali siano fornite gratuitamente.

Dichiarazione sull'uso dei dati PNR alla luce della pronuncia della Corte di giustizia

La dichiarazione 5/2022 del Cepd riguarda la recente sentenza resa dalla CGUE in C-817/19, relativa all'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, individuazione, indagine e perseguimento di reati di terrorismo e reati gravi, ai sensi della direttiva PNR 2016/681. Il 21 giugno 2022, su rinvio della Corte costituzionale belga, la CGUE pur non ritenendo invalida la direttiva, ha stabilito che, al fine di garantire il rispetto della Carta dei diritti fondamentali dell'UE, questa deve essere interpretata nel senso di prevedere importanti limitazioni al trattamento dei dati personali. Tra queste, l'applicazione del sistema PNR solo ai reati di terrorismo e ai reati gravi, aventi un legame oggettivo con il trasporto aereo di passeggeri, e l'applicazione non indiscriminata del periodo di conservazione generale di cinque anni a tutti i dati personali dei passeggeri. Vengono così notevolmente circoscritte le modalità con cui gli Stati membri dell'UE possono trattare i dati PNR. Pertanto, il Comitato ritiene probabile che l'attuale trattamento dei dati PNR nella maggior parte degli Stati membri non sia pienamente conforme alla direttiva PNR secondo l'interpretazione fornitane dalla CGUE ed invita gli Stati membri ad adottare tutte le misure di conseguenza necessarie. A questo proposito, il Comitato rileva che le autorità per la protezione dei dati sono pienamente competenti a verificare la conformità del trattamento dei dati PNR a livello nazionale con il diritto dell'UE in materia di protezione dei dati.

Un'altra dichiarazione adottata dal Comitato nel 2022 ha riguardato la proposta della Commissione europea per un codice di cooperazione di polizia dell'UE volto, in particolare, a rafforzare lo scambio di informazioni tra le autorità competenti. Il codice comprende tre misure principali: la proposta di regolamento Prüm II, la proposta di direttiva sullo scambio di informazioni di polizia e la proposta di raccomandazione del Consiglio sulla cooperazione operativa di polizia. Nella dichiarazione 03/2022 del 12 settembre il Comitato pur riconoscendo che la cooperazione di polizia è un elemento chiave per la creazione di uno spazio di libertà, sicurezza e giustizia, raccomanda l'introduzione di alcune salvaguardie essenziali per garantire che le misure proposte siano necessarie e proporzionate all'obiettivo di contribuire alla sicurezza interna dell'UE. Tra queste, il Cepd propone di fissare la tipologia e la gravità dei reati che possono giustificare una ricerca automatizzata nelle banche dati di altri Stati membri e di operare una chiara distinzione tra i dati personali di criminali condannati, indagati, vittime o testimoni ai sensi dell'art. 6 della direttiva 2016/680 cd. *law enforcement directive* (LED). Inoltre, il Comitato solleva preoccupazioni in merito alle previsioni relative alla ricerca e allo scambio automatizzati di informazioni di polizia con l'introduzione dell'indice europeo degli archivi di polizia (EPRIS) e alla sistematica condivisione di dati personali con Europol tramite il canale per lo scambio sicuro di informazioni tra gli Stati membri ed Europol (SIENA).

Dichiarazione sul codice di cooperazione di polizia dell'UE

Il 22 febbraio il Cepd ha indirizzato una lettera alla Commissione europea sulla proposta di direttiva relativa all'adeguamento delle norme in materia di responsabilità civile all'intelligenza artificiale (IA). Nella lettera il Comitato, richiamato il parere 5/2021 adottato congiuntamente al Gedp sulla proposta di regolamento sull'intelligenza artificiale (cd. AI *Act*), chiede innanzitutto di definire con chiarezza il ruolo e le responsabilità del fornitore dei sistemi di IA volti a garantire la sicurezza nel trattamento di dati personali, tenendo in considerazione l'interazione con gli obblighi di protezione dei dati in capo ai titolari e ai responsabili del trattamento. Inoltre, il Cepd ritiene che i fornitori di sistemi di IA dovrebbero essere tenuti a mettere a disposizione degli utilizzatori strumenti di mitigazione dei rischi derivanti da diversi tipi di attacchi (ad esempio quelli informatici) e ad integrare la sicurezza fin dalla progettazione durante l'intero ciclo di vita del sistema, mentre gli utilizzatori di sistemi di IA dovrebbero essere tenuti a garantire il funzionamento sicuro dello stesso. Nel definire nuove regole sulla responsabilità, un ruolo primario dovrebbe poi essere riconosciuto alla valutazione preliminare della qualità e della rappresentatività dei dati utilizzati dagli algoritmi di *machine learning* per assumere decisioni, in modo da creare un ambiente tecnologico affidabile e limitare gli effetti negativi derivanti da eventuali decisioni errate.

Lettera alla Commissione europea sulla responsabilità civile da intelligenza artificiale

21.2. *La cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

L'Autorità ha continuato a partecipare attivamente, nella propria qualità di *Supervisory Authority* alle riunioni dei gruppi di lavoro in ambito europeo di interesse per l'attività di polizia (Europol, Eurodac, CSC, CIS-Dogane, SIS II), tenutesi a distanza, nonché, dal mese di maggio 2022 anche nuovamente in presenza.

Il gruppo Europol, nella forma di Europol *Cooperation Board*, si è riunito il 31 maggio 2022. Nel corso dell'incontro è stato dato conto, tra l'altro, dell'adozione del *working program* in forma scritta, al fine di agevolare la transizione del gruppo Europol al CSC (*Coordinated Supervision Committee*). Sono state in particolare

Europol *Cooperation Board*

discusse l'evoluzione e le criticità del nuovo regolamento Europol, pubblicato in GUUE il 27 giugno 2022.

Gruppo di supervisione del sistema Eurodac

In data 2 giugno 2022 si è svolta, in formato ibrido, la riunione del Gruppo di supervisione del sistema Eurodac.

Come è noto, a novembre 2016 la Commissione è stata invitata dal gruppo di supervisione Eurodac a presentare la proposta di modifica del regolamento Eurodac. Nel 2020 sono stati presentati emendamenti a tale proposta, i negoziati sono ancora in corso, in particolar modo con riferimento alla parte relativa alla migrazione.

Inoltre sono state presentate le statistiche relative ai dati trasmessi a Eurodac, con un esponenziale aumento, a partire da aprile 2021 sino a marzo 2022, ricondotto alla crisi in Ucraina. La maggior parte degli accessi registrati, inoltre, ha riguardato le impronte digitali relative a individui maggiori di 14 anni che richiedono lo stato di rifugiato in uno dei Paesi membri dell'Unione (cat. 1). A marzo 2022 è risultato il numero più elevato di dati registrati per la categoria di impronte relative a cittadini di Paesi terzi o apolidi utilizzate per confronto con la menzionata cat. 1, al fine di verificare, nel caso di soggetti trovati illegalmente nel territorio di uno Stato membro, se avessero precedentemente presentato una richiesta di asilo.

Nella riunione del 22 novembre 2022 sono stati discussi gli aggiornamenti relativi alle modifiche del regolamento Eurodac e le statistiche fornite da EU-LISA. È stata al riguardo data lettura di una nota da parte della Commissione, che ha sollevato numerose questioni, nonché l'opportunità di sollecitare per le prossime riunioni la presenza di un membro della Commissione al fine di esporre le problematiche emerse dalle modifiche tutt'ora in corso.

La presentazione relativa agli aggiornamenti del *database* centrale di Eurodac ha evidenziato un generale buon funzionamento del sistema, con un significativo incremento delle immissioni di dati correlato alla crisi in Ucraina.

Gruppo di coordinamento della supervisione del sistema di informazione doganale: SID

Nella riunione del 1° giugno 2022 del Gruppo di supervisione, svolta in formato ibrido, è stato dato conto delle risposte di 18 Stati membri al questionario somministrato alle autorità nazionali e alle autorità di supervisione, condividendo un primo rapporto al riguardo. Nelle note è stata specificata la portata della formazione in materia di dati personali impartita al personale che ha accesso al SID sulla base delle risposte fornite dai vari Stati membri.

Agli Stati membri che non hanno ancora risposto al questionario è stata data una nuova scadenza per l'adempimento, entro e non oltre la fine del mese di settembre 2022.

Diverse DPA (*Data Protection Authority*) hanno riferito che il questionario è stato accolto con favore ed è stato ritenuto una buona esercitazione al fine di migliorare i contatti tra le DPA e le autorità nazionali, specialmente sul tema della formazione. La DPA greca ha programmato ispezioni allo scopo di verificare come le autorità nazionali mettano in pratica quanto dichiarato nelle risposte. Le risposte fornite nel questionario possono aiutare ad identificare delle *best practices* per tutti gli Stati membri.

Gruppo di coordinamento della supervisione SIS II

Il 21 novembre 2022 si è riunito per l'ultima volta il Gruppo di coordinamento della supervisione SIS II, prima del definitivo trasferimento dei suoi compiti istituzionali nell'ambito del CSC (*Coordinated Supervision Committee*). In questa veste, si è dato conto dello stato di avanzamento dell'implementazione del nuovo quadro normativo di riferimento *regulation (EU) 2018/1860, regulation (EU) 2018/1861 and regulation (EU) 2018/1862 – at MS level and at central level*; si è altresì introdotto il tema del nuovo meccanismo di svolgimento delle Schengen *evaluation* con riferimento alle modalità ed ai problemi relativi alla composizione degli *evaluation team* con particolare riguardo alla difficoltà di reclutare per detta attività i *data protection experts* appartenenti alle DPA nazionali.

La Commissione (DG HOME) ha altresì informato il Gruppo dello stato dell'arte della cd. *interoperability* in particolare per quanto concerne i tempi di realizzazione di tutti i sistemi, l'implementazione dei medesimi a livello centrale e nazionale ed infine gli aggiornamenti sulle disposizioni normative di riferimento. Il DPO di EU-LISA, come di consueto, ha presentato un documento relativo alle statistiche le quali hanno evidenziato un generale buon funzionamento del sistema.

Infine è stato presentato l'*Activity Report* 2020-2022 e le attività relative al passaggio delle attività del Gruppo al CSC.

Schenghen *evaluation*

Per quanto riguarda i trattamenti per finalità di polizia, una risorsa dell'Autorità ha partecipato, in qualità di esperto selezionato dalla Commissione, alla Schengen *evaluation* che ha avuto luogo in Svezia dal 12 al 17 giugno u.s., al fine di valutare l'ottemperanza con riferimento a l'*acquis* di Schengen da parte del Paese ospite.

Comitato di controllo coordinato (CSC)

In data 6 luglio 2022 si è svolta, in formato ibrido, la riunione del CSC (*Coordinated Supervision Committee*), nell'ambito della quale sono stati discussi per la prima volta i lavori ereditati dai precedenti gruppi di lavoro Europol e sono stati forniti aggiornamenti sul passaggio dei sistemi informativi al CSC e sulla operatività di quelli ancora non attivi come ETIAS ed ECCRIS.

È stato discusso anche lo stato dei seguenti sistemi: a) *European Public Prosecutor's Office* (EPPO), nell'ambito del quale è stato somministrato un questionario ai Paesi membri al quale circa la metà egli intervistati ha fornito risposta; b) IMI, per il quale è stata sollevata la necessità di fornire ai cittadini informazioni chiare circa i dati scambiati e di accrescere la consapevolezza dei soggetti interessati (in particolar modo anche attraverso i siti web delle DPA).

21.3. *La partecipazione dell'Autorità in seno al Consiglio d'Europa, all'OCSE e ad altri gruppi di lavoro internazionali*

Comitato consultivo della Convenzione 108/1981 (T-PD)

È proseguita l'attività dell'Autorità nell'ambito del Consiglio d'Europa, in particolare attraverso la partecipazione al Comitato consultivo della Convenzione 108/1981, cd T-PD, di cui il Garante ha conservato la presidenza per il terzo mandato consecutivo, conclusosi, in quanto non più rinnovabile, con le elezioni nella plenaria di novembre 2022.

L'attività del T-PD ha risentito della difficile situazione politica innescata dall'esclusione della Federazione russa dal Consiglio sancita dalla risoluzione del Comitato dei ministri del Consiglio d'Europa del 16 marzo 2022, a seguito della aggressione dell'Ucraina. Con una successiva decisione, adottata il 30 giugno 2022, il Comitato, circa la partecipazione della Russia ai lavori dei diversi comitati che, come il T-PD, sono aperti anche a Paesi che non fanno parte del Consiglio d'Europa, ha lasciato ai comitati in questione la valutazione sulle possibili misure restrittive da adottare.

La Convenzione 108+

Forte è stato l'impegno del Comitato consultivo nell'attività di promozione della Convenzione 108 modernizzata (cd. Convenzione 108+). Il Protocollo emendativo 223, che ha emendato l'originaria Convenzione 108 attualizzandone i principi in uno scenario fortemente mutato da nuove tecnologie e globalizzazione, conta, al 31 dicembre 2022, 44 firme e 20 ratifiche, tra cui quella dell'Italia, che ha depositato gli strumenti di ratifica l'8 luglio 2021.

In occasione della Giornata della protezione dei dati, che commemora l'apertura alla firma della Convenzione sulla protezione dei dati del Consiglio d'Europa il 28 gennaio 1981, la presidenza italiana del Comitato dei ministri ha ospitato una conferenza per discutere della Convenzione 108+ e del suo potenziale come standard internazionale per la protezione dei dati.

21

In una dichiarazione al termine della conferenza, la presidenza italiana ha sottolineato la necessità che tutte le Parti della Convenzione 108, che non vi abbiano ancora provveduto, ratifichino al più presto il Protocollo emendativo della 108 per permetterne l'entrata in vigore. La dichiarazione evidenzia l'importanza del trattato modernizzato in materia di protezione della *privacy* e dei dati personali a livello internazionale.

Il Garante, che ha svolto un ruolo attivo nella promozione della Convenzione 108, si è peraltro reso promotore di una specifica risoluzione, nell'ambito della *Spring Conference* 2022 (v. *infra*), sulla necessità di ratificare tale Convenzione al fine di assicurare un'efficace protezione dei diritti delle persone nell'era digitale.

Sempre nell'ambito della promozione della Convenzione modernizzata, nella plenaria di novembre 2022, si è svolto un giro di tavolo di tutte le delegazioni dei Paesi che non hanno ancora ratificato per verificare lo stato di avanzamento dei rispettivi processi di ratifica. Il quadro emerso è di maggiore ottimismo rispetto al tempestivo raggiungimento delle 38 ratifiche necessarie all'entrata in vigore della Convenzione, nella consapevolezza della necessità di mantenere alta l'attenzione dei governi sulla rilevanza della ratifica.

Linee guida in materia di identità digitale

Nella plenaria di novembre sono state adottate le linee guida sull'identità digitale (T-PD (2021)2rev9). Il documento muove dal presupposto che gli schemi nazionali di identità digitali, sempre più diffusi nei diversi Paesi, pur potendo portare vantaggi per le persone, anche sul piano del godimento di diritti e posizioni giuridiche rilevanti, devono tuttavia essere opportunamente regolati per evitare ripercussioni negative sui diritti umani, a cominciare da possibili forme di discriminazione, esclusione ed emarginazione di individui e gruppi di persone, nonché forme ingiustificate di profilazione e sorveglianza, fino all'uso improprio dei dati o ai furti di identità.

Significativi rischi per la *privacy* degli individui sorgono anche a causa della moltitudine di attori coinvolti nella gestione dell'identità digitale, inclusi fornitori di identità, di servizi e terze parti autorizzate a sviluppare o utilizzare sistemi nazionali di identificazione digitale.

Le linee guida, destinate ad una pluralità di soggetti quali i governi e i *policy maker*, i titolari del trattamento, i fornitori dei servizi e le autorità di protezione dati, raccomandano in particolare che l'introduzione di sistemi di identità digitale sia preceduta da una valutazione di impatto che non riguardi solamente la protezione dei dati ma anche i diversi diritti fondamentali in gioco (*human rights impact assessment* - HRIA) e che coinvolga segnatamente gli interessati e le categorie di interessati maggiormente colpiti dall'impatto dei sistemi di identità digitale.

Art. 11 della Convenzione modernizzata

Il Comitato ha inoltre proseguito le attività di approfondimento rivolte alla stesura degli ulteriori documenti previsti dal programma di lavoro. È proseguita la riflessione, sull'art. 11 della Convenzione 108+ relativo ai criteri che devono accompagnare le possibili restrizioni ed eccezioni ai principi della stessa 108+ per garantire che, anche in questo caso, sia assicurato il rispetto dell'essenza del diritto alla protezione dei dati.

Scambi automatizzati ai fini di antiriciclaggio e lotta al finanziamento del terrorismo

È altresì proseguito il lavoro sul tema degli scambi automatizzati di dati tra Stati per finalità amministrative e di tassazione, al fine di aggiornare il parere del T-PD del 2014 (T-PD(2014)05), alla luce delle novità nel frattempo intervenute in questi settori. La plenaria, per addivenire ad una più tempestiva finalizzazione del testo, ha confermato la proposta del *Bureau* di concentrarsi sulla prima parte del documento dedicata agli scambi automatizzati finalizzata alla lotta al riciclaggio e al finanziamento del terrorismo, peraltro già piuttosto corposa, tralasciando per ora la questione dei trattamenti per fini fiscali che potrà essere oggetto di un secondo documento da finalizzare in seguito.

È inoltre sensibilmente avanzato il lavoro di aggiornamento, alla luce delle novità introdotte dalla Convenzione 108+, in materia di trasferimento dei dati e delle clausole contrattuali standard per i flussi di dati verso Paesi terzi che non abbiano un adeguato livello di protezione, elaborate dal Consiglio d'Europa nel 1992 e riviste nel 2002.

Clausole contrattuali standard

Il Data *Protection Commissioner* del Consiglio d'Europa Jean-Philippe Walter ha annunciato il 15 giugno 2022 l'adozione del regolamento sulla protezione dei dati del CoE, a lungo auspicato dal T-PD e oggetto di uno specifico parere adottato dallo stesso Comitato il 20 aprile 2022 (T-PD-BUR (2022)1).

È stato conferito il Premio Stefano Rodotà 2022 a Teresa Quintel per la sua tesi di dottorato "*Managing Migration Flows by Processing Personal Data within the Adequate Data Protection Instrument - Scoping Exercise between general and law enforcement data protection rules applicable to Third Country Nationals*" e a Sabrina Nucciotti, per il suo articolo "*European Health Data Sharing is on the wrong track - How the distributed machine learning system, Personal Health Train (PHT), can overcome the European privacy barriers to health data sharing for medical research*". Le due vincitrici hanno presentato i rispettivi lavori alla plenaria come previsto dal regolamento del Premio.

Premio Stefano Rodotà

Nell'ambito del Consiglio d'Europa è stata avviata l'attività del nuovo Comitato *ad hoc* sull'intelligenza artificiale - CAI che, nel solco del lavoro svolto dal precedente comitato CAHAI (v. Relazione 2021, p. 235), ha proseguito l'elaborazione di un quadro giuridico per lo sviluppo, la progettazione e l'applicazione dell'IA, basato sugli standard del Consiglio d'Europa sui diritti umani, la democrazia e lo Stato di diritto (v. cap. 16).

CAI-Comitato *ad hoc* sull'IA

È proseguita l'intensa attività dell'Autorità in ambito OCSE, in particolare attraverso la partecipazione al DGP (*Working Party on Data Governance and Privacy*), di cui il Garante detiene la vicepresidenza dal 2012 (già WPSPDE - *Working Party on Security and Privacy in Digital Economy*), confermata nella plenaria di ottobre anche per il 2023.

