GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione annuale 2024

I numeri del Garante 2024

Servizio relazioni con il pubblico

Contatti **16.045**

e-mail **10.682**

telefonici **5.200**

Notifiche *data breach*

2.204 (di cui 1.706 da soggetti privati)

violazione riservatezza **48,24%**

violazione disponibiilità **24,59%**

Quesiti 386

realtà pubbliche

110 (pervenuti nel 2024)

201 (trattati nel 2024)

realtà economiche e produttive

115 (pervenuti nel 2024)

86 (trattati nel 2024)

I numeri del Garante 2024

Reclami

4.030

reti telematiche e *marketing*
38,4%

realtà economiche e produttive
34,3%

RISCONTRI A RECLAMI NEL 2024 → **4.090**

Segnalazioni

94.948

di cui relative al *telemarketing* automatizzato **87.229**

RISCONTRI A SEGNALAZIONI NEL 2024 → **93.877**

di cui relative al *telemarketing* automatizzato **87.229**

I numeri del Garante 2024

Provvedimenti del Collegio

835

SU RECLAMO → **214**

SU SEGNALAZIONE /D'UFFICIO → **82**

DATA BREACH → **38**

RATIFICHE *REVENGE PORN* → **340**

Pareri resi dall'Autorità **104**

***ex* art. 36(4) RGPD** **73**

I numeri del Garante 2024

Misure correttive **468**

Sanzioni pecuniarie **186**

Ammonimenti **93**

Sanzioni pecuniarie pagate

€ 24.430.856,45

Attività ispettive *in loco*

130

Revenge porn

Determinazioni dirigenziali ratificate **625**

I numeri del Garante 2024

Attività internazionale

Riunioni **280**

CEPD **192**

CoE/OCSE **27**

Comunicazione esterna

Prodotti **165**

Video *spot/teaser* **52**

Comunicati stampa **50**

Indice

Indice

1. Introduzione 3

I – IL QUADRO NORMATIVO E I RAPPORTI CON IL PARLAMENTO E ALTRE ISTITUZIONI 19

2. Principali novità normative in materia di protezione dei dati personali 21
2.1. Le leggi 21
2.2. I decreti-legge 26
2.3. I decreti legislativi 29

3. I rapporti con il Parlamento e le altre istituzioni 33
3.1. L'attività consultiva del Garante 33
3.1.1. La consultazione del Garante nell'ambito del procedimento legislativo o dell'esercizio delle funzioni conoscitive, di indirizzo e controllo delle Camere 34
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 34
3.1.3. I pareri sugli atti regolamentari 36
3.1.4. La consultazione del Garante sugli atti normativi regionali o di province autonome 39
3.1.5. Segnalazioni 39
3.1.6. Quesiti 40
3.2. Il contributo al Governo ai fini del riscontro ad atti di sindacato ispettivo 40
3.3. L'esame delle leggi regionali al vaglio di costituzionalità del Governo 41

II - LE ATTIVITÀ PER SETTORE 43

4. Le amministrazioni pubbliche 45
4.1. L'attività fiscale e tributaria 45
4.2. Previdenza, assistenza e altri benefici 49
4.3. La protezione dei dati personali in ambito scolastico 53
4.4. Trasparenza e pubblicità dell'azione amministrativa 57
4.4.1. Pubblicazioni standardizzate 57
4.4.2. La pubblicazione di dati personali online *da parte delle pubbliche amministrazioni* 58
4.4.3. Accesso civico 59
4.5. Mobilità e trasporti 62
4.5.1. Regolamentazione e trattamenti effettuati a livello centrale 62
4.5.2. Mobilità in ambito locale 64
4.6. Trattamenti in ambito locale 65
4.6.1. Ambiente 65
4.6.2. Diffusione di dati personali sui social network 66
4.6.3. Servizi ai cittadini 68
4.6.4. Utilizzo da parte di enti locali di applicazioni informatiche e altri strumenti tecnologici 69
4.6.5. Trattamenti effettuati dal difensore civico 70

Indice

4.7. Il RPD in ambito pubblico 70
4.8. Ordini professionali 71
4.9. Amministrazione digitale 72
4.9.1. Attività consultiva in materia di digitalizzazione della pubblica amministrazione 72
4.9.2. Vigilanza sulle banche dati e violazioni di dati personali in ambito pubblico 77
4.9.3. PEC e servizi fiduciari 79
4.10. La materia anagrafica, elettorale e diritti civili 80
4.11. Trattamenti di dati personali in ambito pubblico mediante dispositivi video 81