OCSE-DGP (Gruppo di lavoro *Data Governance and Privacy*)

Le due riunioni plenarie del DGP (7 e 8 aprile e 11 ottobre 2022), cui si sono come di consueto aggiunte le relative riunioni del *Bureau* (il gruppo ristretto del DGP), sono state anche per il 2022 caratterizzate da un'altissima partecipazione delle delegazioni dei Paesi membri, agevolata dalla partecipazione da remoto. Nello specifico, in primo piano si pone anche per il 2022 il lavoro di implementazione 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*). In particolare i delegati hanno discusso il piano di lavoro per mettere in pratica la guida per l'attuazione delle OECD *Privacy Guidelines*. Nella riunione plenaria di aprile 2022, il Gruppo di lavoro DGP ha aderito alla bozza di guida e nel luglio 2022, il gruppo consultivo informale, istituito per fornire *feedback* e discutere iterativamente le revisioni proposte, ha ultimato la stesura del capitolo sulla *Responsabilità/Accountability* della medesima guida. In particolare il Gruppo ha convenuto che la prefazione ed il capitolo sull'*accountability* siano maturi per la trasmissione (con revisioni minori concordate) al CDEP (*Digital Economy Policy*) ai fini dell'approvazione e della declassificazione. Tale capitolo ha lo scopo di aiutare i responsabili politici, le autorità di protezione dati, gli enti pubblici e le organizzazioni del settore privato a comprendere meglio e ad attuare il principio di responsabilità delle linee guida sulla *privacy* attraverso i programmi di gestione *privacy*, chiarendo ulteriormente alcune delle questioni sollevate negli anni precedenti. Sebbene le descrizioni e gli esempi nel capitolo riguardano principalmente le organizzazioni del settore privato, possono rappresentare un utile riferimento anche per gli enti

Linee guida dell'OCSE sulla *privacy*

pubblici impegnati in attività connesse al trattamento dei dati personali. Nel corso dell'anno sono stati altresì discussi i prossimi passi per il lavoro sulla localizzazione dei dati, tema su cui dovrebbe concentrarsi il prossimo capitolo della guida e su cui i delegati hanno mandato contributi negli ultimi mesi del 2022.

Raccomandazione OCSE sulla protezione dei minori *online*

Il Gruppo ha proseguito nell'implementazione della raccomandazione sui minori *online* (*Recommendation of the Council on Children in the Digital Environment*) adottata dal Consiglio OCSE nel 2021, che aggiorna la precedente raccomandazione del 2012, alla luce degli sviluppi tecnologici ed applicativi delle innovazioni digitali degli ultimi anni e della loro diffusione, anche tra i minori, accelerata proprio dalla pandemia (cfr. Relazione 2021, p. 238). Per dare attuazione alla raccomandazione, il Gruppo ha elaborato una bozza provvisoria di documento sulla sicurezza digitale *by design* per i bambini. Dato che il contenuto del documento in parola concerne non soltanto la *governance* e la *privacy* dei dati dei minori, i delegati hanno deciso di trasferirlo al CDEP, mantenendo la possibilità di essere regolarmente consultati sugli aspetti di *governance* dei dati e di protezione dati. Ciò in ragione dell'importanza del documento che ambisce a stabilire le condizioni per un ambiente digitale per i minori più sicuro attraverso linee guida chiare e internazionalmente condivise e per il delicato bilanciamento tra le opportunità che il mondo digitale può portare ai bambini e l'effettiva protezione dai rischi.

***Data Governance: Enhanced Access and Sharing of Data* (EASD)**

In relazione alla raccomandazione sul rafforzamento dell'accesso e della condivisione dei dati (*Recommendation of the Council on Enhancing Access to and Sharing of Data* - EASD) adottata dal Consiglio OCSE nel 2021 (cfr. Relazione 2021, p. 238), nell'anno di riferimento è proseguito il lavoro sulla bozza rivista del documento di accompagnamento per l'attuazione della raccomandazione stessa (*Companion Document*) e per la declassificazione del documento.

L'attuazione di questa raccomandazione avrà un importante rilievo soprattutto in relazione allo scopo principale dell'EASD, ossia 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 *benefit* che per individuare rischi potenziali (ad es., affrontare temi sociali condivisi globalmente come l'emergenza Covid-19). L'importante lavoro svolto, dal DGP, unitamente ad altri Comitati quali il CDEP, ed il CSTP, nonché dal PGC, sarà centrale per gli anni a venire anche in relazione agli altri lavori dell'OCSE in materia di protezione dei dati personali. Risulta pertanto quanto mai necessaria una guida per l'attuazione della raccomandazione e il citato *Companion document* nella sua versione aggiornata può senz'altro rappresentare un utile ausilio.

Accesso affidabile dei governi ai dati dei privati

Altro tema delicato affrontato nel corso del 2022 è stato quello dell'accesso affidabile dei governi ai dati detenuti dai privati (*trusted government access to data*). È stato portato a termine il lavoro del Gruppo OCSE di redazione in materia di *trusted government access to data*.

Il Garante ha rappresentato l'Italia in seno al Gruppo di redazione ampliato (*Expanded Drafting Group* - EDG) che si è riunito frequentemente nel corso dell'anno, raggiungendo convergenze sulle garanzie per un accesso realmente *trusted* (basi giuridiche; obiettivi legittimi; autorizzazioni; limiti al trattamento; trasparenza; *oversight* e *redress*). In particolare, dopo 18 riunioni del Gruppo di redazione, comprensivo di rappresentanti di 33 Paesi membri dell'OCSE e dell'Unione europea tra febbraio 2021 e ottobre 2022 il Gruppo di redazione ha definito la bozza di testo, sotto forma di dichiarazione, poi adottata nella riunione ministeriale del CDEP del 13-16 dicembre a Gran Canaria. Si tratta di un grande risultato che sembrava di difficile realizzazione date le iniziali divergenze tra le delegazioni tra cui la contrapposizione tra "anglosassoni", che avrebbero voluto

escludere dalla dichiarazione gli accessi governativi "non *compelled* " (una zona grigia indeterminata che comprende dati comprati, ceduti "volontariamente" dai privati, intercettati dai servizi di sicurezza, ecc.), ed "europei", per i quali i principi della dichiarazione devono coprire ogni tipo di accesso, seppure con delle *nuances* per casi particolari, a cominciare dallo spionaggio. Il lavoro svolto ha dimostrato che i Paesi membri condividono obiettivi e sfide comuni quali la protezione della sicurezza nazionale unitamente ai diritti e alle libertà degli individui nonché la fornitura di una supervisione e mezzi di ricorso efficaci, mantenendo al contempo i segreti di sicurezza nazionale o la riservatezza delle indagini in corso delle autorità di contrasto. In particolare, il Gruppo ha identificato sette principi comuni, che si riflettono nelle leggi e nelle pratiche esistenti dei Paesi membri dell'OCSE.

21.4. *Le conferenze internazionali ed europee*

Global Privacy Assembly (GPA)

La Conferenza annuale della protezione dati (GPA), dedicata al tema "Intelligenza artificiale e metaverso" si è tenuta dal 25 al 28 Ottobre 2022 ad Istanbul, organizzata dall'Autorità per la protezione dei dati personali turca (Kisisel Verileri Koruma Kurumu).

Hanno partecipato 130 autorità provenienti dai cinque continenti impegnate sui temi della *privacy* e della protezione dei dati personali, esperti accademici e rappresentanti del settore privato e della società civile.

Il principale obiettivo della GPA, evento unico nel suo genere per la sua portata globale, è quello di promuovere e potenziare l'azione regolatoria dei suoi partecipanti e la loro cooperazione.

I temi discussi durante l'ultima edizione hanno tenuto in particolare considerazione i recenti sviluppi di nuove tecnologie, tra le quali intelligenza artificiale e metaverso, ed il loro potenziale impatto sulla protezione dei dati personali dei singoli individui.

Il presidente del Garante, prof. Pasquale Stanzione, ha partecipato in qualità di esperto ad una discussione sulla questione della protezione dei dati personali dei bambini nell'era digitale.

Vari sono i gruppi di lavoro permanenti che dovranno procedere su diversi temi: *Data Protection and Other Rights and Freedoms; Global Standards and Frameworks; International Enforcement; International Practice Cooperation; International Working Group on Data Protection in Technology (Berlin Group); Ethics and Data Protection in AI; Digital Citizen and Consumer; Digital Education; Data Sharing; Digital Economy*. Come di consueto la Conferenza si è articolata in una sessione aperta (*open session*) ai diversi *stakeholders* e una sessione ristretta (*closed session*) a cui hanno partecipato solo le autorità di protezione dati.

Conferenza di primavera (*Spring Conference*)

La Conferenza di primavera delle autorità di protezione dati europee, tradizionale momento di scambio e *best practice*, si è tenuta a Cavtat - Dubrovnik il 19-20 maggio dopo due anni di sospensione a causa della pandemia.

Trasferimenti di dati verso Paesi terzi, cooperazione fra autorità, Convenzione 108+ e convergenza delle legislazioni nazionali degli Stati terzi verso il modello europeo, sfide dell'innovazione come l'intelligenza artificiale, giurisprudenza della Corte europea dei diritti dell'uomo, sono stati i temi centrali della Conferenza.

Per il Garante la vice presidente prof.ssa Ginevra Cerrina Feroni ha presentato la risoluzione concernente la necessità di una tempestiva ratifica della Convenzione 108+ e l'avv. Guido Scorza è intervenuto in merito all'esperienza del *Contest* su informative *privacy* più chiare grazie a simboli e icone.

Nel corso della Conferenza sono state adottate due risoluzioni: la prima,

proposta dal Garante, sulla necessità di ratificare la Convenzione 108; la seconda sulla costituzione di un gruppo direttivo della conferenza di primavera, che vigili sull'attuazione delle questioni prioritarie condivise dalle autorità europee della protezione dei dati, in particolare sulla necessità di una più stretta cooperazione tra di esse.

La Conferenza ha inoltre votato a favore del riconoscimento dello *status* di membro della *Spring Conference* all'Autorità di protezione dati della Bassa Sassonia e a quella della *European Space Agency*, nonché dello *status* di osservatore all'EDPB.

G7 delle autorità di protezione dati

Il 7 e l'8 settembre la vice presidente prof.ssa Ginevra Cerrina Feroni ha partecipato per il Garante al secondo *meeting* delle autorità di protezione dati del G7, sotto la presidenza del Commissario federale tedesco per la protezione dei dati e la libertà di informazione. L'incontro si è svolto nel quadro del G7 *Digital Track* dei ministri digitali della Presidenza tedesca del G7 per discutere delle questioni normative e tecnologiche degli sviluppi nel contesto del *Data Free Flows with Trust* (DFFT), proposto nel 2019 dall'allora *premier* giapponese Shinzo Abe. L'obiettivo è la costruzione di un clima di fiducia all'interno di un sistema economico ormai dipendente dai flussi di dati, bilanciando, nell'economia digitale, la tutela dei diritti individuali con la salvaguardia delle libertà del mercato. Il vertice ha avuto come scopo anche quello di condividere le conoscenze sulle prospettive di "spazi di dati internazionali", che rappresentano un approccio emergente alla condivisione di dati affidabile e volontaria all'interno e tra organizzazioni e settori, sia a livello nazionale che internazionale, per sostenere l'innovazione nel mondo accademico, nell'industria e nel settore pubblico. I temi discussi hanno riguardato, in particolare, gli strumenti per il trasferimento internazionale dei dati, inclusa la certificazione; le tecnologie di miglioramento della *privacy* (PET); gli standard di anonimizzazione; il rafforzamento dei principi di minimizzazione dei dati per affrontare le sfide della sorveglianza commerciale. Il Garante italiano ha proposto che le autorità per la protezione dei dati e la *privacy* del G7, in quanto gruppo di autorità dei sette sistemi socio-economici più importanti al mondo, indicassero un modello etico e culturale distintivo per la *governance* dell'IA, e ha ottenuto che nel documento finale dei lavori del G7 venisse inserito "il rifiuto di un uso indiscriminato dell'IA applicata ai dati personali che porti a forme di sorveglianza massiva con l'evidente scopo di controllare e manipolare i comportamenti degli individui a partire dai dati personali, raccolti, analizzati e incrociati in grandi quantità, varietà e velocità". Il documento finale propone anche la costruzione di un'alternativa virtuosa all'uso dell'IA da parte delle autorità pubbliche che tenga conto dei valori e dei principi dello stato di diritto e del governo democratico a cui tutti ci riferiamo. Le conclusioni raggiunte e le direttive per il futuro sono state raccolte in un compendio dedicato alle azioni intraprese da dette *authority* per promuovere la concorrenza nei mercati digitali (*Compendium of approaches to improving competition in digital markets*). I Garanti dei Paesi del G7 continueranno a impegnarsi per sviluppare un piano d'azione e preparare il prossimo incontro, che sarà svolto sotto la presidenza dell'Autorità garante giapponese (PPC) il 20 e 21 giugno 2023 a Tokyo nel corso del quale il Garante anticiperà parte del contenuto del successivo vertice che si svolgerà in Italia nel 2024.

21.5. *Le domande pregiudiziali davanti alla Corte di giustizia dell'Unione europea*

Rinvii pregiudiziali ex art. 267 TFUE

L'attività internazionale del Garante ha riguardato anche le cause pregiudiziali proposte dinanzi alla CGUE dai giudici degli Stati membri, ai sensi dell'art. 267 del TFUE, nei casi in cui le stesse hanno interessato la materia della protezione dei dati

personali. In particolare, si segnalano le seguenti sentenze adottate dalla CGUE nel corso del 2022:

- sentenza 24 febbraio 2022, causa C-175/20 sulla richiesta di informazioni da parte dell'Amministrazione tributaria;
- sentenza 24 marzo 2022, causa C-245/20 sull'accesso agli atti processuali da parte dei giornalisti;
- sentenza 5 aprile 2022, causa C-140/20 sui dati di traffico;
- sentenza 28 aprile 2022, causa C-319/20 sull'art. 80 del RGPD;
- sentenza 21 giugno 2022, causa C-817/19 sulla direttiva PNR (UE) 2016/681 (codice di prenotazione a fini di prevenzione, individuazione, indagine e perseguimento di reati di terrorismo e reati gravi);
- sentenza 1° agosto 2022, causa C-184/20 sull'accesso civico (obbligo di pubblicazione di dati personali su internet);
- sentenza 20 settembre 2022, cause riunite C-339/20 e C-397/20 sui dati di traffico, poteri di vigilanza e d'indagine dell'Autorità dei mercati finanziari;
- sentenza 20 settembre 2022, cause riunite C-793/19 e 794/19 sui dati di traffico e telematici e sulla conservazione generalizzata e indiscriminata di detti dati;
- sentenza 20 ottobre 2022, causa C-77/21 sulla copia di banca dati per effettuare test e finalità del trattamento (finalità diverse);
- sentenza 20 ottobre 2022, causa C-534/20 sulla risoluzione ordinaria del rapporto di lavoro del Rpd;
- sentenza 20 ottobre 2022, causa C-306/21 sulla registrazione di video delle operazioni di scrutinio elettorale all'interno dei seggi in occasione di una procedura elettorale nazionale;
- sentenza 27 ottobre 2022, causa C-129/21 sul consenso alla pubblicazione dei dati negli elenchi degli abbonati telefonici;
- sentenza 17 novembre 2022, causa C-350/21 sulla conservazione generalizzata e indiscriminata dei dati di traffico;
- sentenza 22 novembre 2022, cause riunite C-37/20 e C-601/20 sull'accesso del pubblico alle informazioni sulla titolarità effettiva delle società e delle altre entità giuridiche costituite nel territorio dello Stato membro (prevenzione dell'uso del sistema finanziario a fini di riciclaggio e di finanziamento del terrorismo);
- sentenza 1° dicembre 2022, causa C-564/21 sulla politica di asilo e l'accesso alle informazioni contenute nel fascicolo del richiedente;
- sentenza 8 dicembre 2022, causa C-180/21 sul trattamento dei dati da parte della Procura di uno Stato membro e finalità del trattamento (finalità diverse);
- sentenza 8 dicembre 2022, causa C-460/20 sulla deindicizzazione.

21.6. *I progetti per l'applicazione del RGPD finanziati dall'Unione europea*

Progetto ARC II

Nel mese di settembre 2022 il Garante ha avviato un progetto europeo denominato ARC II (https://arc-rec-project.eu/riguardo-al-progetto-arc-ii/), in partenariato con l'Autorità garante per la protezione dei dati personali della Croazia (capofila del progetto), l'Università degli Studi di Firenze (Dipartimento di scienze giuridiche) che affiancherà il Garante nello sviluppo della programmazione in Italia, l'Università di Zagabria (Facoltà di informatica) e l'Università di Bruxelles (Vrije).

ARC II è un progetto co-finanziato al 90% dalla Commissione europea la cui durata è di 24 mesi, a partire dal mese di settembre 2022.

Gli obiettivi del progetto sono:

- sviluppare uno strumento digitale *open source* denominato Olivia, liberamente

21

accessibile, interoperabile e innovativo, adattato alle esigenze specifiche delle PMI per conformare la loro attività al RGDP;

- condurre 20 *workshop* sul RGPD in Croazia e 20 in Italia durante i quali le PMI potranno ricevere supporto diretto per risolvere i loro problemi specifici relativi alla conformità al RGPD;

- condurre una campagna di sensibilizzazione sui *media* croati e italiani, creare materiali didattici e video;

- organizzare 2 *workshop* di verifica e 2 conferenze internazionali per diffondere i risultati del progetto;

- promuovere lo strumento digitale Olivia e incoraggiare le PMI a utilizzarlo, oltre a sensibilizzare in generale il pubblico sulla protezione dei dati personali.

22 Attività di normazione tecnica internazionale e nazionale

Il Garante ha proseguito la collaborazione in tema di elaborazione di norme tecniche internazionali nell'ambito del *Working Group* 5 del sottocomitato SC27, che si occupa della sicurezza delle informazioni all'interno del comitato tecnico JTC1 dell'Organizzazione internazionale per la normazione (ISO). Il gruppo di lavoro segue gli aspetti di sicurezza nella gestione delle identità relativamente alle tecnologie biometriche e alla protezione dei dati personali. Armonizzando la propria posizione con quelle delle altre autorità di protezione dati tramite il Cepd, che ha un collegamento in proposito con ISO, l'Autorità ha seguito lo sviluppo delle seguenti norme tecniche:

- ISO 27701:2019 - *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*, revisione a seguito della pubblicazione della ISO 27002:2022;

- ISO TR 27563 - *Impact of security and privacy on AI use-cases*, che finalizza l'analisi degli *use-case* del documento ISO/IEC TR 24030 (*Information technology – Artificial Intelligence (AI) – use-cases*) elaborato dal SC42 al fine di fornire informazioni su come valutare l'impatto di sicurezza e *privacy* nell'ambito dell'intelligenza artificiale;

- ISO 27566 - *Information security, cybersecurity and privacy protection – Age assurance systems – Framework*, che si propone di stabilire principi chiave, che includono anche la *privacy*, per abilitare decisioni di fornitura di beni, servizi o contenuti che dipendano dall'età del soggetto richiedente mediante la definizione di un *framework* di indicatori di confidenza di età o di *range* di età delle persone fisiche;

- ISO 27556 - *User-centric framework for the handling of PII based on privacy preference* che definisce un quadro di riferimento per la gestione delle scelte riguardanti le informazioni personali con un approccio *user-centric*;

- ISO TS 27006 - *Requirements for bodies providing audit and certification of privacy information management systems according to ISO/IEC 27701 in combination with ISO/IEC 27001*, che definisce requisiti aggiuntivi alla ISO 17021 e 27006 per gli organismi di certificazione che svolgono *audit* e rilasciano certificazioni secondo la nuova ISO 27701 (*Privacy Information management System*);

- ISO TS 27559 - *Privacy enhancing data de identification framework*, che fornisce una guida sull'implementazione della de-identificazione e la valutazione dei rischi di re-identificazione relativi al ciclo di vita dei dati de-identificati;

- ISO 27557 - *Organizational privacy risk management*, che fornisce linee guida per la gestione del rischio *privacy* delle organizzazioni titolari e responsabili del trattamento integrando la valutazione dell'impatto sugli interessati nel *privacy risk management program* delle medesime;

- ISO TS 27560 - *Consent Receipt and Record Standard*, che definisce una struttura e formato comune per *consent receipt* e *consent record*;

- ISO TS 27561 - *Privacy operationalisation model and method for engineering* (POMME), che, sulla base del modello OASIS-PMRM (*Privacy Management Reference Model*), fornisce elementi e supporta le organizzazioni al fine di definire un modello e metodi standardizzati per la *privacy engineering* di sistemi complessi.

Collaborazione è stata assicurata nell'ambito del *Project Committee* (PC) 317 di ISO, istituito dal *Technical Management Board* a febbraio 2018, per lo sviluppo

di una norma tecnica internazionale su *Consumer protection: Privacy by design for consumer goods and services*.

L'Autorità inoltre, nell'ambito del *Working Group* 5 del comitato tecnico JTC13 del CEN CENELEC che si occupa dello sviluppo di norme tecniche riguardanti *Data Protection, Privacy and Identity Management*, ha contribuito in particolare allo sviluppo delle seguenti norme tecniche:

- EN 17529 - *Privacy Protection by design and by default*, che, in risposta al mandato della Commissione europea (Direzione generale sicurezza e affari interni), individua obiettivi, requisiti di protezione dati e linee guida per supportare sviluppatori, produttori e fornitori di servizi e prodotti nell'implementazione dei principi in materia di protezione dei dati fin dalla progettazione e per impostazione predefinita nello sviluppo, produzione di prodotti e servizi;

- EN 17799 - *Personal data protection requirements for processing activities*, che, sulla base della prassi di riferimento UNI 43.2:2018 *Guideline for personal data management within* ICT *according to Regulation* EU 679/2016 (GDPR) - *Requirements for the protection and conformity assessment of personal data within* ICT, propone requisiti per la protezione dei dati personali gestiti da sistemi informativi utilizzabili anche per certificazioni ai sensi dell'art. 42 del RGDP;

- EN 17740 - *Requirements for professional profiles related to personal data processing and protection*, che, sulla base della norma tecnica UNI 11697:2018, individua requisiti armonizzati a livello europeo e in accordo con il *European Qualifications Framework* (EQF), certificabili, circa le competenze, conoscenze e abilità dei professionisti che svolgono attività nell'ambito del trattamento e della protezione dati personali;

- JT013037 - *Privacy Information Management System per ISO/IEC 27701 - Refinements in European context*, che adatta il *framework* internazionale offerto dalla ISO 27701 nel contesto europeo.

Del pari è proseguita la collaborazione con le diverse commissioni tecniche UNINFO, l'ente di normazione federato con UNI (Ente nazionale italiano di unificazione).

23 L'attività di comunicazione, informazione e di rapporto con il pubblico

23.1. *La comunicazione del Garante*

23.1.1. I 25 anni dell'Autorità

Nel 2022 l'Autorità ha celebrato il 25° anniversario dalla sua istituzione. Tale importante ricorrenza è stata l'occasione per dare nuovo impulso alla diffusione della cultura della *privacy*, per fare un bilancio sul lavoro svolto in questo quarto di secolo e per delineare le sfide future. L'attività di comunicazione e informazione è stata pertanto ricca di eventi ed iniziative grazie anche all'intensificazione delle campagne di comunicazione istituzionale.

A seguito della convenzione stipulata a dicembre 2021 tra il Garante ed il Mise (oggi Ministero per le imprese e il *made in Italy*), l'Autorità ha promosso attività dedicate sia alla comunicazione che alla formazione, rivolte soprattutto alla generalità dei cittadini, con particolare attenzione ai minori ed ai consumatori.

Le iniziative hanno riguardato i fenomeni più invasivi della sfera della riservatezza delle persone, quali la pubblicità commerciale indesiderata e la profilazione degli utenti, il *revenge porn*, il *phishing*, gli assistenti digitali. Particolare attenzione è stata rivolta all'utilizzo responsabile della rete e dei nuovi *social media*, innanzitutto promuovendo, sui *media* tradizionali e sui *social network*, la conoscenza dei diritti e delle tutele previste dalla normativa in materia di protezione dati. Con tale obiettivo, a fine anno, è stata lanciata la campagna di comunicazione istituzionale, intitolata "Finalmente un po' di *privacy*" incentrata su una narrazione in cui il Garante, impersonato da un attore, interviene in diverse situazioni quotidiane in aiuto delle persone che vedono violato il diritto alla riservatezza dei propri dati personali. Negli *spot* sono stati illustrati i rischi di un uso improprio dei dati e indicate le forme di tutela esistenti. Dall'uso delle *app* alle frodi digitali, dal cyberbullismo al *revenge porn*, dal *telemarketing* selvaggio agli assistenti digitali, dai dati sanitari alla profilazione e all'uso delle *password*. Il *claim* finale "Se proteggi i tuoi dati proteggi te stesso" è un invito ad essere sempre più consapevoli del "valore *privacy*". I video sono disponibili al link: https://www.garanteprivacy.it/finalmente-un-po-di-*privacy*.

Nell'ambito della menzionata campagna, il Garante ha realizzato un totale di 27 *spot* istituzionali e informativi di cui 18 su canali Rai e 9 diffusi sul web e sui *social media*.

Gli eventi

Ha dato inizio alle celebrazioni del 25° anniversario la presentazione del volume "25 anni di *Privacy* in Italia. Dalla distanza di cortesia all'algoritmo", che, attraverso le foto dell'Agenzia Ansa, ha raccontato i primi 25 anni di impegno del Garante in difesa dei diritti delle persone accompagnando lo sviluppo sociale e culturale del Paese, ed ha gettato anche lo sguardo alle nuove sfide sulle quali l'Autorità è impegnata: intelligenza artificiale, algoritmi, riconoscimento facciale, internet delle cose, neurodiritti.

L'evento si è svolto il 6 aprile, presso la Camera di commercio-Tempio di Adriano, alla presenza di Anna Macina, Sottosegretaria di Stato al Ministero della giustizia. Al dibattito – moderato da Bruno Vespa – sono intervenuti il Collegio del Garante; Luigi Contu, direttore dell'Ansa; Andrea Jelinek, presidente del Comitato dei Garanti *privacy* europei in remoto; Lorenzo Tagliavanti, presidente della Camera di commercio di Roma. Le relazioni finali sono state tenute dai Presidenti emeriti della Corte costituzionale, Giovanni Maria Flick e Ugo De Siervo.

23

Nel corso della presentazione è stato proiettato il *videoclip*, appositamente realizzato dall'Ufficio, con il supporto di una società esterna (https://www.garanteprivacy.it/25-anni-di-*privacy*-in-italia).

"Il ruolo del Garante per la protezione dei dati personali: la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro" è il titolo del convegno istituzionale che si è tenuto il 24 maggio 2022 in Campidoglio (Sala della protomoteca), coordinato dalla vice presidente del Garante Ginevra Cerrina Feroni, inconcentrato sul rapporto tra protezione dei dati e Pnrr, sulla digitalizzazione del Paese, sulla *data economy* e l'intelligenza artificiale. Particolare attenzione è stata dedicata alla tutela dei consumatori nel mondo digitale.

Al convegno, alla presenza del Ministro dello sviluppo economico Giancarlo Giorgetti e del sindaco di Roma Roberto Gualtieri, hanno partecipato ex Garanti, costituzionalisti, esperti, esponenti del mondo accademico ed imprenditoriale.

Il 4 luglio, presenti il vice Ministro dello sviluppo economico Gilberto Pichetto Fratin, il presidente della Regione Piemonte Alberto Cirio e il sindaco di Torino Stefano Lo Russo, si è svolto a Torino presso la sala delle Guardie svizzere di Palazzo Reale il convegno dal titolo "La protezione dati: da 25 anni la bussola del futuro". L'evento è stato coordinato da Agostino Ghiglia, ed ha visto la partecipazione dei Componenti del Garante, di giuristi, esperti, giornalisti e di esponenti del mondo accademico. Il dibattito si è concentrato su temi di strettissima attualità, quali le prospettive tecnologiche e giuridiche connesse al metaverso, la *cybersecurity, la cyberwar*, le *fake news*, l'intelligenza artificiale e l'internet delle cose.

A settembre il Garante ha lanciato una *call to action* per il futuro ed ha invitato a Pietrarsa, presso il Museo nazionale delle Ferrovie dello Stato, i rappresentanti di alcuni dei principali *stakeholders* pubblici e privati per ragionare su idee e progetti volti a promuovere e rafforzare il diritto alla protezione dati. Nel Convegno "*State of privacy* '22", coordinato da Guido Scorza, sono stati coinvolti più di 250 rappresentanti tra Istituzioni nazionali e internazionali e amministrazioni, rappresentanti delle *big tech*, dei consumatori, dei *media* e dei servizi di comunicazione oltre ad esperti e rappresentanti del settore universitario e della ricerca. L'evento ha rappresentato un'occasione di confronto e di stimolo reciproco, con l'ambizioso obiettivo di individuare idee e soluzioni in risposta alle ormai indifferibili sfide che attendono la società dei dati nella quale viviamo.

Il 21 ottobre 2022 presso il Teatro Argentina di Roma è stata organizzata l'iniziativa conclusiva, nell'ambito delle celebrazioni per i 25 anni di *privacy* in Italia: "*Privacy First!* dalla parte dei giovani". Per parlare di *social media*, cyberbullismo, *revenge porn*, rischi della rete, il Garante ha invitato a teatro 500 studenti provenienti dalle scuole secondarie di secondo grado, associazioni a tutela dei minori, associazioni dei consumatori e i rappresentanti delle Istituzioni. Sul palco sono intervenuti, oltre al Collegio del Garante, la filosofa Maura Gancitano, il giovane sacerdote e *influencer* don Alberto Ravagnani, il giornalista esperto di tecnologie Raffaele Angius, lo scrittore Pietro Grossi. Ha moderato l'incontro la giornalista Rai Annalisa Bruchi.

L'evento è stato costruito con la formula dei "TED *Talks*", denominati per l'occasione "*Privacy-Talks*", in cui ognuno dei relatori ha raccontato in 10-15 minuti una storia, un'esperienza personale, ha dato consigli, o illustrato un tema legato alla *privacy* interagendo con il pubblico. Ogni intervento è stato intervallato da un video informativo ideato e prodotto dall'Ufficio. L'intenzione dell'Autorità è stata infatti quella di proporre una forma di divulgazione quanto più possibile empatica capace di coinvolgere i ragazzi spiegando in maniera efficace l'importanza di proteggere i dati personali e la sfera più intima, propria e degli altri.

Il 14 settembre 2022, su bozzetto del Garante, il Mise ha emesso il francobollo celebrativo realizzato dall'Istituto poligrafico e Zecca dello Stato e distribuito da Poste italiane. L'immagine raffigurata rappresenta la stilizzazione grafica dell'uomo vitruviano di Leonardo che idealmente si trasforma in dati digitali.

Il francobollo celebrativo

Il presidente dell'Autorità, Prof. Pasquale Stanzione, ha al riguardo sottolineato come l'emissione del francobollo celebrativo abbia rappresentato "un riconoscimento dall'alto valore simbolico ai Collegi del Garante che si sono succeduti in questi anni e ai suoi dipendenti che, con dedizione e competenza, hanno contribuito a convertire valori e princìpi in realtà".

I Protocolli e la partecipazione alle manifestazioni

L'Autorità ha partecipato all'edizione 2022 del *Forum* P.A. "Il Paese che riparte. Insieme per una sfida condivisa" dedicata alla formazione ed alla condivisione di *best practice* della p.a. e delle imprese innovative, svoltasi a Roma dal 14 al 17 giugno presso il Centro Congressi *Auditorium* della Tecnica e *online* sulla piattaforma diretta del *Forum*. I temi guida sono stati: investimenti e riforme del Pnrr, programmazione europea, tecnologie e nuovi paradigmi della trasformazione digitale, *governance*. Nell'ambito della manifestazione, sono stati messi a disposizione degli utenti una serie di volantini informativi, realizzati dall'Ufficio, su diverse tematiche relative alla protezione dei dati personali, alla sicurezza informatica e all'educazione digitale.

Ad ottobre è stata altresì firmata la convenzione triennale tra il Garante e la Rai volta a rafforzare e diffondere una conoscenza più consapevole dei diritti fondamentali della persona, delle tutele riconosciute agli individui e degli strumenti da utilizzare per difendersi.

La collaborazione si realizzerà attraverso progetti e azioni comuni dedicate ai temi della *privacy*, attraverso una pluralità di strumenti editoriali – dalla *fiction*, ai programmi di intrattenimento, ai momenti di informazione – e di soluzioni televisive e tecnologiche ritenute più adatte.

Nel mese di novembre è stato avviato, con il supporto tecnico di Skuola.net, la progettazione del *contest* dedicato alle scuole: "Gira un video e diventa 'ambasciatore' della *privacy*", per sensibilizzare insegnanti e studenti sui temi della protezione dati, attraverso un percorso formativo predisposto dal Garante da svolgere nelle ore di educazione civica. Il *contest*, destinato agli studenti delle scuole secondarie di secondo grado pubbliche e private che frequentano le classi I e II nell'anno scolastico 2022-2023, ha messo in palio donazioni fino a 3.000 euro, da destinare all'acquisto di dispositivi tecnologici utili alla didattica degli istituti che realizzeranno i migliori video sulla tutela della riservatezza e sui rischi derivanti da un utilizzo non corretto degli strumenti accessibili in internet.

23.2. *I prodotti informativi*

Nel corso del 2022 sono stati diffusi 71 comunicati stampa e 13 *Newsletter*.

La *Newsletter* del Garante è una pubblicazione periodica, registrata al Tribunale di Roma, giunta al XXIV anno di diffusione (per un totale di 498 numeri e 1.695 notizie). È inviata in via telematica a redazioni, professionisti, amministrazioni pubbliche, imprese e semplici cittadini che ne fanno esplicita richiesta o si iscrivono *online* alla *Newsletter* sul sito dell'Autorità, per divulgare i più importanti provvedimenti adottati, rielaborati in chiave giornalistica, l'attività in ambito nazionale, europeo ed internazionale nonché le molteplici iniziative legate alla protezione dei dati personali e alla tutela dei diritti fondamentali.

Sul sito è possibile consultare l'archivio tematico che raccoglie, divisi per categorie, tutti gli articoli e i comunicati stampa prodotti dall'Ufficio.

23

Nell'ambito dell'attività di divulgazione occorre menzionare le 11 uscite del GPDPDigest, il *magazine online* del Garante che raccoglie mensilmente i principali interventi dell'Autorità nonché una sintesi delle principali attività di *European Data Protection Board* e *European Data Protection Supervisor*.

23.3. *Il sito istituzionale, i prodotti multimediali e le pubblicazioni*

Nel 2022 è stato incrementato il numero e la varietà di prodotti di comunicazione specificatamente ideati per la diffusione sul web e sui *social media*. Quasi tutti i *format* e contenuti sono stati ideati e sviluppati *in house* dall'Ufficio, che ha curato le fasi creative, progettuali e redazionali. Tra i temi trattati la sensibilizzazione sull'importanza della protezione dei dati, l'educazione digitale, l'informazione sui rischi e sulle buone pratiche nel campo della cybersicurezza, la conoscenza dei diritti e dei principali adempimenti previsti dalla normativa in materia di protezione dei dati personali. Un grande investimento è stato profuso soprattutto nella realizzazione di *clip* video, particolarmente utili all'implementazione di una strategia sempre più votata ai *social media*. Nel 2022 ne sono stati realizzati 25 *in house* (tra cui interviste, *teaser*, video informativi, montaggi e rielaborazione di eventi), cui si aggiungono 9 *spot* video da 30" e 9 *spot* da 60" realizzati con l'aiuto di una società specializzata e destinati alla diffusione su *social media*, web e canali televisivi.

La pubblicazione di contributi sui profili *social media* dell'Autorità (su LinkedIn, YouTube, Telegram, Instagram e Twitter) è cresciuta in modo cospicuo, similmente alla crescita del numero di *followers*, che ha raggiunto le 81.079 unità.

Il sito web è stato arricchito con un numero elevato di contenuti (oltre 1.900 nell'anno) e di interventi sull'*home page*, il cui *design* è stato aggiornato per migliorare la fruibilità e ricerca degli utenti.

Nell'anno di riferimento sono state realizzate 11 infografiche funzionali a rendere gradevoli e comprensibili testi spesso complessi e non privi di criticità. Un grosso investimento progettuale è stato effettuato per la realizzazione di nuove e importanti campagne informative (9 nell'anno) sia sui canali web e *social media* dell'Autorità, sia su quelli televisivi e radiofonici della Rai, nonché attraverso affissioni digitali in alcuni importanti aeroporti.

Su tutte le questioni sulle quali il Garante è intervenuto i *media* hanno posto sempre una costante attenzione. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali, delle testate *online* e *blog* che hanno trattato i temi legati alla *privacy* sono state 6.516, quelle relative all'attività del Garante 4.156. Gli articoli aventi per oggetto interviste, interventi e dichiarazioni del Garante sono stati 219 su stampa e web, mentre 56 su radio e tv. Si contano, infine, 1.180 articoli relativi ai comunicati stampa e 490 relativi agli argomenti delle *Newsletters*.

Per il settore editoriale si è curata la realizzazione del libro "La *privacy* dell'era digitale. Le relazioni dei presidenti dell'Autorità Garante 1997-2022" che andrà ad aggiungersi alla già ricca collezione dell'Autorità.

23.4. *Le manifestazioni e convegni*

A partire dal 2007, promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le autorità europee per la *privacy*, il 28 gennaio di ogni anno viene celebrata la Giornata europea per la protezione dei dati personali,

per sensibilizzare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali.

Il Garante ha dedicato la giornata europea 2022 ai minori, che, oltre a essere tra i soggetti più vulnerabili della società, ne rappresentano anche il futuro.

Il Convegno, intitolato "Visibili o sorvegliati? La vita nella Rete", si è svolto in presenza ed in diretta *streaming* presso il convitto nazionale Vittorio Emanuele II di Roma ed ha visto protagonisti oltre 60 studenti. I Componenti del Garante sono intervenuti su importanti temi quali i social *network*, il *revenge porn*, il cyberbullismo. Ma sono stati innanzitutto i ragazzi ad essere chiamati ad esprimere le proprie considerazioni, ad esporre le proprie esperienze e a fare domande sulla *privacy online*. Nel corso del convegno sono stati proiettati i video informativi realizzati dal Garante per sviluppare la consapevolezza dei più giovani sull'uso della rete e promuovere l'educazione civica digitale. La Giornata europea è stata anche l'occasione per illustrare i dati del sondaggio commissionato dall'Autorità a Skuola.net sul grado di attenzione alla difesa della *privacy*, soprattutto *online*, da parte dei più giovani. La ricerca è stata effettuata attraverso la raccolta di un questionario compilato da 2.600 ragazzi tra gli 11 e i 24 anni (doc. web n. 9740438).

Il 7 luglio, alla presenza di Ministri, rappresentanti del Parlamento, delle Istituzioni, dell'imprenditoria e delle associazioni di categoria è stata presentata la Relazione annuale sull'attività svolta nel 2021. L'evento è stato trasmesso in diretta tv ed in *streaming* sul sito web istituzionale.

Nel corso dell'anno, il Presidente e i componenti del Collegio hanno infine partecipato a numerosi eventi, convegni e giornate di studio, di rilievo nazionale ed internazionale.

23.5. *L'attività internazionale*

L'Autorità ha altresì svolto numerose riunioni a distanza e molteplici funzioni intermedie di coordinamento, accanto al gruppo di comunicatori istituito presso l'EDPB per realizzare attività coordinate di comunicazione, con la condivisione, tra l'altro, di comunicati stampa e la gestione comune dei casi con valenza transnazionale dei quali si riferisce nel par. 21.4.

23.6. *L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi*

Nel corso del 2022 il Servizio relazioni con il pubblico ha continuato a promuovere la conoscenza delle tematiche connesse alla disciplina sulla protezione dei dati personali e contestualmente a svolgere una funzione di "filtro", curando, laddove possibile, il diretto riscontro delle richieste di chiarimenti. In tale ottica si è data visibilità all'attività dell'Autorità, garantendo al cittadino sia la possibilità di partecipare e di accedere alle diverse fasi procedimentali, espressamente regolamentate, sia il costante aggiornamento sulle tematiche di interesse dell'Autorità.