5. La sanità 84
5.1. La sanità digitale 84
5.1.1. Il Fascicolo sanitario elettronico 84
5.1.2. L'Ecosistema dati sanitari 87
5.1.3. Il dossier *sanitario* 89
5.2. L'uso dell'intelligenza artificiale in sanità 89
5.3. Trattamenti di dati personali nell'ambito dei sistemi informativi sanitari centrali: pareri dell'Autorità 90
5.4. Trattamenti per finalità di cura e amministrative correlate alla cura 91
5.4.1. Provvedimenti derivanti da data breach 91
5.4.2. Provvedimenti derivanti da reclami e segnalazioni 93
5.4.3. Provvedimenti relativi al trattamento dei dati personali effettuato nell'ambito dell'emergenza sanitaria 94
5.5. Trattamenti per finalità ulteriori rispetto a quelle di cura e/o amministrative correlate alla cura 95
5.6. Esercizio dei diritti 96
5.7. Oblio oncologico 97

6. La ricerca scientifica 99
6.1. La modifica dell'art. 110 del Codice 99
6.2. Provvedimenti adottati ai sensi dell'art. 110 del Codice prima della riforma di aprile 2024 100
6.3. L'art. 110-*bis,* comma 4, del Codice 102
6.4. Le regole deontologiche per trattamenti a fini statistici o di ricerca scientifica 102
6.5. Altri provvedimenti in materia di trattamenti per scopi di ricerca scientifica 103

7. La statistica 105
7.1. La statistica ufficiale 105

8. I trattamenti in ambito giudiziario e di sicurezza 106
8.1. Trattamenti in ambito giudiziario 106
8.2. Trattamenti da parte di forze di polizia 107
8.3. Pareri resi su schemi di decreti in ambito giudiziario o in relazione ad attività di polizia 107
8.4. Il controllo sul CED del Dipartimento della pubblica sicurezza 109
8.5. Il controllo sul Sistema di informazione Schengen 109
8.5.1. Follow up *della valutazione Schengen relativa all'Italia* 110
8.5.2. L'attività di controllo e monitoraggio sul SIS 110

Indice

9. L'attività giornalistica 111
9.1. Trattamento dei dati personali nell'esercizio dell'attività giornalistica 111
9.1.1. Dati giudiziari 111
9.1.2. Illecita diffusione di dati sanitari 112
9.1.3. Dati relativi a minori 112
9.1.4. Notizie di rilevante interesse pubblico e rispetto dell'essenzialità dell'informazione 113
9.2. Trattamento di dati personali da parte dei motori di ricerca e deindicizzazione 114

10. Cyberbullismo e *revenge porn* 118

11. *Marketing* e trattamento di dati personali 120
11.1. Il fenomeno del *telemarketing* indesiderato e l'azione di contrasto 117
11.1.1. Il telemarketing *illegale nel settore delle compagnie telefoniche* 121
11.1.2. Il telemarketing *illegale nel settore energetico* 124
11.1.3. Il telemarketing *illegale in altri settori commerciali* 126
11.1.4. Attivazione illecita di schede telefoniche 129
11.1.5. Utilizzo di call center *ubicati fuori dall'Unione europea* 130
11.2. *Marketing* e profilazione 130
11.3. *Marketing* attraverso dati estratti da pubblici registri e attività promozionale 132

12. Servizi di comunicazioni elettroniche e internet 133
12.1. Meta *Election Day Information* (EDI) 133
12.2. *Cookie* e altri strumenti di tracciamento dei dati personali 134
12.3. Trattamento dei dati personali e *age verification* 135
12.4. Attività in materia di trattamento dati mediante sistemi di intelligenza artificiale 135
12.5. "Monetizzazione" dei dati personali 136