Dal mese di maggio 2022 è stato ripristinato il ricevimento del pubblico precluso durante la pandemia nel rispetto della normativa emergenziale.

Nel periodo in esame è stato notevole l'incremento di richieste di informazioni specifiche riferibili all'interpretazione e al coordinamento tra la normativa di settori peculiari e la protezione dei dati personali, in particolare in ambito sanitario, lavorativo e scolastico sia nel settore privato che pubblico.

L'interesse degli utenti rispetto a tali temi è dimostrato dai dati numerici relativi

23

ai contatti con il Servizio, che ammontano in totale a 16.464 di cui 12.154 *e-mail*, 270 fascicoli, circa 4.000 via telefono e 40 visitatori in sede a partire dalla predetta apertura al pubblico (cfr. parte IV, tab. 15).

Nella gestione di tutte le richieste il Servizio ha avuto cura di conciliare l'efficienza, la professionalità e una aggiornata conoscenza giuridica delle questioni esaminate, con cortesia e tempestività tramite riscontri spesso dirimenti, forniti peraltro in tempi molto rapidi, nonostante l'elevatissimo numero di istanze.

Ai fini del potenziamento degli strumenti informativi a disposizione del pubblico, alla luce delle questioni maggiormente segnalate e dell'evoluzione della normativa, sono state predisposte note dedicate a specifiche tematiche allo scopo di fornire riscontro alle richieste degli utenti. È stata inoltre predisposta e pubblicata sul sito dell'Autorità e sui canali *social* una scheda informativa che illustra, in modo dettagliato, caratteristiche, differenze e modalità di impiego degli strumenti di tutela a disposizione dell'interessato previsti dalla normativa in materia di protezione dei dati personali, in particolare sulla segnalazione e il reclamo.

A seguito inoltre dell'attivazione, a partire dalla metà del mese di febbraio 2022 (in adempimento a specifiche previsioni del Cad, dettagliate dalle più recenti linee guida AgID sui documenti informatici), del meccanismo di risposta automatica al cittadino generata dal sistema di protocollo informatico, è stata predisposta una nota di riscontro con la quale si richiede ai corrispondenti di rispedire i messaggi agli indirizzi *e-mail* istituzionali dell'Autorità pubblicati nell'Indice delle pubbliche amministrazioni (Ipa).

Tra le attività ordinarie e di supporto agli utenti (cittadini, aziende, scuole, enti, ecc.), va anche evidenziata l'assistenza alle istanze concernenti i servizi telematici di segnalazione di comunicazioni indesiderate, di *data breach* e di comunicazione dei dati di contatto del Rpd, in coordinamento con il Dipartimento tecnologie digitali e sicurezza informatica.

Si è rilevato infatti un forte incremento delle richieste di informazioni sulla comunicazione dei dati di contatto del Rpd e sulla modalità *online* di segnalazione di comunicazioni indesiderate.

Segnalazioni su eventuali anomalie riscontrate nei moduli *online* e richieste sul miglioramento/funzionamento del sito ufficiale sono state riscontrate in autonomia o, se del caso, in collaborazione con il Servizio relazioni esterne e *media* nonché il Dipartimento tecnologie digitali e sicurezza informatica.

Tematiche d'interesse

Tra le tematiche di carattere generale si segnalano quelle concernenti le forme di tutela (circa 1.250 *e-mail* ricevute) e quelle relative gli adempimenti previsti dal RGPD (in particolare oltre 1.600 *e-mail* hanno riguardato la designazione del Rpd e la procedura *online* realizzata dal Garante per la comunicazione dei dati di contatto dello stesso).

Altre questioni hanno riguardato i trattamenti di dati personali in ambito lavorativo pubblico e privato (circa 350 *e-mail*); la videosorveglianza in ambito privato, lavorativo e scolastico (oltre 500 *e-mail*); i trattamenti di dati personali nell'ambito della rete internet e dell'utilizzo di Google Analytics, dei *social network* e delle *app*, nonché in ambito giornalistico, con particolare riferimento alle richieste di deindicizzazione dei dati personali dai motori di ricerca, volte all'esercizio del diritto all'oblio di cui all'art. 17 del RGPD (circa 700 *e-mail*); il trattamento dei dati sanitari anche a seguito dell'allentamento delle misure adottate per il contrasto del Covid-19, nonché per finalità di cura e ricerca scientifica (oltre 500 *e-mail*).

Si è "riaccesa" l'attenzione da parte dei cittadini sul fenomeno del *telemarketing*, anche in considerazione dell'emanazione del d.P.R. 27 gennaio 2022, n. 26, che ha esteso il funzionamento del Rpo anche alle numerazioni non presenti negli elenchi

telefonici pubblici, cellulari inclusi, secondo quanto previsto dalla legge 11 gennaio 2018, n. 5. Numerose richieste (oltre 800 *e-mail*) hanno riguardato le nuove funzionalità del Rpo e la perdurante ricezione di telefonate di disturbo, nonostante l'iscrizione.

È stato inoltre fornito pronto riscontro, a molteplici richieste relative a fascicoli assegnati ad altre Unità (per oltre 900 *e-mail*) previe le opportune verifiche con l'Ufficio protocollo.

24 Attività di studio e documentazione

Attività di studio, documentazione e supporto giuridico

L'attività di studio e ricerca ha riguardato molteplici questioni tecnico-giuridiche sulle materie di interesse, anche oggetto di rinvio pregiudiziale alla Corte di giustizia dell'Unione europea.

Particolari approfondimenti sono stati svolti tra l'altro in materia di esercizio del diritto dell'interessato ad accedere ai propri dati trattati mediante algoritmi, e sullo svolgimento dei procedimenti sanzionatori.

In ragione dei profili di interesse e delle criticità sussistenti in materia di protezione dei dati personali, sono state seguite, anche nel 2022, con particolare attenzione l'evoluzione giurisprudenziale e dottrinale dell'accesso documentale e dell'accesso civico generalizzato, la cui procedura prevede la richiesta di parere al Garante da parte dei Responsabili della prevenzione della corruzione e della trasparenza nonché dei difensori civici (cfr. par. 4.4.3).

In continuità con il lavoro svolto da diversi anni, è stato curato un Osservatorio ad uso interno con cadenza mensile quale documentazione di sintesi del costante monitoraggio della normativa, giurisprudenza e dottrina nazionale ed eurounitaria in materia di protezione dati, unitamente ad approfondimenti su questioni o settori specifici.

Anche attraverso il menzionato Osservatorio sono stati resi diversi approfondimenti tematici, spesso in occasione della pubblicazione di sentenze provenienti da giurisdizioni europee e nazionali.

A titolo meramente esemplificativo si menzionano, in ragione delle dirette implicazioni in materia di protezione dati, la questione della legittimità di un ordine di deindicizzazione globale nei confronti di un motore di ricerca (Cass. civ., ord. n. 34658/2022), collegata a quella del diritto all'oblio (Cass. civ., 8 febbraio 2022, n. 3952; Cass. civ., ord. 28 marzo 2022, n. 9923; Cass. civ., ord. 30 agosto 2022, n. 25481; Cass. civ., ord. 24 novembre 2022, n. 34658); quella relativa alla responsabilità dell'*hosting provider* (C.d.S., ord. 27 gennaio 2021, n. 592; Cass. civ., ord. 8 giugno 2022, n. 18430; C.d.S., 13 settembre 2022, n. 7949); quella della conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione afferenti alle comunicazioni elettroniche per finalità di lotta ai reati gravi (*data retention*) (CGUE Grande Sezione 5 aprile 2022 C-140/20; Grande Sezione della Corte di giustizia 20 settembre 2022 cause riunite C-793/19 e C-794/19; Grande Sezione della Corte di giustizia 20 settembre 2022 cause riunite C-339/20 e C- 397/20); quella della trascrivibilità dell'atto di nascita di un minore nato, attraverso la tecnica della maternità surrogata, in un Paese extracomunitario o in Italia (Cedu, 22 novembre 2022 affaire D.B. et autres c. Suisse nonché, in ambito nazionale, Cass. civ., ord. 13 luglio 2022, n. 22179 e l'ord. 22 gennaio 2022, n. 1842 con la quale la Cass. civ. è tornata a chiedere in tale materia una pronuncia delle Sezioni Unite).

Relazione annuale

In attuazione della normativa nazionale ed europea (cfr. artt. 154, comma 1, lett. *e*), del Codice nonché 59 del RGPD) è stata curata la redazione del testo della Relazione annuale, volta a rendere conto, anzitutto al Parlamento e al Governo, dell'attività svolta dall'Autorità. La struttura della Relazione, che presenta tradizionalmente una parte generale e molteplici sezioni tematiche (ivi comprese quelle contenenti dati di natura statistica), agevola la rapida e sintetica consultazione

di informazioni puntuali in particolare con riguardo all'attività provvedimentale, sanzionatoria e comunicativa, nonché all'ambito europeo ed internazionale.

In conformità a quanto previsto dall'art. 22, d.l. n. 90/2014 convertito in legge 11 agosto 2014, n. 114, la Relazione annuale del Garante (non diversamente da quella delle altre autorità amministrative indipendenti) è stata altresì trasmessa alla Corte dei conti.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

L'Ufficio del Garante

RELAZIONE ANNUALE
2022

III - L'Ufficio del Garante

25 La gestione amministrativa e dei sistemi informatici

25.1. *Il bilancio e la gestione economico-finanziaria dell'Autorità*

L'attività amministrativa si è svolta nel corso dell'esercizio sulla base del bilancio di previsione, avente carattere autorizzatorio, ed in coerenza con gli obiettivi programmatici approvati dal Garante.

L'intera gestione è stata improntata ad una attenta acquisizione delle entrate ed all'osservanza di generali principi di una prudente programmazione delle spese, nel rispetto delle specifiche disposizioni legislative e regolamentari in materia di contabilità pubblica applicabili all'Autorità.

Le fonti di finanziamento sono costituite in misura largamente prevalente da trasferimenti erariali che il legislatore rende disponibili per consentire il corretto funzionamento della struttura e l'espletamento delle molteplici attività attribuite all'Autorità sia da norme nazionali che da disposizioni adottate dai competenti organismi dell'Unione europea.

In tale contesto, nel corso del 2022 il Garante ha potuto beneficiare, oltre alle risorse finanziarie parametrate alle correnti esigenze gestionali, di trasferimenti aggiuntivi quantificati sulla base di un incremento dell'organico e per esigenze perequative, in ragione di ulteriori competenze attribuite dal legislatore alla stessa Autorità.

La legge di bilancio 30 dicembre 2021, n. 234 ha previsto, infatti, un finanziamento complessivo di oltre 36,2 milioni di euro, il cui importo si è sommato al trasferimento di 8,4 milioni di euro previsto nell'ambito della modifica delle attività e dell'incremento del personale che il Garante è stato autorizzato ad attuare dalla legge 3 dicembre 2021, n. 205, di conversione del d.l. 8 ottobre 2021, n. 139.

Per effetto di tali disposizioni legislative il 2022 ha fatto registrare l'acquisizione di entrate da trasferimenti erariali per complessivi 44,6 milioni di euro, con un incremento di oltre 8,9 milioni di euro rispetto al precedente esercizio finanziario, in relazione ai nuovi compiti e alle funzioni aggiuntive da svolgere, e, quindi, al conseguente potenziamento della struttura.

Va evidenziato, tuttavia, che l'onere posto a carico del bilancio dello Stato per assicurare il corretto funzionamento dell'Autorità risulta mitigato dalle somme acquisite direttamente alle casse erariali per effetto di pagamenti conseguenti all'attività sanzionatoria curata dal Garante nell'espletamento dei propri compiti istituzionali.

La complessiva gestione è stata assoggettata ai controlli dell'organo interno preposto alla verifica della regolarità amministrativo-contabile, che non ha rilevato irregolarità.

25

Il rendiconto della gestione è stato trasmesso alla Corte dei conti, nel rispetto di puntuali disposizioni legislative, per le verifiche di competenza.

Sotto il profilo più strettamente contabile, il risultato finanziario dell'esercizio ha fatto registrare un avanzo di amministrazione di 11,1 milioni di euro, determinato da una dinamica della spesa più contenuta rispetto alle previsioni, in ragione di una politica gestionale volta a valorizzare ed ottimizzare l'impiego delle risorse erariali.

Inoltre, le procedure per l'immissione in servizio del nuovo personale, previsto con l'incremento della pianta organica, hanno richiesto tempi di selezione che non si sono esauriti nell'ambito di un solo esercizio e tale circostanza ha contribuito ad una contrazione della spesa rispetto alle risorse disponibili con effetti positivi sul risultato della gestione finanziaria.

Nel 2022, al netto delle partite di giro pari a 10 milioni di euro, le entrate acquisite dall'Autorità, comprensive dei trasferimenti a carico del bilancio dello Stato, sono state di complessivi 45,3 milioni di euro a fronte delle quali sono stati registrati impegni di spesa per 34,2 milioni di euro.

L'importo delle risorse finanziarie acquisite è quantificato annualmente nell'ambito della legge di bilancio. Ulteriori importi, meno significativi, derivano da contributi per l'espletamento di attività disciplinati nell'ambito di apposite convenzioni, nonché da rimborsi di varia natura erogati da amministrazioni nazionali ed organismi dell'Unione europea.

Rispetto al precedente esercizio finanziario, l'incremento delle entrate complessive registrato nel 2022 è stato di 9,3 milioni di euro, con una variazione di circa il 26 per cento.

Con riferimento alla spesa, invece, gli oneri registrati nell'anno, pari a 34,2 milioni di euro, risultano in aumento di 7,9 milioni di euro rispetto al 2021, con uno scostamento di circa il 30 per cento.

La spesa complessiva è da imputare in massima parte alla gestione corrente, nella misura di 33,7 milioni di euro, mentre la parte residuale 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 2022 la struttura della spesa fa emergere, come per il passato ed in analogia alla generalità delle altre autorità amministrative indipendenti, una significativa incidenza degli oneri del personale rispetto alla spesa complessiva per il funzionamento.

L'indennità di carica riconosciuta al presidente ed ai componenti del Collegio del Garante è stata definita nei limiti e sulla base di parametri specificati dalla legge ed alla relativa erogazione l'Ufficio ha provveduto nel rispetto dei vincoli e delle prescrizioni vigenti.

Con riferimento, infine, agli oneri strettamente connessi alle esigenze gestionali, l'Autorità ha curato il rispetto dei limiti di legge.

Si rinvia alla sez. IV, tab. 18 per una sintetica illustrazione dei valori della gestione finanziaria suddivisa tra entrate e spese correnti, in conto capitale e per meri trasferimenti. I relativi importi sono posti a raffronto con i corrispondenti valori del precedente esercizio finanziario in modo da evidenziare i rispettivi scostamenti, sia in valore assoluto che in termini percentuali.

25.2. *L'attività contrattuale, la logistica e la manutenzione dell'immobile*

Anche nel 2022, come nel biennio precedente, in vigenza di normative di carattere emergenziale, volte a snellire l'azione amministrativa, l'Autorità ha fatto ricorso, ove

possibile, a procedure comparative di affidamento, adoperando gli strumenti di acquisto e negoziazione messi a disposizione da Consip spa.

Ciò ha consentito di continuare ad applicare con rigore i principi fondamentali del codice dei contratti pubblici, ed in particolare quelli di rotazione delle imprese affidatarie e di concorrenza tra le stesse, come dimostrato dall'ampia diversificazione dell'identità delle ditte contraenti, anche in corrispondenza di affidamenti di modesto importo.

Nel corso del 2022 sono proseguite, analogamente all'anno precedente, alcune peculiari difficoltà derivanti dalle note vicende internazionali, che hanno comportato in alcuni casi significativi ritardi nelle consegne di beni, a causa della scarsità della relativa componentistica (ad es., stampanti, gruppi di continuità); in altri, l'incremento dei prezzi, connesso ai costi dell'energia e delle materie prime (ad es. fornitura di carta in risme). Un'ulteriore difficoltà è derivata dalla temporanea chiusura del Portale acquisti in rete di Consip, per attività di aggiornamento e reingegnerizzazione dello stesso, cui è seguito un periodo, invero inatteso e non prevedibile, di difficoltosa operatività dello stesso.

Programmazione

In materia di programmazione biennale degli acquisti di beni e servizi, l'Autorità, dopo un'intensa attività di raccordo delle informazioni, ha acquisito i fabbisogni d'acquisto con le relative verifiche delle coperture finanziarie, per approvare il programma degli acquisti per il biennio 2023-2024.

Procedure di affidamento

L'ambito merceologico in cui si è esplicata la maggior parte dell'attività negoziale dell'Ufficio è stato quello del settore *hardware*/*software*, anche a seguito dell'aumentata consistenza della dotazione organica e della contemporanea adozione dei provvedimenti volti a dare stabilità alla modalità di lavoro da remoto. Tra le acquisizioni di beni e servizi afferenti al settore informatico possono essere ricordati i servizi in adesione ad Accordi quadro SPC *Cloud,* l'affidamento del servizio di supporto sistemistico *on site* – che contribuisce a garantire la necessaria operatività dei servizi tecnologici anche per i lavoratori che operano da remoto – i servizi di sicurezza, di *cloud backup,* assistenza sistemistica, noleggio stampanti, reti locali ed altri come Pec e firme digitali. È stata inoltre aggiudicata, a seguito di procedura comparativa informale, la fornitura del *software* per la gestione degli appalti dell'Autorità, ormai da tempo completamente digitalizzati in ottemperanza alle vigenti disposizioni.

Tra i contratti afferenti ad altri settori, stipulati mediante le Convenzioni o Accordi quadro Consip, il più rilevante per valore economico è stato quello relativo alla stipula del contratto con il nuovo aggiudicatario del lotto n. 7 della Convenzione Consip "Buoni pasto 9", risultato vincitore in un contenzioso con il precedente aggiudicatario. Sono stati altresì sottoscritti contratti esecutivi relativi ad altre forniture, come le *fuel card* o l'energia elettrica.

Nel quadro delle iniziative connesse al venticinquennale dell'istituzione dell'Autorità sono stati organizzati, in sinergia con il Servizio relazioni esterne e *media,* convegni ed eventi, sul territorio nazionale (Roma, Torino, Napoli), che hanno comportato l'affidamento di numerosi contratti di appalto.

Sul piano della comunicazione istituzionale e dell'informazione sono state svolte significative attività, anche in esecuzione di apposita Convenzione stipulata con il Mise nel mese di dicembre del 2021, quali la realizzazione di *spot* radio-tv in materia di *privacy* o di affissioni digitali presso aeroporti e stazioni ferroviarie; da segnalare anche, in materia di comunicazione, l'aggiudicazione del contratto per la gestione dell'*account* Twitter dell'Autorità, a seguito di procedura comparativa informale (cfr. par. 23.3).

È infine proseguito il 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. Nell'anno in esame è stato affidato un incarico di rappresentanza in giudizio.

La manutenzione dell'immobile

La sede degli uffici del Garante è condotta in locazione e l'Autorità non detiene immobili adibiti ad abitazione o foresteria. Nella prospettiva dell'implementazione, anche futura, della pianta organica, è stata avviata un'indagine di mercato per valutare eventuali manifestazioni di interesse concernenti la vendita ovvero la locazione di un immobile da destinare ad uso ufficio come propria sede istituzionale. Non sono però emerse proposte in linea con le esigenze dell'Autorità.

Per quanto attiene alla logistica e manutenzione dell'attuale immobile, sono state effettuate attività di adeguamento funzionale, miglioramento dei locali e inventario degli arredi, di concerto con la società proprietaria e con il Rspp dell'Autorità, che ha coadiuvato l'Ufficio al fine di assicurare il costante rispetto della normativa sulla sicurezza nei luoghi di lavoro e di prevenzione incendi in stretta collaborazione, ove necessario, con la società proprietaria. È stato inoltre adibito un magazzino idoneo alla custodia dei beni librari.

Tenuto conto dell'emergenza energetica registrata nell'anno, sono state attivate e curate le necessarie misure di contenimento della spesa energetica, nel rispetto delle direttive e delle disposizioni, anche comunali, diramate in materia.

25.3. *L'organizzazione dell'Ufficio*

Ha avuto avvio nel periodo di riferimento un processo di riordino complessivo dell'Ufficio per il miglior raggiungimento dei risultati programmati, secondo una linea strategica orientata, da un lato, a rafforzare l'organico, modernizzare e snellire l'attività lavorativa, dall'altro a valorizzare forme di collaborazione esterne in settori dell'ordinamento che si intersecano con la materia della protezione dei dati personali (es. lotta al cyberbullismo, sviluppo dell'intelligenza artificiale).

Il rafforzamento dell'Autorità

Con riguardo al reclutamento del personale, l'Autorità ha dato seguito alle attività destinate alla progressiva copertura della pianta organica, procedendo alla definizione ed alla successiva pubblicazione dei seguenti bandi di mobilità volontaria esterna: n. 9 posti di impiegato operativo (doc. web n. 9819229); n. 4 posti di dirigente con competenza specifica in materia di protezione dei dati personali (doc. web n. 9766540); n. 20 posti di funzionario con competenza specifica in materia di protezione dei dati personali (doc. web n. 9766554). L'Autorità ha altresì curato la predisposizione e la pubblicazione di sei bandi di concorso, rispettivamente per la copertura di n. 2 posti di funzionario area comunicazione (doc. web n. 9736591); n. 1 posto di funzionario, area comunicazione - *digital communication specialist* (doc. web n. 9736619); n. 2 posti nella qualifica di impiegato con profilo informatico-tecnologico, nell'ambito di una procedura svolta congiuntamente all'Anac (doc. web n. 9753853); n. 4 funzionari con profilo informatico-tecnologico nell'ambito di una procedura svolta congiuntamente all'Anac (doc. web n. 9753866); n. 20 posti di funzionario con competenze specifiche in materia di protezione dei dati personali (doc. web n. 9813756); n. 4 posti di dirigente con competenze specifiche in materia di protezione dei dati personali (doc. web n. 9813714). Nel corso del 2022 sono state selezionate e assunte con rapporto di lavoro a tempo pieno e indeterminato, n. 2 unità di personale con profilo professionale di esecutivo, qualifica commesso, rientranti tra i soggetti di cui all'art. 1, l. n. 68/1999, iscritti nell'elenco del collocamento mirato della Regione Lazio (doc. web n. 9754115). Sempre nel 2022, a seguito dell'espletamento delle relative prove concorsuali, è stato assunto n. 1 dirigente giuridico-internazionale (doc. web n. 9083307).

L'Autorità ha continuato ad adeguare le procedure interne alle disposizioni normative succedutesi per fare fronte alla situazione emergenziale, a partire dal d.l. 17 marzo 2020, n. 18, fino alle disposizioni in tema di certificazione per l'accesso ai luoghi di lavoro (cd. *green pass*). Sulla base dell'esperienza maturata nel periodo emergenziale, nel corso 2022 per regolare l'istituto del lavoro agile l'Autorità ha stipulato un accordo con le organizzazioni sindacali, in applicazione delle disposizioni normative vigenti, comprese quelle riguardanti i dipendenti con carattere di fragilità.

Lavoro agile

Con riferimento alla gestione delle relazioni sindacali, anche il 2022 è stato contrassegnato dal costante confronto con le organizzazioni sindacali su varie questioni negoziali, come la già evidenziata regolamentazione del lavoro agile, l'adeguamento delle tabelle stipendiali ed il piano sanitario a beneficio del personale dell'Autorità.

Relazioni sindacali

Relativamente alla sicurezza ed alla salute nei luoghi di lavoro, l'Autorità ha continuato a dare applicazione alle disposizioni previste dalla normativa in materia, avvalendosi della collaborazione del medico competente e del Rspp. Durante il periodo emergenziale l'Autorità ha definito ed attuato le misure di sicurezza anti-contagio per il contrasto e il contenimento della diffusione del virus Covid-19 nell'ambiente di lavoro. Si evidenzia in particolare che, a seguito della stipula di specifica convenzione con il Policlinico militare del Celio, l'Autorità ha assicurato al proprio personale un presidio in sede con l'effettuazione, a cadenza settimanale, di tamponi molecolari. Sul piano della sorveglianza sanitaria, l'Autorità, anche nel periodo pandemico, ha sempre garantito le visite mediche a tutela della salute del proprio personale, secondo le tempistiche e le modalità stabilite dal decreto legislativo 9 aprile 2008, n. 81. È stata effettuata la consueta riunione periodica prevista dall'articolo 35 del citato decreto legislativo n. 81/2008 e, nel mese di dicembre, ha avuto luogo la prova di evacuazione dalla sede. Per assicurare le migliori condizioni di sicurezza all'interno della sede è stato incrementato il numero delle unità componenti le squadre di primo soccorso e di antincendio.

Sicurezza sul lavoro

Le attività di formazione si sono svolte avvalendosi dell'offerta formativa continua della Scuola nazionale dell'amministrazione (Sna), il cui catalogo è costantemente aggiornato anche grazie al lavoro svolto dal Club dei formatori della medesima Scuola, progetto al quale l'Autorità partecipa da diversi anni con l'obiettivo di migliorare le metodologie di rilevazione del fabbisogno formativo del proprio personale secondo criteri di efficienza ed adeguatezza.

Formazione del personale

Con riguardo, infine, ai percorsi formativi obbligatori in tema di salute e sicurezza nei luoghi di lavoro, di cui al d.lgs. n. 81/2008, nel 2022 sono stati effettuati interventi di aggiornamento a carattere generale a beneficio della quasi totalità del personale dell'Autorità, anche mediante l'utilizzo di piattaforme formative *online*. Sono stati altresì erogati i percorsi specifici destinati al personale individuato per le squadre di primo soccorso, antincendio ed utilizzo dei defibrillatori, installati in numero adeguato presso la sede dell'Ufficio.

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.

Servizio controllo di gestione

La Responsabile per la protezione dati (Rpd) ha svolto le attività di competenza in relazione sia alle attività di supporto al titolare del trattamento sia a quelle di vigilanza previste dall'art. 39 del Regolamento, fornendo, tra l'altro, riscontro alle questioni di interesse interno all'Autorità e alle richieste di origine esterna. L'intensificarsi delle iniziative svolte dall'Autorità in adempimento al mandato istituzionale a questa conferito ha inevitabilmente comportato, rispetto allo scorso anno, un netto e

Rpd

significativo intensificarsi delle attività attribuite alla figura del Rpd. Con delibera 27 gennaio 2022 il Collegio ha approvato l'aggiornamento del registro delle attività di trattamento ai sensi dell'art. 30 del Regolamento: nel finalizzare tale attività, la Rpd ha coadiuvato le unità organizzative nella raccolta e strutturazione delle informazioni obbligatorie di cui al citato art. 30 nonché di quelle ritenute ulteriormente necessarie a caratterizzare in maniera idonea le categorie delle attività di trattamento svolte sotto la responsabilità del titolare. È stata inoltre curata l'attività di supporto alle reti dei Responsabili della protezione dei dati. In particolare, nell'ambito della EDPB-DPO *Network* (la rete dei Dpo/Rpd delle autorità di protezione dati europee costituita nell'ambito Cepd) si è contribuito alle diverse iniziative tese a identificare, nel rispetto dell'autonomia decisionale delle autorità di protezione dati degli Stati membri, un approccio unitario alle questioni più rilevanti. Per quanto concerne la rete nazionale dei Rpd delle autorità indipendenti, è stato offerto un significativo supporto alla condivisione di conoscenze ed al consolidamento degli indirizzi e delle pratiche operative di competenza. Costante è stato inoltre il monitoraggio della casella di posta istituzionale della Rpd a cui pervengono istanze di diversissima natura ed oggetto, che costituisce un rilevante adempimento istituzionale relativo ad un punto di contatto per l'esercizio dei diritti dell'interessato, come disposto dal Regolamento ed esplicitato nell'informativa sul sito del Garante.

25.4. *"Autorità trasparente" e adempimenti relativi alla disciplina anticorruzione*

L'Autorità ha continuato a dare attuazione alla disciplina di trasparenza dotandosi, con il provvedimento 28 aprile 2022, n. 140, del Piano triennale di prevenzione della corruzione e della trasparenza 2022-2024 (doc. web n. 9765649) ed alimentando la sezione "Autorità trasparente" del sito web istituzionale: in particolare, al suo interno è stata pubblicata la griglia di rilevazione di cui all'all. 2 della delibera Anac 13 aprile 2022, n. 201 (doc. web n. 9785708) che il Responsabile della prevenzione della corruzione e della trasparenza (Rpct), in assenza di Oiv o strutture equivalenti presso l'Autorità, è tenuto a pubblicare, mentre è prevista dopo la data di riferimento di questa Relazione la pubblicazione della relazione annuale del Rpct per l'anno 2022.

Dando continuità all'attuazione delle misure generali, nel 2022 sono state intraprese le attività prodromiche all'adozione del nuovo Piano triennale di prevenzione della corruzione e della trasparenza (Ptpct), considerato che le autorità amministrative indipendenti non sono tenute all'adozione del Piao (cfr. gli "Orientamenti per la pianificazione anticorruzione e trasparenza 2022" formulati dall'Anac nel documento del 2 febbraio 2022 (in particolare alle pp. 3-4) e il Piano nazionale anticorruzione 2022, p. 26). Tali attività hanno visto il coinvolgimento di tutto il personale mediante la compilazione di apposite schede di rilevazione predisposte dal Rpct finalizzate alla realizzazione di una rinnovata mappatura dei processi in essere presso il Garante e dei relativi rischi.

A cura del Rpct sono stati altresì realizzati e distribuiti a quanti operano presso l'Autorità due *dossier* di approfondimento (ad uso interno) dedicati, rispettivamente, alla materia del "conflitto di interesse" e del *"pantouflage"*.

Infine, 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 (pari a quattordici); è pervenuta un'unica istanza di accesso civico relativa a dati a pubblicazione obbligatoria (ex art. 5, comma 1, d.lgs. n. 33/2013) della quale si è tenuto conto per aggiornare la tabella relativa ai compensi spettanti ai dirigenti riferita al 2021 (doc. web n. 9806246).

Il 2022 è stato ancora caratterizzato da intensa attività di gestione e sviluppo dei sistemi informativi.

Aggiornamenti funzionali o applicativi

Le principali attività hanno riguardato aspetti infrastrutturali, tecnologici, funzionali ed applicativi, con la configurazione di sistemi in dotazione a supporto del lavoro documentale dematerializzato e con il mantenimento e lo sviluppo dei sistemi a sostegno delle forme di lavoro agile e remoto adottati a seguito della emergenza pandemica.

I maggiori interventi hanno riguardato la digitalizzazione della procedura per la ricezione di comunicazioni da parte di soggetti esterni che si rivolgono al Garante in qualità di interessati o segnalanti con la configurazione di strumenti aggiuntivi per la gestione interna di tali segnalazioni.

Nel corso dell'anno sono stati, infatti, resi disponibili all'interno del portale dei servizi *online* i nuovi servizi telematici "segnalazione telefonate indesiderate" e "segnalazioni in materia d*i revenge porn*" includendo anche gli interessati nella platea di riferimento dell'utenza del portale. Con tali strumenti è stato possibile gestire efficacemente l'elevato numero di segnalazioni di telefonate indesiderate (circa 16.000 nel corso dei primi 40 giorni di attivazione del servizio) a seguito dell'ampliamento del Registro pubblico delle opposizioni alle utenze telefoniche mobili.

Per quanto riguarda altri aspetti funzionali o applicativi, sono state portate a compimento diverse attività di sviluppo e integrazione, tra cui lo sviluppo dei web *services* per l'integrazione nelle applicazioni *online* delle funzionalità del sistema di gestione documentale, l'automazione delle risposte alla ricezione della corrispondenza tramite protocollo informatico, la migrazione di test dei dati del vecchio registro delle violazioni oltre a vari sviluppi minori sull'applicativo di protocollo informatico, finalizzati a favorire una più efficiente gestione da parte degli operatori dell'Ufficio.

È stato inoltre sviluppato il sito web istituzionale con la realizzazione di un nuovo sistema di statistiche, la realizzazione di moduli *online* per l'iscrizione alle iniziative convegnistiche in occasione del 25° anniversario dell'istituzione dell'Autorità, la creazione di un archivio *offline* di *backup* del sito precedente (circa 15.000 documenti oltre a immagini e allegati) con dismissione del *server* precedentemente utilizzato. La gestione della sicurezza del sito ha comportato lo svolgimento di *penetration tests* e *security assessments* e un costante *change management* con l'aggiornamento della dichiarazione di accessibilità sul sito AgID.

È stata realizzata, per le finalità correlate allo *smartworking,* una nuova modalità di sottoscrizione di documenti informatici pdf, estendendo l'uso della firma digitale remota, aggiornando di conseguenza il manuale per la firma digitale in uso presso il Garante e il regolamento sull'uso dei dispositivi elettronici e dei sistemi informatici in lavoro agile elaborato all'inizio del 2020 per fare fronte all'emergenza pandemica.

È continuata la gestione delle utenze IMI secondo le nuove indicazioni del coordinatore nazionale IMI (NIMIC), per cui sono state eseguite specifiche e continue azioni per il mantenimento di utenze secondo stringenti *policy* di sicurezza.

Aggiornamenti infrastrutturali o di sicurezza

In merito ai profili infrastrutturali, sono state svolte diverse attività tra le quali, l'aggiornamento delle piattaforme *hardware* a supporto delle applicazioni *on premise*; il progetto di migrazione dell'infrastruttura verso servizi *cloud* IaaS; la realizzazione del *cloudbox* per la ricezione e la gestione sicura delle segnalazioni di *revenge porn*; l'attivazione di nuovi servizi di *backup* remoto e la realizzazione di una infrastruttura di *backup* immutabile per accrescere i livelli di sicurezza a fronte della diffusione di *ransomware*; l'*upgrade* del sistema di *collaboration* interno.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

I dati statistici

RELAZIONE ANNUALE
2022

IV - I dati statistici 2022

Tabella 1. Sintesi delle principali attività dell'Autorità

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	442
Pareri su norme di rango primario statale, delle regioni e delle autonomie	12
Pareri su atti regolamentari e amministrativi	69
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	24
Pareri ai sensi dell'art. 110 del Codice per la realizzazione di un progetto di ricerca medica, biomedica ed epidemiologica nonché ex art. 36 del RGPD	4
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	94
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché a seguito di accertamenti d'ufficio con contestuale ordinanza-ingiunzione	137
Provvedimenti collegiali a seguito di notifica di violazione di dati	6
Provvedimenti collegiali a seguito di notifica di violazione di dati con contestuale ordinanza-ingiunzione	12
Provvedimenti di approvazione di codici di condotta	1
Comunicazione di violazione dei dati	1.351
Riscontri a segnalazioni e reclami (art. 11, reg. Garante n. 1/2019)	9.218
Riscontri a quesiti (art. 11, reg. Garante n. 1/2019)	396
Risposte ad atti di sindacato ispettivo e di controllo	1
Audizioni del Presidente del Garante o memorie scritte trasmesse al Parlamento	9
Contatti Servizio relazioni con il pubblico	16.464
Accertamenti e controlli effettuati *in loco* (artt. 157-158, d.lgs. n. 196/2003)	140
Pagamenti derivanti dall'attività sanzionatoria	9.459.457
Comunicazioni di notizia di reato all'Autorità giudiziaria	5
Opposizioni (trattate) a provvedimenti del Garante	123
Ricorsi giurisdizionali trattati ex art. 152, d.lgs. n. 196/2003	70
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 1, d.lgs. n. 33/2013	1
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 2, d.lgs. n. 33/2013	14
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 RGDP)	317
Misure correttive e sanzionatorie (d.lgs. n. 51/2018)	2
Riunioni del Comitato europeo per la protezione dei dati personali	15
Partecipazione a sottogruppi di lavoro del Comitato europeo per la protezione dei dati personali	162
Riunioni e ispezioni autorità comuni di controllo/organismi di supervisione (Europol, SIS II, Dogane, Eurodac, VIS)	10
Conferenze internazionali	4
Riunioni presso l'OCSE e il CoE	12
Altre conferenze e incontri internazionali	13

Tabella 2. Attività di comunicazione dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	71
Newsletter	13
Prodotti editoriali	6
Campagne informative	10
Video *spot* e *teaser* informativi	32
Infonografiche e pagine tematiche	64

Tabella 3. Pareri ex art. 36, par. 4, del RGPD su norme di rango primario statale, delle regioni e delle autonomie

Pareri ex art. 36, par. 4, del RGPD su norme di rango primario statale, delle regioni e delle autonomie	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	3
Giustizia	1
Lavoro	3
Sanità	4
Trasporti	1
Totale	**12**

Tabella 4. Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi al Governo

Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi al Governo	
Temi	**Riscontri resi nell'anno***
Ambiente	2
Digitalizzazione p.a.	19
Diritti fondamentali	2
Fisco	6
Giustizia	2
Istruzione	4
Marketing	1
Sanità	6
Sanità: Covid-19	3
Settore privato	2
Trasporti	4
Totale	**51**

(*) inerenti anche ad affari pervenuti anteriormente al 2022

Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi ad altre Istituzioni	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	8
Fisco	5
Sanità	1
Statistica	4
Totale	**18**

Tabella 5. Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi ad altre Istituzioni

Misure correttive e sanzionatorie	
Avvertimenti a titolare/responsabile del trattamento (art. 58, par. 2, lett. *a*), del RGPD)	7
Ammonimenti a titolare/responsabile del trattamento (art. 58, par. 2, lett. *b*), del RGPD)	44
Ingiunzioni a titolare/responsabile del trattamento a soddisfare le richieste dell'interessato concernenti l'esercizio dei diritti riconosciuti dal RGPD (art. 58, par. 2, lett. *c*), del RGPD)	28
Ingiunzioni a titolare/responsabile del trattamento di conformare i trattamenti alle disposioni del RGPD (art. 58, par. 2, lett. *d*), del RGPD)	35
Ingiunzioni a titolare del trattamento di comunicare all'interessato una violazione dei dati personali (art. 58, par. 2, lett. *e*), del RGPD)	3
Imposizioni di limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento (art. 58, par. 2, lett. *f*), del RGPD)	25
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)	23
Sanzioni amministrative pecuniaria ex art. 83 (art. 58, par. 2, lett. *i*), del RGPD)	149
Ordine di sospensione dei flussi di dati verso un destinatario in un Paese terzo o un'organizzazione internazionale, ai sensi dell'art. 58, par. 2, lett. *j*), del RGPD	3
Totale	**317**

Tabella 6. Misure correttive e sanzionatorie (art. 58, par. 2, del RGPD)

Misure correttive e sanzionatorie	
Sanzioni amministrative pecuniarie (art. 42, d.lgs. n. 51/2018)	2
Totale	**2**

Tabella 7. Misure correttive e sanzionatorie (d.lgs. n. 51/2018)

Comunicazioni di notizia di reato all'Autorità giudiziaria	
Violazioni in materia di controlli a distanza dei lavoratori (art. 171, d.lgs. n. 196/2003)	3
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168, d.lgs. n. 196/2003)	2
Totale	**5**

Tabella 8. Comunicazioni di notizia di reato all'Autorità giudiziaria

Tabella 9. Pagamenti derivanti dall'attività sanzionatoria

Pagamenti derivanti dall'attività sanzionatoria	
Pagamenti spontanei dei contravventori	7.273.875,91
Riscossione coattiva	2.185.581,15
Totale	**9.459.457,06**

Tabella 10. Cooperazione tra autorità nazionali di protezione dei dati personali in IMI (Capo VII RGPD)*