13. La protezione dei dati personali nel rapporto di lavoro privato e pubblico 137
13.1. Trattamenti di dati effettuati mediante piattaforme digitali 137
13.2. Il codice di condotta delle agenzie per il lavoro 139
13.3. Riconoscimento facciale per finalità di rilevazione della presenza dei lavoratori 141
13.4. Violazione di dati personali 142
13.5. Esercizio dei diritti 143
13.6. Trattamenti illeciti di dati particolari riferiti ai lavoratori 148
13.7. Pubblicazione di dati in internet 149
13.8. Dati di lavoratori e clienti trattati tramite sistemi di videosorveglianza 149
13.9. Trattamento di dati di un lavoratore da parte di un sindacato 151
13.10. La protezione di dati nell'ambito del rapporto di lavoro pubblico 151
13.11. Trattamenti di dati personali mediante dispositivi tecnologici 152
13.11.1. Metadati e posta elettronica nel contesto lavorativo 152
13.11.2. Sistemi di videosorveglianza 152
13.12. Trattamento di dati per finalità di instaurazione e gestione del rapporto di lavoro 153
13.12.1 Trattamento di dati nell'ambito di procedure concorsuali 152
13.12.2. FAQ in materia di oblio oncologico e assenze per motivi di salute 155

Indice

13.12.3. Ordine delle professioni sanitarie. Comunicazione a terzi di dati trattati nell'ambito dei procedimenti per l'accertamento del requisito vaccinale 156
13.12.4. Comunicazione di dati personali a terzi nei contesti lavorativi 156
13.12.5. Trattamento di dati personali relativi all'orientamento sessuale del dipendente 158
13.13. Diffusione *online* di dati personali dei lavoratori 159
13.13.1. Dati personali di lavoratori in banche dati pubbliche 161

14. Le attività economiche 162
14.1. Trattamento di dati personali in ambito assicurativo 162
14.2. Trattamento di dati personali in ambito bancario-finanziario e sistemi di informazioni creditizie 162
14.3. Imprese 167
14.4. Concessionari di pubblici servizi 170
14.5. Attività di recupero crediti 172
14.6. Accreditamento e certificazioni 173

15. Altri trattamenti in ambito privato 174
15.1. Trattamento di dati personali nell'ambito del condominio 174
15.2. Trattamento di dati da parte di associazioni e fondazioni 175
15.3. Videosorveglianza nel settore privato 176

16. Intelligenza artificiale e diritto alla protezione dei dati personali 178

17. Violazione dei dati personali 182

18. Il trasferimento dei dati personali verso paesi terzi 184

19. L'attività ispettiva 185
19.1. L'attività ispettiva fra conferme e novità 185
19.2. Modalità operative 187
19.3. La collaborazione con la Guardia di finanza 187

20. Il contenzioso giurisdizionale 188
20.1. Considerazioni generali 188
20.2. Le opposizioni ai provvedimenti del Garante e le decisioni giudiziali di maggior rilievo 188
20.3. Il contributo del Garante nei giudizi in materia di protezione dati 195

21. Le relazioni comunitarie e internazionali 197
21.1. La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dei dati 198
21.2. La cooperazione delle autorità di protezione dati nel settore libertà, giustizia e affari interni 213
21.2.1. Comitato di controllo coordinato 213
21.2.2. EUROJUST 213
21.2.3. EES ed ETIAS 214
21.2.4. EURODAC 216
21.2.5. Sistema di informazione Schengen (SIS) 217

Indice

21.2.6. Sistema di informazione EUROPOL 217
21.2.7. Sistema di informazione Prüm II 218
21.3. La partecipazione dell'Autorità in seno al Consiglio d'Europa, all'OCSE e ad altri gruppi di lavoro internazionali 218
21.4. Le Conferenze internazionali ed europee delle autorità di protezione dati e *privacy* 223
21.5. Le domande pregiudiziali davanti alla Corte di giustizia dell'Unione europea 224
21.6. I progetti per l'applicazione del RGPD finanziati dall'Unione europea 226

22. Trattamenti transfrontalieri di dati personali e cooperazione europea 228
22.1. Trattamenti transfrontalieri e società dell'informazione 228
22.2. Trattamenti transfrontalieri in ambito economico-produttivo 230

23. Attività di normazione tecnica internazionale e nazionale 233

24. L'attività di comunicazione, informazione e di rapporto con il pubblico 235
24.1. La comunicazione del Garante: profili generali 235
24.2. I prodotti informativi 237
24.3. Il sito istituzionale, i prodotti multimediali e le pubblicazioni 237
24.4. Le manifestazioni e i convegni 238
24.5. L'attività internazionale 239
24.6. L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi 239

III - L'UFFICIO DEL GARANTE 241

25. Attività di studio e documentazione 243

26. La gestione amministrativa e dei sistemi informatici 244
26.1. Il bilancio e la gestione economico-finanziaria dell'Autorità 244
26.2. L'attività contrattuale e le procedure di affidamento 245
26.3. L'organizzazione dell'Ufficio 247
26.4. "Amministrazione trasparente" e adempimenti relativi alla disciplina anticorruzione 250
26.5. Il settore informatico-tecnologico e la transizione digitale 251

IV - I DATI STATISTICI 253

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.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 (d.lgs. 30 giugno 2003, n. 196)
Corte EDU	Corte europea dei diritti dell'uomo
Cost.	Costituzione
d.d.l.	disegno di legge
d.l.	decreto-legge
d.lgs.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica
doc.	documento
es.	esempio
FAQ	*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
l.	legge
lett.	lettera
MEF	Ministero dell'economia e delle finanze
n.	numero
p.	pagina
p.a.	pubblica amministrazione/pubbliche amministrazioni
par.	paragrafo
PEC	posta elettronica certificata
PNRR	Piano nazionale di ripresa e resilienza
provv.	provvedimento del Garante
r.d.	regio decreto
reg.	regolamento
RGPD o Regolamento	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
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

GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione annuale 2024

1 Introduzione

Il panorama della protezione dei dati in Italia, e a livello mondiale, si caratterizza sempre di più per l'accelerazione di tutti i processi di trattamento dei dati, anche personali, e la conseguente necessità di approcci agili ed efficaci da parte di un'Autorità, come il Garante, che è chiamata a vigilare sui trattamenti ma anche a promuovere una "cultura" della protezione dei dati, secondo quello che ne è lo statuto normativo. In questo senso, volendo trovare un filo conduttore delle attività condotte nel 2024, si può veramente parlare di una stagione di conferme e novità: un binomio indissolubile che costituisce la cifra del lavoro svolto.

1. Cominciando dall'"intelligenza artificiale", è inevitabile, e forse scontato, dire che si è confermata, anche nel 2024, quale elemento di importanza assolutamente primaria e tale da pervadere di sé praticamente ogni attività. Al contempo, l'anno trascorso si è caratterizzato anche per un accento posto in modo più marcato sulle applicazioni concrete dell'IA e, nell'ottica del Garante, sulla ricerca di soluzioni in grado di conciliare la fame di informazioni di questa tecnologia con i diritti della persona. Ricordiamo che lo stesso G7 a presidenza italiana ha voluto porre l'IA e la persona umana al centro delle proprie riflessioni, e non ha fatto eccezione neppure la tavola rotonda delle autorità di protezione dei dati del G7 (cfr. cap. 21) che nel 2024 si è tenuta a Roma ed è stata organizzata dal Garante. L'incontro ha offerto l'occa-

1 Introduction

The data protection scenario in Italy – and globally – is increasingly characterised by the acceleration of data processing, including the processing of personal data. This evolution calls for agile and effective approaches from an authority such as the Garante, which is called upon not only to supervise processing operations but also to promote a 'culture' of data protection, in line with its institutional mission. In this context, if we were to identify a common thread running through the activities carried out in 2024, it would be fair to speak of a season where continuity and innovation were so closely intertwined as to become the hallmark of the work done.

1. Beginning with 'artificial intelligence', it is perhaps inevitable – if not obvious – to note that it proved also in 2024 to be a matter of paramount importance, permeating virtually every activity. At the same time, the past year was marked by a stronger focus on the practical applications of AI and, from the Garante's perspective, by the search for solutions capable of reconciling the technology's appetite for data with the protection of individual rights. It is worth recalling that the G7 under the Italian Presidency placed the relationship between AI and the individual at the heart of its reflections – and the G7 DPA Roundtable (see Chapter 21), held in Rome in 2024 and hosted by the Garante, was no exception. The meeting offered an opportunity to develop shared, high-level proposals not only to align emerging tech-