Cooperazione tra autorità nazionali di protezione dei dati personali - procedure IMI (Capo VII RGPD)		
1) Decisioni finali adottate nell'ambito della attività di cooperazione rispetto alle quali il Garante ha agito in qualità di:		**222**
a)"autorità capofila" (LSA)	8	
b)"autorità interessata" (CSA)	214	
2) Procedure preliminari ex art. 56 del RGPD		**601**
a) Procedure preliminari pervenute rispetto alle quali l'Autorità si è dichiarata "autorità interessata"	370	
b) Procedure preliminari pervenute rispetto alle quali l'Autorità si è dichiarata "autorità non interessata"	180	
c) Procedure preliminari pervenute rispetto alle quali l'Autorità ha assunto il ruolo di "autorità capofila"	7	
d) Procedure preliminari pervenute rispetto alle quali l'Autorità ha fornito altro riscontro	4	
e) Procedure preliminari promosse dall'Autorità	4	
f) Altro	36	
3) Procedure di cooperazione ad impatto esclusivamente locale ex art. 56, par. 2, del RGPD		**0**
4) Procedure di cooperazione informale ex art. 60 del RGPD rispetto alle quali vi è stata una partecipazione dell'Autorità in qualità di:		**65**
a)"autorità interessata"	62	
b)"autorità capofila"	3	
5) Progetti di decisione ex art. 60 del RGPD rispetto ai quali l'Autorità ha cooperato in qualità di:		**235**
a1)"autorità interessata"	212	
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"	2	
6) Richieste di assistenza reciproca ex art. 61 del RGPD		**210**
a) ricevute da altre autorità	180	
b) inviate ad altre autorità	30	

Tabella 11. Procedure IMI nell'ambito del meccanismo di coerenza

Meccanismo di coerenza - procedure IMI (Capo VII RGDP)	
Procedure relative all'attività decisoria dell'EDPB per la risoluzione delle controversie ex art. 65 del RGPD con la partecipazione dell'Autorità	4
Procedure d'urgenza ex art. 66 del RGPD	1

*in relazione a procedure pervenute dal 01/01/2022

Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza	
Assicurazioni	8
Associazioni	2
Biometria	1
Concessionari	1
Credito	57
Dati in ambito pubblico	11
Dati in ambito sanitario	10
Diritto all'oblio	32
Imprese	181
Informazioni commerciali	1
Lavoro	8
Liberi professionisti	2
Libertà di espressione e di informazione	15
Notificazioni di violazione dei dati	79
Recupero crediti	7
RGPD	3
Reti telematiche	915
Sistema sanzionatorio	1
Trasferimento dati all'estero	1
Videosorveglianza	2
Altro	1
Totale	**1338**

Tabella 12. Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza

Segnalazioni e reclami		
	Pervenuti nell'anno	**Riscontri resi nell'anno (*)**
Attività ispettive	0	28
Affari legali e giustizia	163	119
Intelligenza artificiale	1	0
Libertà di manifestazione del pensiero e cyberbullismo	774	888
Realtà economiche e produttive	2.867	2.990
Realtà pubbliche	1.569	881
Reti telematiche e *marketing*	24.867	3.687
Sanità e ricerca	579	559
Tecnologie digitali e sicurezza informatica	60	66
Totale	**30.880**	**9.218**

Tabella 13. Segnalazioni e reclami

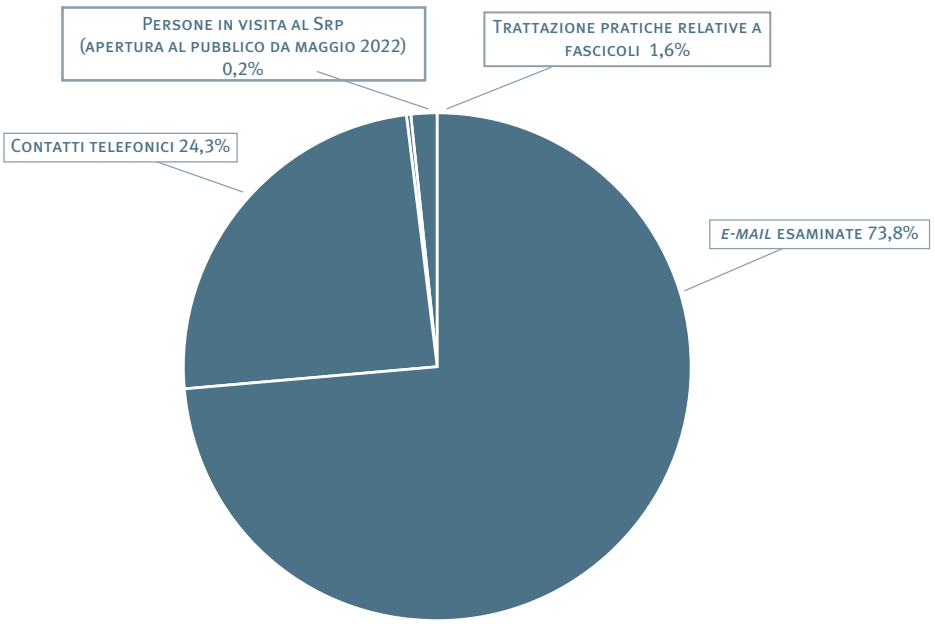
(*) inerenti anche ad affari pervenuti anteriormente al 2022

Tabella 14. Quesiti

Quesiti		
	Pervenuti nell'anno	**Riscontri resi nell'anno (*)**
Attività ispettive	1	2
Affari legali e giustizia	18	14
Libertà di manifestazione del pensiero e cyberbullismo	6	7
Realtà economiche e produttive	148	203
Realtà pubbliche	187	101
Reti telematiche e *marketing*	45	23
Sanità e ricerca	49	46
Tecnologie digitali e sicurezza informatica	3	0
Totale	**457**	**396**

Tabella 15. Servizio relazioni con il pubblico

Servizio relazioni con il pubblico	
E-mail esaminate	12.154
Contatti telefonici	4.000
Persone in visita al Srp (apertura al pubblico da maggio 2022)	40
Trattazione pratiche relative a fascicoli	270
Totale	**16.464**



(*) inerenti anche ad affari pervenuti anteriormente al 2022

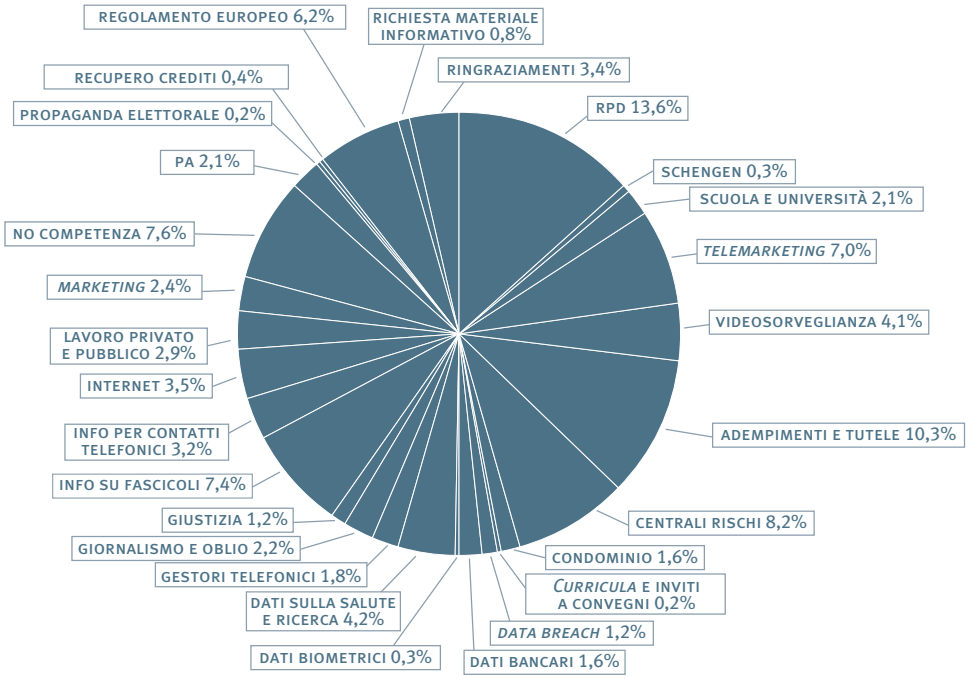


Grafico 16. Oggetto delle *e-mail* esaminate dal Servizio relazioni con il pubblico

Personale in servizio (*)				
Area	ruolo (a)	fuori ruolo (b)	comandato presso altre amm.ni o in aspettativa (c)	impiegato dall'Ufficio (a+b-c)
Segretario generale	0	1	0	1
Dirigenti	17	0	1	16
Funzionari	91	4	2	93
Operativi	25	0	0	25
Esecutivi	2	0	0	2
Totale	**135**	**5**	**3**	**137**
Personale a contratto (art. 156, comma 5, del Codice)				11

Tabella 17. Personale in servizio

Risorse finanziarie				
Entrate accertate	**Anno 2022**	**Anno 2021**	**Variazione**	
Entrate correnti	44.584.987	35.627.273	8.957.714	25,14%
Altre entrate, trasferimenti e rimborsi	726.554	342.242	384.312	112,29%
Totale entrate	**45.311.541**	**35.969.515**	**9.342.026**	**25,97%**
Spese impegnate	**Anno 2022**	**Anno 2020**	**Variazione**	
Spese di funzionamento	33.347.228	25.280.392	8.066.836	31,91%
Spese in c/capitale	448.728	624.459	-175.731	-28,14%
Trasferimenti ad amministrazioni	380.968	333.451	47.517	14,25%
Totale spese	**34.176.924**	**26.238.302**	**7.938.622**	**30,26%**

Valori in euro

Tabella 18. Risorse finanziarie

(*) Situazione alla data del 31/12/2022

Tabella 19. Attività internazionali dell'Autorità

Unione europea			
Comitato europeo per la protezione dati	**Sessioni plenarie**		18 gennaio
			10 e 22 febbraio
			14 marzo
			6 aprile
			4 e 12 maggio
			14 giugno
			12 e 28 luglio
			12 settembre
			10 ottobre
			14 novembre
			5 e 13 dicembre
	Riunioni dei sottogruppi	**Sottogruppo questioni strategiche e attività consultiva (SAESG)**	1° aprile
			7 giugno
			5 e 15 settembre
			21 ottobre
			14 novembre
		***Border Travel Law Enforcement* (BTLE)**	11 e 27 gennaio
			3 marzo
			7 aprile
			19 maggio
			7 luglio
			22 settembre
			27 ottobre
			24 novembre
		Cooperation	26 gennaio
			15 e 24 febbraio
			22 marzo
			26 aprile
			30 maggio
			22 giugno
			20 luglio
			21 settembre
			21 ottobre
			23 novembre
			15 dicembre
		Compliance, E-Government and Health	17 gennaio
			25 febbraio
			17 e 28 marzo
			8 e 21 aprile
			17-18 maggio
			10, 20, 29-30 giugno
			13 luglio
			14 settembre
			13-14 ottobre
			10 e 21 novembre
			19-20 dicembre

Riunioni dei sottogruppi	***Financial Matters***	9 febbraio
		3 e 18 marzo
		12 aprile
		19 maggio
		28 giugno
		4 luglio
		9, 13, 19 e 28 settembre
		22 novembre
		19 dicembre
	Cookie Banner Task Force	12 gennaio
		20 febbraio
		8 e 29 marzo
		13 aprile
		11 maggio
		17 giugno
		29 settembre
		28 ottobre
		12 dicembre
	Key Provisions	9 e 31 marzo
		31 maggio
		5 luglio
		27 settembre
		10 novembre
		9 dicembre
	International Transfers, BCR Session, Task Force on Supplementary Measures	25-26 gennaio
		4, 15-16 febbraio
		30 marzo
		20 aprile
		17-18 e 31 maggio
		7 giugno
		1 e 19 luglio
		8 settembre
		18-19 ottobre
		6-7 dicembre
	Technology	20 gennaio
		16-17 febbraio
		16 marzo
		7 aprile
		5 maggio
		2 giugno
		6-7, 11 e 15 luglio
		7 settembre
		19-20 ottobre
		9 novembre
		7 dicembre
	IT *Users*	29 marzo
		25 luglio
		20 settembre
		1° dicembre
	Enforcement	25 gennaio
		23 marzo
		24-25 maggio
		8, 20, 23 e 30 giugno
		5, 18-19 luglio
		20 settembre
		12-13 e 24-26 ottobre
		4, 7, 11, 15-17 e 21-22 novembre

Comitato europeo per la protezione dati	**Riunioni dei sottogruppi**	***Fining Task Force, Drafting Team (Guidelines on the calculation of administrative fines)***	9 e 25 marzo
			10 giugno
			24 novembre
		Task Force 101 Complaints	11 gennaio
			9 febbraio
			23 marzo
			20 aprile
			20 maggio
			22 luglio
			5 ottobre
			3 e 23 novembre
		Supplementary Measures Task Force	9 e 25 marzo
			10 giugno
			24 novembre
		Social Media Working Group	10 febbraio
			31 marzo
			5 maggio
			8 settembre
			20 ottobre
			8 dicembre
		Coordinated Enforcement Framework	19 gennaio
			10 febbraio
			24 marzo
			5 maggio
			23 giugno
			15 settembre
			20 ottobre
			8 dicembre
		EDPB DPO *Network*	27 gennaio
			27 aprile
			21 settembre
			30 novembre
		EDPB *Communications Network*	12 gennaio
			10 e 30 marzo
			6 maggio
			9 giugno
			16 novembre
		FATCA *Drafting Team*	5 luglio

Unione europea	
Gruppo di coordinamento della supervisione SIS II	1° giugno e 21 novembre
Gruppo di coordinamento della supervisione VIS	2 giugno e 22 novembre
Gruppo di supervisione del sistema Eurodac	2 giugno e 22 novembre
Gruppo di coordinamento della supervisione del sistema di informazione doganale: SID	1° giugno
Europol *Coordination Board*	31 maggio
Comitato di controllo coordinato (CSC)	6 luglio e 30 novembre

Riunione presso l'OCSE e CoE		
Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	**Comitato DGP *(Data Governance and Privacy in the Digital Economy)***	11 ottobre
	Gruppo di redazione sull'accesso dei governi ai dati personali del settore privato	3 febbraio 24 marzo 21-22 giugno 26 settembre 18-19 ottobre
Consiglio d'Europa	**Comitato Consultivo Convenzione n. 108/1981 (T-PD)**	16-18 novembre (plenaria)
	T-PD *Bureau*	23-25 marzo 21-22 settembre 15-16 dicembre
	***Committee on Artificial Intelligence* (CAI)**	4 aprile 21-23 settembre

Conferenze internazionali	
GPA (Conferenza internazionale delle autorità di protezione dati)	18-21 ottobre
***Spring Conference* (Conferenza di primavera delle autorità di protezione dati)**	19-20 maggio
***Privacy Symposium* 2022**	4-7 aprile
IWGDPT (Gruppo di Berlino)	28-30 novembre

Altre conferenze e *meeting*	
FINTECH **Incontro del Garante con i rappresentanti dell'*International Finance Corporation* (Gruppo Banca Mondiale), delle Banche centrali di diversi Paesi (Angola, Algeria, Stati dell'Africa centrale, Congo, Libia, Marocco, Tunisia, Ucraina) e dell'Autorità per la privacy angolana**	4 ottobre
GPA **Gruppo di lavoro in materia di intelligenza artificiale**	22 luglio 30 novembre
TAIEX ***(Technical Assistance and Information Exchange Instrument)*** **(Visita di studio presso il Garante di una delegazione dell'Autorità di protezione dati moldava)**	26-28 settembre
G7 dei Garanti per la protezione dei dati	7-8 settembre
Progetto ARC II	12 ottobre *(Kick-off meeting)* 29 novembre
European Case Handling Workshop	18-19 novembre
***Working Group 5* del JTC 21 del CEN CENELEC (ex CEN/CLC/TC8)**	28 giugno 4-5 luglio
***Working Group 5* del JTC 13 del CEN CENELEC (ex CEN/CLC/TC8)**	6 luglio
CPC-DPA **(Tavolo di lavoro relativo alla cooperazione fra autorità di protezione dati e autorità di tutela dei consumatori)**	2 maggio

IMPAGINAZIONE GRAFICA • STAMPA

TIBURTINI
CARATTERE TIPOGRAFICO

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

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il potere dell'innovazione e la solitudine digitale

La protezione dei dati a tutela della persona

Relazione del Presidente Pasquale Stanzione
2022

Roma, 6 luglio 2023

Signor Presidente della Camera,

Autorità,

Signore e Signori,

Tecnica e geopolitica

la relazione che oggi presento espone alcune delle sfide cui l'Autorità è stata chiamata nel corso di quest'anno, di particolare rilevanza sotto il profilo sociale, etico, giuridico, persino democratico; mentre altre, non meno importanti, iniziano a delinearsi con la forza delle grandi questioni epocali.

Si svolge oggi un'altra, non meno cruciale fase, di quella rivoluzione pacifica che Stefano Rodotà attribuiva all'introduzione delle prime norme sulla privacy in Italia.

Da allora, infatti, questa disciplina, adeguandosi progressivamente a una realtà in costante evoluzione, si è affermata come potente strumento di redistribuzione del potere informativo, di fronte al quale la persona rischia di divenire sempre più vulnerabile. E se ieri si trattava di "democratizzare" la privacy, emancipandola dalla dimensione tradizionalmente borghese del right to be let alone, oggi la sfida è rendere questo straordinario diritto di libertà - con l'evoluzione che l'ha caratterizzato - protagonista di uno sviluppo inclusivo e umano-centrico del digitale.

Con l'urgenza delle più forti istanze democratiche emerge infatti, progressivamente più chiara, la necessità di uno statuto, giuridico ma anche etico, delle neotecnologie, che ne promuova

massimamente lo sviluppo, ma al servizio della persona, della solidarietà, dei diritti fondamentali.

Ad oltre un anno dal ritorno, alle porte dell'Europa, dello spettro, drammatico e dimenticato, della guerra, il primato sul digitale e l'indipendenza tecnologica assumono un crescente valore strategico, anche dal punto di vista geopolitico. E' significativa l'ipotesi di divieto, al vaglio della Commissione Ue, di utilizzo delle tecnologie offerte da Huawei per lo sviluppo delle reti 5G. Le limitazioni, imposte da alcuni Governi, all'uso di piattaforme di origine cinese o il divieto statunitense di esportazione di materiale hi-tech sensibile verso Pechino esprimono anche la preoccupazione per la capacità di condizionamento, persino sotto il profilo militare, della tecnica. La guerra dei chip è, in fondo, solamente un'altra faccia della stessa, silente ma nettissima, contrapposizione tra Usa e Cina. Sembra delinearsi una nuova, ma non meno temibile, guerra fredda, sempre più "privatizzata" e ibrida, come si è detto, per l'incidenza delle big tech nelle dinamiche belliche.

E mentre sugli schermi scorrono le immagini, quasi antistoriche, di carri armati schierati tra trincee e confini contesi, cresce il non infondato timore di una delega all'algoritmo persino di quelle "tragic choices" che sono le scelte in materia militare, con sullo sfondo jet a guida autonoma e droni kamikaze. Il segretario generale delle Nazioni Unite ha espresso preoccupazione per la potenziale applicazione dell'intelligenza artificiale nel settore delle armi, auspicando la definizione di "alcune linee rosse".

L'autonomia decisionale che taluni sistemi d'intelligenza artificiale sono pronti a sviluppare preoccupa dunque, anche in campo militare, soprattutto in uno scenario internazionale ancora dominato dalla guerra. Si temono, infatti, rischi non fronteggiabili neppure con quel, pur innovativo, "codice etico" per un'intelligenza artificiale, "responsabile" in campo bellico, adottato dagli Usa già due anni fa, all'insegna della trasparenza e della supervisione umana.

Matura così, anche sulla base di questi timori l'intenzione americana, come quella degli Stati riuniti al G7 di fine maggio, di voler regolare l'aspetto forse più dirompente delle neotecnologie: l'intelligenza artificiale appunto, già oggetto, in Europa, di una proposta di regolamento in fase avanzata di discussione. Ancora una volta l'"effetto Bruxelles", la vis attractiva di molte norme europee promuove, come già per il Gdpr in questi cinque anni di applicazione, una spinta globale alla regolazione delle neotecnologie. E non certo per una pretesa egemonia culturale del vecchio continente né, probabilmente, per la deterrenza delle sanzioni previste in caso di violazione delle norme europee che, con efficacia parzialmente extraterritoriale, si applicano (tanto per la protezione dei dati quanto per l'intelligenza artificiale) a chiunque si rivolga al mercato europeo.