sione per elaborare proposte comuni, di alto livello, in generale per armonizzare le tecnologie emergenti e l'intelligenza artificiale con i diritti e le libertà della persona, ma anche per promuovere una più stretta ed efficace azione di controllo sull'applicazione della normativa. Del resto, nel 2024, a livello UE, è stato pubblicato l'AI *Act*, ovvero il primo regolamento europeo volto a stabilire regole armonizzate sull'IA; sul piano internazionale, nell'ambito del Consiglio d'Europa, è stata aperta alla firma delle Parti la "Convenzione-quadro in materia di intelligenza artificiale, diritti umani, democrazia e stato di diritto", destinata a divenire, una volta entrata in vigore, il primo trattato internazionale legalmente vincolante in questo campo – significativamente al crocevia fra tecnologia e tutela dei diritti umani anche in chiave di tutela del dialogo democratico (v. capp. 16 e 21). In questo scenario, una delle questioni più significative ha riguardato il tema della *governance* e del ruolo cruciale giocato dalle autorità di protezione dei dati; la centralità di tale ruolo è stata affermata sia dal CEPD in una dichiarazione adottata il 16 luglio 2024 sia dalle autorità del G7 attraverso un'apposita dichiarazione adottata a Roma l'11 ottobre 2024 (cfr. cap. 16 e par. 21.1); in Italia, è stata evocata con forza dal Presidente del Garante in più occasioni, sia in sede di audizione dinanzi alle competenti commissioni parlamentari sia attraverso i contributi resi in sede consultiva a Parlamento e Governo sugli atti variamente intesi a disciplinare le applicazioni dell'IA a livello nazionale (cfr. cap. 3). Vale la pena di sottolineare che la rivendicazione del ruolo del Garante in questo ambito non risponde a una mera logica di potere, essendo piuttosto radicata nella fattiva competenza e conoscenza della materia e nella capacità, maturata anche nello scorso anno, di individuare un punto di equilibrio fra diritto e tecnologia. Come prima ricordato, il Garante si è infatti esercitato in tutti i campi nella ricerca di soluzioni a problematiche concrete poste dall'impiego dell'IA

nologies and artificial intelligence with individual rights and freedoms, but also promote stronger and more effective oversight of the implementation of the relevant legislation. Indeed, at the EU level, the AI Act was adopted in 2024 – Europe's first regulation establishing harmonised rules on artificial intelligence. At the international level, the Council of Europe's 'Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law' was opened for signature. Once in force, that Convention will become the first-ever legally binding international treaty in this field – marking a critical intersection between technological progress and the protection of human rights, also from the perspective of safeguarding democratic dialogue (see Chapters 16 and 21). In this scenario, governance and the crucial role of data protection authorities (DPAs) have been among the most significant issues. The pivotal role of DPAs has been affirmed both by the EDPB, in a declaration adopted on 16 July 2024, and by the G7 data protection authorities through a declaration adopted in Rome on 11 October 2024 (see Chapter 16 and Section 21.1). In Italy, this role has been strongly underscored by the President of the Garante on several occasions – both during hearings before the relevant parliamentary committees and through contributions submitted in the course of consultations with Parliament and the Government on various legislative initiatives concerning the regulation of AI applications at the national level (see Chapter 3). It is worth emphasising that the Garante's claim to a role in this field is not driven merely by power ambitions, as it is instead grounded in its substantive expertise, deep knowledge of the subject matter, and the proven capacity – further demonstrated over the past year – to strike a balance between law and technology. As previously mentioned, the Garante has in fact been actively engaged across all fields in seeking solutions to the concrete challenges raised by the use of AI in its many

nelle sue varie declinazioni (dai *large language models* agli algoritmi utilizzati nei processi decisionali automatizzati, sempre secondo il paradigma del *machine learning*). In ambito sanitario, dopo l'adozione del Decalogo in materia di IA di cui alla Relazione 2023, si è giunti alle interlocuzioni con il Ministero della salute e AGENAS con riferimento alla realizzazione di una piattaforma informatica di IA a supporto dell'assistenza primaria nell'ambito dei servizi sanitari regionali; significativi anche due pareri resi con riguardo al cosiddetto Ecosistema dati sanitari (EDS) (cfr. par. 5.1.2) e alla Piattaforma nazionale sulla telemedicina (PNT), nei quali il Garante ha ribadito che l'introduzione di sistemi di IA negli strumenti di sanità digitale deve avvenire nel rispetto del RGPD, del regolamento sull'IA e di quanto indicato nel Decalogo, secondo puntuali requisiti. Se passiamo al settore della ricerca scientifica, oltre a esaminare in concreto la natura e le possibilità di utilizzo dei dati sintetici (v. cap. 9) quale alternativa all'impiego di dati personali, nonché le modalità della loro realizzazione con tecniche di IA che garantiscano la conformità delle informazioni sintetizzate ai principi di protezione dei dati personali, il Garante ha valutato positivamente l'impiego di informazioni riferite anche a soggetti deceduti per evitare *bias* nello sviluppo di un algoritmo predittivo, indicando al contempo la necessità di garantire trasparenza sui modelli matematico-statistici utilizzati attraverso la pubblicazione da parte del titolare della necessaria valutazione di impatto. In ambito lavoristico, sono proseguiti gli approfondimenti sull'impiego di algoritmi di IA da parte di una primaria società di *food delivery* (v. cap. 13) per l'organizzazione dell'attività lavorativa dei *rider* da essa utilizzati, in particolare con riguardo al deficit di trasparenza già riscontrato nel 2021 (v. Relazione 2021). Quanto all'utilizzo di tecniche di IA in grandi *database* pubblici, ricordiamo in particolare le indicazioni fornite rispetto al Sistema informativo per l'inclusione

forms (from large language models to algorithms used in automated decision-making processes, all developed under the machine learning paradigm). In the field of healthcare, following the adoption of the Decalogue on artificial intelligence outlined in the 2023 Annual Report, the Garante engaged in discussions with the Ministry of Health and AGENAS concerning the development of an AI-based IT platform intended to support primary care within regional health services. Of particular significance were also two opinions issued in relation to the so-called *Ecosistema dati sanitari - EDS* (Health Data Ecosystem) (see Paragraph 5.1.2) and the *Piattaforma nazionale sulla telemedicina - PNT* (National Telemedicine Platform). In both instances, the Garante reiterated that the deployment of AI systems within digital health tools must comply with the GDPR, the AI Regulation and the guidance set out in the Decalogue, based on specific requirements.Turning to the field of scientific research, the Garante not only examined the nature and potential use of synthetic data (see Chapter 9) as an alternative to personal data, but also explored the methods of generating them through AI techniques in a manner that ensures compliance with personal data protection principles. The Garante expressed a favourable opinion on the use of information relating to deceased individuals to help avoid bias in the development of a predictive algorithm, while at the same time stressing the importance of ensuring transparency regarding the mathematical-statistical models employed, including through the publication by the data controller of the necessary impact assessment. In the employment sector, the Garante continued its inquiry into the use of AI algorithms by a major food delivery company (see Chapter 13) for organising the work of its riders, in particular as to the lack of transparency continuing since 2021 (see 2021 Annual Report). With regard to the use of AI in large public databases, it is worth recalling

sociale e lavorativa (SIISL), in cui l'IA trova impiego sia per l'abbinamento fra offerta e domanda di lavoro sia per la generazione del cd. indice di affinità, che si basa su un modello di calcolo algoritmico e necessita di specifiche garanzie tecniche e organizzative (v. cap. 4). Infine, non si può non citare l'impegno profuso dal Garante in chiave preventiva per evitare che nell'addestramento dei sistemi di IA generativa fossero utilizzate informazioni raccolte massivamente dal web (web *scraping*) o che un sistema di IA relazionale potesse utilizzare contenuti editoriali sulla base di un accordo con il titolare del trattamento (v. par. 12.1).

2. Quello della digitalizzazione della pubblica amministrazione è un altro tema che si colloca in continuità con il pregresso e che ha confermato la propria rilevanza nel 2024. Si tratta di un processo che viene da lontano e ha assunto negli ultimi anni una dimensione molto più pregnante, anche in rapporto con il Piano nazionale di ripresa e resilienza (PNRR – v. Relazione 2023). Se, in via generale, gli interventi condotti hanno mirato ad assicurare il rispetto di standard rigorosi in materia di protezione dei dati evitando la duplicazione di servizi e informazioni, l'Autorità ha operato, in concreto e nel dettaglio, attraverso la definizione delle specifiche di attuazione di numerosi progetti che sono stati avviati da tempo o più di recente, fra i quali il cd. redditometro – con un parere reso sullo schema di decreto del Ministro dell'economia e delle finanze che stabilisce il contenuto induttivo degli elementi indicativi della capacità contributiva – nonché l'Anagrafe nazionale dell'istruzione (ANIST) – attraverso puntuali indicazioni per il monitoraggio qualitativo e quantitativo del sistema di istruzione tecnologica. Significativo anche il lavoro svolto in campo sanitario, ove la digitalizzazione è ormai una realtà ma necessita di sempre più puntuali aggiustamenti e prescrizioni; basti ricordare le indicazioni contenute nel "Compendio sulla sanità digitale" con cui il Garante ha fornito chiarimenti sul-