La forza attrattiva delle norme europee deriva, piuttosto, dalla lungimiranza delle sue scelte, con quello sguardo anticipatore proprio, anche etimologicamente, della figura emblematica del dominio della tecnica: Prometeo. Il governo del digitale e la regolazione dei dati assumono, così, una valenza geopolitica strategica, capace di riorientare assetti di potere

consolidati. Lo dimostrano gli effetti della sanzione irrogata dal Garante irlandese a Meta e la complessità della definizione dell'accordo per il trasferimento dei dati negli Usa, su cui si gioca una partita importante anche in termini di politica internazionale.

Il diritto alla protezione dei dati ma, più in generale, la tutela della persona rispetto al potere della tecnica necessita di una garanzia universale, che superi asimmetrie normative del tutto inadeguate a una realtà, come quella digitale, che prescinde dal limite territoriale.

Verso il futuro

In tale contesto l'Europa, prima nel mondo, si avvia a disciplinare l'intelligenza artificiale per renderla "trustworthy", affidabile. E' una scelta importante in sé, soprattutto in un contesto in cui la frequente tendenza alla deregulation finisce con il delegare alla legge del mercato e al potere dell'innovazione, insofferente ai limiti, la definizione del perimetro di diritti e libertà.

Quest'opzione caratterizza tutta la politica europea del digitale, dal Gdpr sino ai più recenti Data Governance, Digital Services e Digital Markets Act, accomunati dall'esigenza di riequilibrare il rapporto tra Stato e mercato, persona e tecnica, libertà e innovazione.

Anche nel metodo, la regolazione europea delinea un modello notevolmente distante, tanto da quello liberista americano, quanto da quello statalista cinese, regolando non la

tecnica, ma i suoi vari usi, in una prospettiva il più possibile "future-proof".

La convergenza tra innovazione e libertà si realizza nella tassonomia dei livelli di rischio dei vari usi dell'intelligenza artificiale, sino a quelli vietati perché potenzialmente idonei a violare la dignità umana o amplificare le discriminazioni dalle quali, invece, proprio le macchine avrebbero dovuto liberarci. Di qui, ad esempio, il divieto di ricorso alle tecniche subliminali o intenzionalmente manipolative, tali da sfruttare le vulnerabilità soggettive o a sistemi di social scoring.

Anche se pensate per favorire l'inclusione offrendo prestazioni sociali ai soggetti più svantaggiati, per eterogenesi dei fini queste applicazioni rischiano invece **-** come dimostra il sistema antifrode olandese Syri - di determinare ulteriore divario sociale, anche per effetto di discriminazioni algoritmiche sempre più opache e, dunque, difficili da individuare. La classificazione delle persone in base al comportamento sociale, alla condizione socio-economica, alle caratteristiche soggettive, già di per sé problematica, lo diviene ancor più se affidata a un algoritmo, con bias che possono caratterizzarlo (per scarsa inclusività e sub-rappresentatività del set di dati su cui si è formato), distorcendone l'esito. Se ne è occupato anche il Garante, rispetto ad iniziative locali volte all'erogazione di benefici sulla base di meccanismi di scoring associati a comportamenti "virtuosi" del cittadino in vari settori. Peraltro, come dimostrano il Social credit system cinese e il, pur diverso, Gosuslugi russo, il monitoraggio centralizzato dell'accesso alle prestazioni sociali necessita di cautele, tali da evitarne la degenerazione in una forma di controllo

sociale panottico, se non, addirittura, di totalitarismo digitale. Per altro verso, l'utilizzo dell'i.a. nel campo della ricerca è agevolato e tanto più potrà essere valorizzato grazie alla possibilità di condivisione dei dati a fini solidaristici e, appunto, di promozione della ricerca consentita dal Data Governance Act, con l'innovativo istituto dell'altruismo dei dati.

Il Regolamento sull'intelligenza artificiale ha introdotto limiti rigorosi rispetto alla congiunzione tra potere investigativo e potenza della tecnica, che impone condizioni tanto più stringenti quanto più avanzato sia il grado d'autonomia decisionale della macchina. Così, oltre ai sistemi di polizia predittiva e rilevazione delle emozioni, il divieto si è esteso al riconoscimento facciale, in luoghi pubblici.

L'utilizzo dell'intelligenza artificiale nel settore investigativo necessita, infatti - come chiarito anche dal Garante - di cautele tali da scongiurare il rischio della delega all'algoritmo - tutt'altro che immune da errori - di attività potenzialmente incidenti sulla libertà personale e della sorveglianza massiva. Ciò che si teme non è tanto e non è solo il "pendio scivoloso", quanto la tendenza all'acritica accettazione sociale di una progressiva limitazione della libertà.

L'uomo di vetro

Tra le garanzie necessarie per impedire effetti socialmente regressivi dell'intelligenza artificiale, quelle già sancite dalla disciplina di protezione dei dati – dal divieto di uso discriminatorio al diritto alla spiegazione oltre, appunto, al principio di

proporzionalità - rappresentano un presidio essenziale. E concorrono alla definizione del limite che l'uomo deve saper (op)porre alla tecnica, il diritto al potere, la democrazia all'ideologia del controllo.

Il caso Chat Gpt è, in questo senso, significativo. L'intervento del Garante ha, infatti, consentito di indirizzare lo sviluppo di questa forma d'intelligenza artificiale generativa in una direzione compatibile con la tutela della persona, contrastando lo sfruttamento di quei frammenti dell'io che sono i dati personali.

La loro protezione è protezione della libertà e della dignità della persona, tanto più quando sono coinvolti i minori, con la comprensibile voglia, propria di quella fase della vita, di fare esperienza di tutto, anche di ciò che è troppo più grande di loro. Importante anche, in questo senso, il provvedimento adottato nei confronti del chatbot Replika, presentato addirittura come una sorta di amico virtuale, capace di migliorare il benessere emotivo dell'utente, con un'incidenza psicologica potenzialmente significativa su soggetti, come i minori, dalla personalità ancora in formazione.

In entrambi i casi su descritti, l'uso dell'intelligenza artificiale, non presidiato da alcune necessarie garanzie, avrebbe esposto gli utenti, soprattutto se minori, a rischi non irrilevanti.

Nell'esigere il rispetto degli obblighi di trasparenza, di verifica dell'età e di liceità del trattamento, il Garante ha infatti potuto sollecitare l'attenzione (non solo europea) sulla necessità che il progresso non si affermi in danno della persona,

limitandone la libertà e sacrificando i diritti sul terreno del mercato, ma promuova invece un ragionevole equilibrio tra iniziativa economica, innovazione, tutela della persona.

Questo vale anche per le ulteriori frontiere dell'intelligenza artificiale nel campo, ad esempio, delle neuroscienze, dove si è realizzato un decoder "semantico" dell'attività neurale a partire dai dati forniti da una risonanza magnetica funzionale, combinando scansione cerebrale e database di modelli linguistici, come quelli usati da Chat Gpt. E' recente, peraltro, l'autorizzazione resa a una nota società dal competente ente regolatorio statunitense, all'avvio dei test per impiantare un chip nel cervello umano, per aiutare alcuni pazienti neurologici a comunicare direttamente con un device esterno, attraverso il pensiero. Si tratta di un'innovazione potenzialmente rivoluzionaria, capace di apportare benefici senza precedenti per la cura di stati neurodegenerativi e, per ciò, meritevole di sviluppo, purché con l'adozione di ogni misura necessaria a impedire derive post-umaniste.

L'applicazione dell'intelligenza artificiale in campo neuroscientifico e, soprattutto i sistemi di brain reading, idonei almeno potenzialmente a decodificare il pensiero, devono infatti sempre garantire, come primo dei "neurodiritti", la privacy mentale, condizione ineludibile di autodeterminazione, presupposto intangibile di libertà. Varcata la soglia della lettura del pensiero, la deriva da impedire è rendere la persona un archivio liberamente accessibile, le cui idee siano messe a nudo senza più alcuno spazio per la libertà, anzitutto di determinazione.

Mai come in questo caso, alla infinita volontà di potenza della tecnica, a ciò che si è definito il “playing God”, deve porsi un indirizzo e un limite, etico e giuridico, a tutela della dignità della persona. Il rischio, altrimenti, è che le tecniche divengano sempre più opache, mentre le persone sempre più trasparenti, secondo l’idea dell’uomo di vetro cara a sistemi tutt’altro che democratici.

Rischi non meno trascurabili pone il metaverso, destinato ad avere implicazioni dirimenti sulla società e sulla stessa antropologia contemporanea. L’esperienza immersiva e totalizzante che esso consente, rendendo l’utente protagonista e non solo fruitore del suo mondo, avrà un impatto non trascurabile sul rapporto tra uomo e tecnica. Alcuni ricercatori prefigurano, addirittura, un’ibridazione così profonda tra reale e virtuale nella percezione degli utenti, da potersi ipotizzare persino delle “cyberemozioni”, in grado di trasformare l’esperienza soggettiva.

Molto delle sue potenzialità e dei suoi rischi dipenderà da come verrà strutturato, se cioè sarà terreno di conquista dei soli big tech, riproducendo l’oligopolio del capitalismo digitale, se sarà open source o se invece vedrà una presenza, da definire nei modi e nelle forme, del pubblico. Certo è che la concentrazione di dati che comporterà questa vera e propria società della simulazione, dovrà essere bilanciata da responsabilità rilevanti delle piattaforme. L’impostazione tecnologicamente neutra del Gdpr potrà fornire una regolazione tendenzialmente completa sui principali aspetti di questo mondo nuovo. Ma emergeranno certamente nuove istanze di tutela, a fronte di vulnerabilità e persino soggettività nuove, come quella del gemello digitale in cui

si proietterà il nostro io o nuovi tipi di dati, quali quelli inferiti dalle interazioni on-line, suscettibili di esprimere stati emotivi, cui dovrà accordarsi una particolare "privacy relazionale".

Ma, rispetto al metaverso, andranno adottate tutte le misure necessarie ad impedire un'eccessiva dipendenza, soprattutto dei giovani, da questa dimensione quasi onirica, capace di alienarli dalla realtà e di svincolarli dal rapporto con essa, proiettandoli nello spazio dell'infinitamente possibile.

La solitudine digitale

Quello dello straniamento è, del resto, un rischio tutt'altro che remoto se si considera il fenomeno, sempre crescente, della violenza non solo assistita in maniera del tutto inerte, ma addirittura filmata e poi esibita sul web. Poche settimane fa, a Napoli, un bambino di dodici anni è stato massacrato di calci e pugni, mentre il branco riprendeva il pestaggio, per poi "esibirlo", come macabro trofeo, in rete. Mesi prima, a Civitanova Marche, un uomo è stato ucciso a bastonate mentre i passanti si limitavano a riprendere quel dramma con il telefono. Ebbene, questo inerte osservare la violenza, con il telefono in mano, non può non interrogarci, come singoli e come istituzioni. Ed esige una riflessione la ricerca spasmodica, da parte dei giovani, di una "visibilità" sui social spinta sino al punto di mettere a rischio la vita degli altri.

Si rischia così troppo spesso di divenire spettatori inerti del male o, come nel recente caso di cronaca, di sacrificare la vita di un bambino per un like in più. Se tutto ciò è frutto dell'alienazione

dal reale cui può condurre la sempre più marcata traslazione on line della vita, è prioritario ricostruire una coscienza comune che tenga conto degli effetti, sulle relazioni, della digitalizzazione di tutto.

Se confondiamo la persona con la sua immagine, se non interveniamo sul male che si compie, ma lo filmiamo, rinunciamo a cogliere, della tecnica, le sue straordinarie potenzialità inclusive e ci condanniamo a un'inconsapevole solitudine digitale, celata da una malintesa idea di connessione totale. Perché, nel rapporto impari con la tecnica e la sua potenza geometrica, la più grande vulnerabilità della persona (soprattutto, ma non solo minorenne) è la sua solitudine, il suo confrontarsi, quasi inerme, con un potere che rischia di divenire insindacabile e totalizzante, più dei vecchi arcana imperii.

La disciplina di protezione dei dati mira a colmare questo vuoto, riequilibrando il rapporto tra uomo e tecnica nel segno della tutela dei diritti e delle libertà. Proprio il caso Chat Gpt (rispetto al quale l'intervento dell'Autorità ha fornito l'impulso per la costituzione di una task force a livello europeo) dimostra come il dialogo con il Garante, lungi dal "bloccare" l'innovazione, possa orientarla verso una direzione compatibile con la tutela della persona e dei suoi diritti.

E questo anche rispetto a un'altra accezione della solitudine digitale: l'autismo informativo e relazionale cui, paradossalmente, ci costringe la rete, relegandoci in "filter bubbles" alimentate dei soli contenuti ritenuti affini al profilo di utente stilato, con il pedinamento digitale, dall'algoritmo. Questa

presentazione selettiva della realtà (il fenomeno del “Daily me”, la personalizzazione algoritmica della rete), può produrre intolleranza a tutto ciò che è diverso da noi, distorsioni significative sul processo di formazione dell’opinione pubblica, sempre più polarizzata su opposti estremismi. La crisi della democrazia scomparsa è, non a caso, correlata da Byung Chul Han proprio alla scomparsa dell’”Altro” e, quindi, alla “crisi dell’ascolto” indotta dalla dinamica autoreferenziale della rete: “il like esclude qualsiasi rivoluzione”.

Ed è significativo che nell’Artificial Intelligence Act i sistemi di raccomandazione con valenza condizionante le scelte elettorali siano compresi tra quelli ad alto rischio, per gli effetti potenzialmente distorsivi sulle garanzie democratiche che possono avere, come insegna il caso Cambridge Analytica, già oggetto, anni fa, di un provvedimento sanzionatorio del Garante. Un ulteriore intervento dell’Autorità ha invece riguardato la funzione Election day information offerta da Meta in occasione delle scorse elezione politiche. Il trattamento di dati ad essa correlato è stato oggetto di un provvedimento di limitazione (successivo a un avvertimento), per l’assenza di garanzie e della necessaria trasparenza rispetto all’utilizzo di dati potenzialmente anche espressivi dell’orientamento politico del cittadino, peraltro in un momento, quale quello dell’esercizio del diritto di voto, centrale nelle dinamiche democratiche.

Un’ulteriore criticità del capitalismo delle piattaforme riguarda la tendenza alla remunerazione del consenso al trattamento dei dati personali, assunto come parte di uno scambio tra dati e servizi. Il Garante se ne sta occupando, in

particolare, nell'ambito dell'istruttoria, avviata lo scorso autunno, sull'uso dei cookie wall da parte di molte testate giornalistiche on-line, che subordinano l'accesso ai contenuti alla prestazione del consenso ad attività di profilazione o, alternativamente, al pagamento di un prezzo. Per non derubricare i dati personali, oggetto di un fondamentale diritto di libertà a mera risorsa economicamente sfruttabile, va delineato un confine tra data-economy e monetizzazione della privacy, con tutti i rischi, in termini di libertà ed eguaglianza, suscettibili di derivarne, come abbiamo avuto modo di sottolineare anche al Senato, in audizione sul recepimento della direttiva "omnibus". Benché il modello capitalistico attuale (non meno "estrattivo" del suo archetipo) si fondi sempre più sulla deduzione dei dati nel sinallagma negoziale, bisogna evitare ogni deriva che renda la privacy un lusso per pochi, contraddicendo quel percorso che l'ha resa, da tradizionale prerogativa borghese, uno straordinario presidio di tutela di tutte e tutti, soprattutto dei più vulnerabili.

Per altro verso si diffondono, con incredibile viralità, notizie false e immagini artefatte, che si finisce con il credere vere per quel meccanismo autoconfermativo che fa dipendere l'attendibilità non dalla verificabilità del contenuto, ma dalla quantità di condivisioni ottenute: dalla sua diffusività e non dalla sua intrinseca veridicità. Il DSA – parallelamente al DMA - introduce una responsabilizzazione complessiva delle piattaforme, anche sotto il profilo della trasparenza, rilanciando la scommessa europea di regolare la rete senza limitarne la libertà, proprio quando la Corte suprema americana conferma l'immunità (pur condizionata) delle piattaforme rispetto alla

responsabilità per i contenuti diffusi dagli utenti. Le norme europee da poco approvate disciplinano, con un ragionevole equilibrio tra libertà di espressione, di iniziativa economica e tutela degli utenti gli obblighi di trasparenza delle piattaforme e le garanzie da accordare nell'attività di moderazione e raccomandazione. Significativi sono, in particolare, le limitazioni poste alle possibilità di combinazione di dati da fonti diverse, gli obblighi informativi sulla pubblicità e sui sistemi di raccomandazione, i divieti di pratiche di autopreferenza e di inserzioni pubblicitarie basate sulla profilazione di utenti minori, le misure di prevenzione della pubblicità occulta, capace di condizionare fortemente scelte e comportamenti individuali.

Queste distorsioni dell'informazione e delle relazioni in rete, l'eclissi del reale, sono tanto più pregiudizievoli per chi, come i giovani, non dispone ancora delle risorse cognitive e del senso critico per discernere le notizie vere dalle fake news, la critica dall'hate speech, la nuova amicizia dal grooming. I giovani fanno esperienza del mondo soprattutto tramite il web, senza tuttavia disporre degli strumenti per comprenderlo e spesso imbattendosi, da soli, in contenuti inadatti alla loro età, con attitudine manipolativa.

Così, ad esempio, relazioni intrattenute sui social possono determinare il coinvolgimento del minore in sfide potenzialmente anche letali, nella cessione di scatti intimi poi utilizzati a fini estorsivi, in incontri pericolosi, non più solo virtuali. Solo quest'anno, sono stati ben 4618 i casi trattati dal Centro Nazionale per il Contrasto della Pedofilia Online relativi ad adescamento, pedopornografia e altri reati correlati all'abuso

sessuale, tecnomediato, di minori. 430 sono risultati, invece, i casi di adescamento online, di cui ben 264 in danno di infratredicenni. Tra il 2021 e il 2022, la circolazione di materiale pedopornografico autoprodotto è cresciuta, a livello internazionale, del 374% rispetto ai livelli pre-pandemici, in virtù anche del maggior uso della rete da parte dei minori.

Le infinite possibilità d'interazione, non sempre positive, consentite dai social network eludono così, spesso, le cautele preposte dai genitori nel mondo off-line, con la selezione della cerchia di amici di riferimento, dei contesti e delle attività consentite al minore, delle sue possibilità di scelta autonoma.

Le straordinarie opportunità di crescita, di informazione, di conoscenza offerte dalla rete si affiancano così a pericoli che si amplificano, in misura esponenziale, quanto più piccoli e, dunque, tendenzialmente immaturi siano gli utenti delle piattaforme. Stabilire la soglia di accesso autonomo dei minori alla rete diviene, dunque, tema cruciale per impedire i rischi della "solitudine digitale" e, quindi, dell'esposizione del minore a contenuti potenzialmente lesivi per lo sviluppo della sua personalità, senza neppure la mediazione degli adulti di riferimento. Ora, non si tratta di proibire l'uso dei social (le cui potenzialità emancipatrici sono simboleggiate ad esempio dall'ausilio che hanno, in vario modo, fornito al movimento femminista iraniano) ma, certamente, di renderlo più sicuro; per i minori innanzitutto.

La disciplina di protezione dei dati offre, sotto questo profilo, un presidio importante, di cui va garantita effettività

soprattutto grazie a sistemi di age verification che, pur non comportando una schedatura dei minori, assicurino adeguata verifica dell'età, anche incaricando di ciò terze parti affidabili. In questa direzione si muove, ad esempio, il tavolo istituito con il recente protocollo d'intesa tra Garante ed Agcom, per la promozione di un codice di condotta relativo ai sistemi per la verifica dell'età delle piattaforme.