the guidance on the *Sistema informativo per l'inclusione sociale e lavorativa – SIISL* (Information System for Social and Labour Inclusion), where AI is deployed both to match labour supply and demand and to generate the so-called 'affinity index'. This index, which is derived from an algorithmic calculation model, requires the implementation of specific technical and organisational safeguards (see Chapter 4). Finally, it is worth highlighting the Garante's proactive efforts to prevent the mass collection of information through web scraping from being used to train generative AI systems, or to ensure that relational AI systems would not make use of editorial content on the basis of agreements with data controllers (see Section 12.1).

2. The digitalisation of public administration is another area of continuity that remained key throughout 2024. While this process has long been underway, it has gained greater momentum in recent years, particularly in connection with the National Recovery and Resilience Plan (see 2023 Annual Report). Generally speaking, efforts have focused on ensuring strict compliance with data protection standards and avoiding duplication of services and information. In practical and detailed terms, the Garante worked to that end by defining the implementation specifications for numerous projects—both old and new. These include the so-called *Redditometro,* with an opinion issued on the draft decree by the Minister of the Economy and Finance concerning the generalisation potential of indicators of taxpayers' financial capacity, as well as the *Anagrafe nazionale dell'istruzione – ANIST* (National Register of Education), for which the Authority provided specific guidance on the qualitative and quantitative monitoring of higher technological education. Significant progress has also been made in the healthcare sector, where digitalisation has become a reality but still requires increasingly specific adjustments and regulatory measures: one need only recall the guidance provided in the 'Compendium on Digital Healthcare' in which

l'utilizzo e sul funzionamento delle sempre più diffuse piattaforme e *app* per la gestione dei rapporti fra medico e paziente, compresi i profili di responsabilità per i trattamenti svolti. La disciplina attuativa del FSE 2.0 ha poi impegnato notevolmente l'Autorità dopo il parere generale reso nel giugno 2023 (v. Relazione 2023); soprattutto, le modalità di esercizio della facoltà di opposizione all'alimentazione del FSE sono state oggetto di approfonditi pareri, anche rispetto all'individuazione di idonei meccanismi per informare i pazienti. Proprio su quest'ultimo aspetto, il Garante ha operato per ridurre le difformità di attuazione della relativa disciplina sul territorio nazionale, in linea con lo spirito della riforma che intendeva introdurre garanzie e misure omogenee – di cui le 20 diverse tipologie di informativa predisposte da regioni e province autonome costituivano un'evidente contraddizione. Una positiva novità è stata in questo campo la nuova soluzione architetturale predisposta dal Ministero della salute con riguardo all'EDS (Ecosistema dei dati sanitari), già previsto dalla disciplina sul FSE, perché, da un lato, tiene conto dei principi di *privacy by design* e, dall'altro, prevede (a seguito dell'intervento del Garante in fase istruttoria) l'alimentazione dell'EDS con i dati del FSE solo su richiesta specifica ed espressa degli interessati (compresi professionisti e pazienti) (cfr. par. 5.1). Inoltre, occorre sottolineare che l'azione del Garante è risultata indispensabile perché spesso la digitalizzazione è intervenuta su sistemi e *database* costituiti molti anni addietro e bisognosi, per tale motivo, di opportuni adeguamenti; è il caso del sistema informativo che monitora le prestazioni sanitarie in emergenza/urgenza (EMUR), creato nel 2008, in cui si è reso necessario aggiornare il sistema di codifica e aggregazione dei dati e riconfigurare i ruoli *privacy* dei vari soggetti coinvolti nonché individuare un periodo congruo per la conservazione dei dati (cfr. par. 5.3). Su questa stessa linea, si è collocato, in ambito giudiziario, il contributo fornito dal Garante nel trac-