La tutela preventiva assicurata dall'age verification è, del resto, il necessario complemento della tutela remediale accordata dal Garante, in particolare rispetto al cyberbullismo e al revenge porn**,** che si conferma essere un presidio essenziale per ragazze e ragazzi vittime di un uso violento della rete, purtroppo anche da parte dei loro coetanei. Proprio in ragione della sua efficacia questa misura, caratterizzata peraltro da una procedura rapida come richiedono i tempi contratti del web, potrebbe essere estesa – come si era proposto nella scorsa legislatura e come si è suggerito alla Camera - ai contenuti istigativi all'autolesionismo. In tal modo, infatti, si potrebbe limitare il rischio di coinvolgimento dei minori in sfide pericolose, che troppo spesso hanno indotto adolescenti e, persino, bambini, a scelte fatali.

Strategie integrate

In quest'anno, il Garante si è misurato con la sfida di rendere la protezione dei dati un obiettivo da raggiungere anche con attività di indirizzo e impulso, nella consapevolezza dell'importanza di promuovere questo diritto come fondamento di una civiltà digitale matura.

Così, a fronte del tradizionale strumento sanzionatorio e correttivo, applicato in 317 casi, l'Autorità ha valorizzato anche la funzione consultiva e, lato sensu, d'indirizzo, volta alla promozione della protezione dei dati anzitutto come "cultura", insieme di diritti ed obblighi costitutivi, oggi, della cittadinanza.

Particolarmente rilevante, in tal senso, è il settore lavoristico, nel quale l'attività consultiva ha affiancato, su temi importanti, quella di tipo correttivo. Per un verso, infatti, si è sanzionato l'accesso datoriale alla mail dell'ex dipendente, non giustificabile né con l'interesse a mantenere i rapporti con i clienti né con l'esigenza di tutela giurisdizionale dei diritti in sede contenziosa. Analogamente, è stata sanzionata la rilevazione biometrica della presenza dei propri dipendenti da parte di una società sportiva, in assenza di ragioni idonee a giustificare la raccolta sistematica di dati, quali appunto quelli biometrici, cui l'ordinamento accorda una tutela rafforzata.

Per altro verso, però, il Garante ha fornito indicazioni particolarmente importanti sulle garanzie lavoristiche alla luce delle innovazioni introdotte dal c.d. "decreto trasparenza", n. 104 del 2022. Si è, in particolare, chiarito come il dipendente abbia diritto di conoscere i principali parametri utilizzati per programmare i sistemi automatizzati, anche di valutazione delle prestazioni e come il ricorso a sistemi particolarmente invasivi, quali il machine learning, il rating e ranking, presenti notevoli criticità per la libertà e dignità del lavoratore. Il ricorso intensivo alle neo-tecnologie nel contesto lavorativo (già cresciuto esponenzialmente con la pandemia) non può, infatti, rappresentare l'occasione per eludere le essenziali garanzie di

autodeterminazione, frutto delle più antiche conquiste raggiunte per il lavoro tradizionale, quasi come in un nuovo neotaylorismo digitale.

Una significativa convergenza di misure correttive e d'indirizzo è stata realizzata anche sul terreno - quantomai cruciale per la democrazia - del giornalismo e, in particolare, della cronaca giudiziaria, che deve poter sempre coniugare diritto di (e all') informazione e dignità. Anche lo scorso anno il Garante ha dovuto richiamare i media, al rispetto di un ragionevole equilibrio tra queste due istanze, non indulgendo alla spettacolarizzazione soprattutto rispetto alla cronaca giudiziaria. Così, è stato necessario sanzionare la divulgazione, da parte di una testata giornalistica, di immagini fotosegnaletiche o di analogo tenore, di soggetti fermati. Per altro verso, rispetto ad alcuni eccessi riscontrati nella cronaca della cattura di un noto latitante, si è richiamata l'esigenza del rispetto del principio di dignità della persona e di essenzialità dell'informazione, che impongono di astenersi dalla rivelazione, certamente lesiva, di dettagli non rilevanti ai fini informativi, tanto più quando attengano a patologie di cui soffra il soggetto.

Una strategia integrata peculiare ha richiesto, anche, il telemarketing illegale, endemico per diffusione e radicamento nelle strutture economico-sociali; spesso la "spia" di un più complesso sistema d'illegalità e concorrenza sleale. L'estensione alle utenze mobili del registro delle opposizioni, a partire da luglio scorso, ha solo in minima parte arginato il problema senza, tuttavia, risolverlo, anche per l'incidenza dello "spoofing", capace di eludere il sistema di garanzie previsto. In tale contesto sono

state irrogate sanzioni anche elevate (una di 4.900.000 euro, a un'importante società del settore energetico), in presenza di violazioni connesse a una più generale condizione di inosservanza sistemica degli obblighi propri del titolare. E' stata anche disposta, per la prima volta, la confisca di banche dati illecitamente costituite, da parte di società aduse allo sfruttamento sistematico dei dati dei cittadini.

Ma, quale misura destinata ad avere un'efficacia maggiore nel lungo periodo, il Garante ha promosso un codice di condotta per gli operatori del settore, che in ragione della sua maggiore efficacia conformativa potrebbe risultare persino più risolutivo della deterrenza sanzionatoria. E questo soprattutto se, parallelamente, si prestasse, da parte dei consumatori, maggiore attenzione alla prestazione del consenso al trattamento dei dati a fini promozionali.

Inoltre, al fine di agevolare l'accesso alla tutela accordata dal Garante, si è predisposto uno specifico servizio telematico per la segnalazione di telefonate indesiderate, risultato particolarmente utile se si considera che, in un solo mese, ha ricevuto quasi 11.000 segnalazioni.

Il Garante ha peraltro offerto, anche quest'anno, un contributo significativo rispetto alle misure attuative del PNRR e, in particolare, al processo di delineazione dell'architettura digitale del Paese, nella consapevolezza dell'esigenza, oggi più forte ancora di ieri, di rendere meno permeabile e, quindi, meno vulnerabile la frontiera digitale. E' significativo che, come osserva il Clusit, proprio nell'anno dell'avvio della guerra in Ucraina sia

stato registrato il valore più alto di attacchi cyber a livello globale, con impatto critico nell'80% dei casi. L'Italia e' risultata, secondo l'Agenzia per la Cybersicurezza nazionale, tra i Paesi maggiormente interessati dalla diffusione generalizzata di malware e da attacchi cibernetici mirati. Il settore sanitario (il terzo per numero di cyber attacks) ha registrato, secondo le stime di Ibm, il costo medio più alto per violazione, destinato probabilmente anche a crescere per effetto dell'affinamento delle tecniche intrusive. Proprio per la sua centralità nella strategia di difesa cibernetica del Paese, quello sanitario è stato uno dei settori oggetto di particolare attenzione da parte del Garante, anche nell'ambito dell'attività conseguente alla comunicazione di data breach. Essa è, infatti, spesso il fattore propulsivo di un'azione di controllo e di riorganizzazione nel segno della resilienza informatica, come dimostrano anche i recenti attacchi subiti da alcune aziende sanitarie locali e le attività successivamente intraprese.

Anche per questo, il dialogo con il Governo sull' Ecosistema Dati Sanitari (e parallelamente sul FSE) è stato particolarmente articolato e ha richiesto modifiche progressive.

Rispetto al FSE, è stato peraltro necessario chiarire che l'inserimento, al suo interno, del referto sulla sieropositività è subordinato alla comunicazione dell'esito dell'esame al paziente, di persona. Il processo di digitalizzazione non può, infatti, determinare l'elusione di garanzie fondamentali nel rapporto terapeutico.

Specifiche indicazioni sono state fornite anche rispetto alla piattaforma per l'erogazione dei benefici economici ai cittadini che, in quanto destinata a raccogliere informazioni su aspetti, anche i più delicati, della vita quotidiana dell'intera popolazione, va protetta dal rischio di usi impropri e accessi abusivi.

Le campagne di comunicazione istituzionale (in particolare quella rivolta alle scuole e quella, più generale, sulle garanzie di sicurezza) hanno svolto, peraltro, un ruolo centrale nell'attività di quest'anno, nella convinzione di quanto più efficace della sanzione possa essere la promozione della consapevolezza dell'importanza di proteggere i nostri dati, per rendere la tecnica alleata della libertà e della democrazia.

Il processo, le parti, i terzi

Particolarmente rilevante è stata, nell'anno trascorso, l'attività consultiva svolta dal Garante in relazione alle riforme in materia di giustizia.

Sul versante processuale, civile e penale, le modifiche introdotte hanno, in primo luogo, promosso una rilevante digitalizzazione di attività e flussi informativi, che tanto più garantirà efficienza quanto più potrà assicurare l'effettiva protezione dei dati personali delle parti e dei terzi coinvolti. La riforma del processo penale, poi, ha introdotto alcune importanti innovazioni che il Garante ha contribuito a migliorare. In primo luogo rileva l'oblio per i destinatari di provvedimenti di archiviazione e proscioglimento, realizzato nella forma della deindicizzazione preventiva o successiva, alla pubblicazione, di

questi atti. Si tratta di misure volte a circoscrivere gli effetti della pubblicità del provvedimento giurisdizionale, mediante la limitazione della sua reperibilità attraverso i motori di ricerca. Esse – anche grazie alle indicazioni fornite dal Garante - coniugano tutela della dignità, presunzione d'innocenza ed esigenze informative, secondo una direttrice analoga a quella sottesa al d.lgs. 188 del 2021.

Ma la protezione dati è anche presupposto d'efficacia di un altro degli istituti innovativi della riforma, alla cui definizione il Garante ha fornito un contributo importante: la giustizia riparativa. La riservatezza dei colloqui in cui si articola il percorso riparativo- e dunque, garanzie elevate di protezione dei dati - è, infatti, il presupposto necessario per il buon esito di questa giustizia dell'ago e del filo capace, si è detto, di abbandonare i tre simboli tradizionali della spada, della benda e della bilancia. Il Garante, nel parere sullo schema di decreto legislativo e, poi, di regolamento attuativo, ha infatti fornito indicazioni per assicurare che i programmi rappresentino uno spazio franco, in cui favorire il più ampio confronto tra imputato e vittima, in virtù delle garanzie di riservatezza e confidenzialità accordate.

Per altro verso, il Garante ha anche fornito il proprio contributo nell'ambito dell'indagine conoscitiva condotta, dalla Commissione giustizia del Senato, sulla disciplina delle intercettazioni. In quella sede si è, in particolare, sottolineato come le vere innovazioni delle riforme recenti siano state la previsione di criteri di essenzialità nella redazione dei brogliacci o nella citazione delle conversazioni nei provvedimenti cautelari e la devoluzione delle conversazioni irrilevanti o inutilizzabili all'

archivio riservato, con l'applicazione del regime del segreto d'ufficio e sanzioni rilevanti in caso di diffusione. L'effettiva impenetrabilità dell'archivio rappresenta, pertanto, il punto di forza della disciplina vigente, che va però concretizzato con misure realmente idonee a impedire la circolazione extraprocessuale delle intercettazioni irrilevanti. Per questo, l'archivio in cui esse sono custodite dev'essere protetto adeguatamente, con misure indicate da tempo dal Garante e che devono rappresentare lo standard uniforme di garanzia per ciascun ufficio giudiziario.

Bisogna investire su queste soluzioni per coniugare esigenze di giustizia, diritto di difesa, privacy e informazione, senza che nessun interesse sia tiranno rispetto all'altro. Importante è anche la possibilità di ottenere la rettifica o la cancellazione di propri dati illegittimamente trattati in sede processuale, che può offrire una tutela significativa ai terzi le cui conversazioni siano state intercettate e riportate in atti processuali, in maniera scorretta o eccedente. Anch'essa, tuttavia, andrebbe valorizzata con la previsione – già proposta nelle scorse legislature - di un onere comunicativo, a carico del Pubblico ministero, che informi il terzo dell'esistenza, negli atti processuali, di proprie conversazioni, per consentirgli di attivare la specifica tutela prevista.

Più complesso è il tema della pubblicazione, in violazione del segreto (meramente) esterno ex art. 114, c. 2 cpp, di stralci spesso ampi di conversazioni captate. Benché questo divieto sia posto a tutela non tanto della privacy quanto della neutralità conoscitiva del giudice, la sua violazione (che ben può ledere la riservatezza) integra comunque un trattamento illegittimo di dati

personali. Ad esso si applicano rilevanti sanzioni amministrative previste dalla disciplina di protezione dei dati, che possono svolgere una rilevante funzione deterrente rispetto alla divulgazione acritica e indiscriminata delle conversazioni captate, ben oltre le reali esigenze di cronaca (il giornalismo "di trascrizione" di cui parla taluno).

Per quanto invece concerne le intercettazioni mediante captatori, le potenzialità intrusive di tali strumenti impongono uno scrutinio rigoroso di proporzionalità nel rapporto tra esigenze investigative e privacy. Esso deve orientare non solo la definizione del perimetro, oggettivo e soggettivo di ammissibilità di tali captazioni, ma anche l'adozione di alcune garanzie essenziali, modulate sulla capacità d'incidenza, sul nucleo intangibile della vita privata, di un mezzo potenzialmente ubiquitario e dalle operazioni non agevolmente predeterminabili.

Tali garanzie devono, in particolare, salvaguardare la funzione investigativa delle intercettazioni impedendone, però, la degenerazione in mezzi di sorveglianza eccessivamente ampia o, per converso, in fattori di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio, reso inevitabilmente permeabile se allocato in server non sicuri o, comunque, posti al di fuori dei confini nazionali.

Si potrebbe dunque ipotizzare un divieto di utilizzo almeno delle meno garantite modalità di uso dei captatori, mediante software che non siano inoculati direttamente sul dispositivo-ospite, ma scaricati da piattaforme liberamente accessibili a tutti o, per altro verso, con archiviazione cloud in server posti fuori dal

territorio nazionale. Si dovrebbe, inoltre, vietare il ricorso a captatori idonei a modificare il contenuto del dispositivo ospite e a cancellare le tracce delle operazioni svolte. Ai fini della corretta ricostruzione probatoria, del diritto di difesa e della stessa privacy è, infatti, indispensabile disporre di software idonei a ricostruire, nel dettaglio, ogni attività svolta sul sistema ospite e sui dati ivi presenti, senza alterarne il contenuto, con una verbalizzazione analitica delle operazioni compiute.

Quest'esigenza è tanto più indispensabile rispetto ad operazioni investigative, come quelle in esame, ad alto tasso di esternalizzazione e che come tali presentano maggiori vulnerabilità, essendo in larga parte affidate a privati che devono, quindi, essere adeguatamente responsabilizzati rispetto agli obblighi di sicurezza da garantire.

Come sottolineato anche dal Procuratore della Repubblica di Milano, andrebbe peraltro specificamente disciplinato (con l'estrazione dei soli contenuti essenziali e la tempestiva restituzione) il sequestro dei dispositivi elettronici, ormai porta d'ingresso per la parte più intima della nostra vita privata. Non a caso la Corte suprema americana, nel 2014, vi ha esteso le garanzie tradizionalmente previste per le misure limitative della libertà personale, con un significativo parallelismo tra habeas corpus e habeas data.

Infine, l'orientamento della CGUE ormai consolidato (nell'ultimo anno con tre nette sentenze) sull'inammissibilità della data retention generalizzata - legittima solo se e in quanto "mirata" (ovvero delimitata, soggettivamente, oggettivamente e

cronologicamente) o rapida - imporrebbe una revisione della disciplina interna. La pur recente e condivisibile riforma operata con il d.l. 132 del 2021 si è, infatti, limitata a recepire, dei principi europei, l'esigenza di terzietà dell'organo titolare del potere autorizzatorio continuando, tuttavia, a prevedere - pur a fronte di una differenziazione per titolo di reato in fase acquisitiva - la conservazione preventiva e generalizzata dei dati di traffico relativi alla generalità indistinta dei cittadini.

Corpo e identità

La protezione dei dati incrocia anche altre e nuove istanze di tutela, legate al corpo, alle sue fragilità, alla soggettività e alle relazioni che esprime. Il corpo è del resto, con le parole di Nietzsche, una grande "regione, una pluralità con un solo senso (...) un possente sovrano, un saggio ignoto".

Tra le molteplici istanze legate al corpo l'oblio oncologico assume una rilevanza particolare. Pazienti ormai da tempo guariti si vedono negare la concessione di mutui a lungo termine, mutare radicalmente le condizioni di assicurazione, affievolirsi la possibilità di stipulare un contratto di lavoro o persino di adottare un bambino. Sembra insomma, come si è scritto, che sia possibile guarire dalla malattia, ma impossibile liberarsi del suo stigma, come se proiettasse la sua ombra sulla vita futura del paziente.

Proprio per questo; per impedire che la persona sia risolta nella sua malattia, il Parlamento europeo ha raccomandato agli Stati membri l'adozione di norme (già presenti in alcuni Paesi) che vietino la richiesta di informazioni sulle patologie pregresse,

dopo un tempo ragionevole in assenza di recidive. L'introduzione, nel nostro ordinamento, di norme analoghe – proposte in vari progetti di legge, già dalla scorsa legislatura – contribuirebbe a garantire il diritto della persona di prescindere dal male che ha sofferto.

Per altro verso, la vicenda del piccolo Enea richiama l'esigenza di dare seguito al monito rivolto, da tempo, dalla Corte costituzionale al Parlamento, sul bilanciamento tra diritto del nato alla ricerca delle proprie origini e anonimato materno. Di tale istituto, indispensabile per la garanzia del diritto della donna a una maternità effettivamente libera, va infatti superata quell'irreversibilità che finisce, paradossalmente, per privare la madre della possibilità di rivedere, se del caso, la propria scelta e il figlio dell'opportunità di cogliere tale disponibilità. Per questo la Corte ha sollecitato il legislatore a introdurre una procedura che consenta l'eventuale incontro della volontà del figlio di ricercare la madre e quella di costei di rivedere, in piena autonomia, la propria scelta passata, garantendo la riservatezza di ciascuno.

Sarebbe opportuno, dunque, riprendere l'esame dei progetti di legge in materia (alcuni dei quali, peraltro, attribuivano al Garante la gestione di tale procedura), soprattutto garantendo un'estrema riservatezza nella comunicazione di dati così importanti. La loro rivelazione può rompere, anche traumaticamente, equilibri delicatissimi su cui si fondano vite e relazioni, potendo anche precludere quel rapporto – umano, benché non giuridico – tra madre e figlio, che la revoca dell'anonimato dovrebbe poter consentire. La protezione dati tutela, del resto, scelte femminili non meno complesse, come

quelle sull'interruzione della gravidanza, la cui riservatezza è condizione prima della loro effettiva libertà. Anche per questo, il Garante è intervenuto rispetto all'indebita rivelazione di queste scelte, determinata dall'indicazione, sulla sepoltura dei feti nel comune di Roma, del nome della madre.

Quelli su cui ci siamo soffermati oggi sono soltanto alcuni degli ambiti nei quali si esprime la protezione dei dati. Diritto definito, non a caso, di frontiera, richiamando un concetto che, nella narrativa occidentale, è il luogo simbolico tanto della sfida quanto dell'incontro con l'altro-da-sé, perché la protezione dei dati vive del confronto, sempre dinamico, con una realtà mai eguale a sé stessa.

Dalla bioetica all'intelligenza artificiale, dai poteri privati delle piattaforme al cyberbullismo; dai discorsi d'odio all'oblio; dagli invisibili digitali della gig economy alla telemedicina: in tutti questi ed altri contesti il Garante fornisce il proprio contributo, a tutela di chi viva la solitudine digitale (per assenza di protezione, per asimmetrie cognitive, per necessità) come soggezione all'altrui potere. La solitudine - scriveva, del resto, Michel Foucault - è la condizione prima della totale sottomissione.

Contrastarla, a tutela della libertà e della dignità della persona, è l'obiettivo che il Garante persegue ogni giorno, anche e soprattutto grazie al lavoro prezioso del personale tutto, che voglio qui, unitamente al Collegio e al Segretario generale, sinceramente ringraziare. E ringrazio anche le Autorità che hanno

inteso offrirci, in vario modo, sostegno, nonché il corpo della Guardia di Finanza, per la ormai consueta collaborazione.

Essere all'altezza delle sfide epocali che ci attendono, come singoli e come società, è l'obiettivo che il Garante continuerà a perseguire, con profondo rispetto per la così grande responsabilità affidatagli dal Parlamento.

Vi ringrazio.