the Garante offered clarifications on the use and functioning of the growing numbers of platforms and apps designed to manage the doctor-patient relationship, including the liability implications related to data processing activities. The implementing legislation of the *FSE* (Electronic Health Record) also demanded considerable attention from the Authority, following the general opinion delivered in June 2023 (see the 2023 Annual Report). Particular focus was placed on the procedures for exercising the right to object to the inclusion of data in the *FSE*. The Garante provided in-depth opinions on these procedures, also in relation to the development of appropriate mechanisms to inform patients. Precisely with regard to the latter aspect, the Garante worked to reduce inconsistencies in the application of relevant rules – which ran counter to the reform's intent to ensure homogeneous safeguards and measures. The existence of 20 different information notices issued by the regions and autonomous provinces reflected this inconsistency. A positive innovation in this field was the new architectural solution developed by the Ministry of Health regarding the *EDS*. Already foreseen in the regulatory framework of the *FSE*, this solution reflects the principles of privacy by design and – thanks to the Garante's intervention – it now also provides that the *EDS* may only be fed with *FSE* data following a specific and explicit request by the data subjects (including both patients and healthcare professionals) (see Section 5.1). Moreover, it is also worth emphasising that the Garante's action proved indispensable, particularly because digitalisation often involved adapting systems and databases created many years ago. This was the case, for example, with the *EMUR* system for monitoring emergency and urgent healthcare services, which was established in 2008, where it was necessary to revise the data aggregation and coding systems, redefine the data protection responsibilities of the various parties involved, and determine appropriate data retention

ciare il percorso del Ministero della giustizia verso la transizione digitale, con riguardo ai presupposti per la corretta distruzione di atti e documenti originali analogici nei procedimenti civili (cfr. par. 8.3).

3. Appartiene indubbiamente al perimetro delle conferme tutta la galassia che ruota intorno al principio di *accountability* dei titolari e responsabili del trattamento, vera chiave di volta della riforma a suo tempo operata dal RGPD. La responsabilizzazione, per usare il termine italiano, costituisce infatti un vero e proprio filo rosso nella trama di tutti i trattamenti; più volte, anche attraverso le attività di comunicazione istituzionale (cfr. cap. 24), il Garante ha ricordato che la sua *ratio* non è quella di un adempimento formale e *una tantum*, richiedendo in realtà una cura continua degli *asset* informativi che – per usare quello che rischia di divenire un trito luogo comune – sono il petrolio del XXI secolo. Copiosa è la casistica che conferma l'importanza di un approccio responsabile e avvertito alla gestione delle informazioni, soprattutto quando queste abbiano natura particolare (i dati "sensibili" di cui al Codice n. 196/2003). Un esempio quasi plastico al riguardo è offerto dalla riforma operata dal legislatore nazionale rispetto all'art. 110, comma 1, del Codice, concernente i trattamenti di dati personali per finalità di ricerca scientifica in campo medico, biomedico ed epidemiologico (cfr. par. 6.1): ossia, l'eliminazione del requisito della consultazione preventiva del Garante nei casi in cui non sia possibile acquisire il consenso degli interessati o non vi siano altri presupposti normativi per svolgere trattamenti ulteriori per le finalità in questione. I titolari dovranno invece osservare autonomamente le garanzie individuate dal Garante nella deliberazione di promovimento delle nuove regole deontologiche per trattamenti a fini statistici o di ricerca scientifica e, in particolare, motivare adeguatamente, nel progetto di ricerca, le ragioni etiche o organizzative che impediscono il ricorso al consenso quale fondamento giuridico del trattaperiods (see Section 5.3). Along the same lines, in the judicial domain, the Garante contributed to shaping the Ministry of Justice's digital transition process, with regard to the requirements for the proper destruction of original paper-based acts and documents in civil proceedings (see Section 8.3).

3. The entire galaxy revolving around the principle of accountability of data controllers and processors – undeniably the true cornerstone of the reform introduced by the GDPR – can certainly be counted among the confirmations. Accountability, in fact, underpins all processing operations. On several occasions, including through its institutional communication initiatives (see Chapter 24), the Garante has emphasised that accountability is not to be understood as a merely formal or one-off obligation. Rather, it requires continuous and careful management of information assets which – to use an expression that risks becoming a cliché – are the oil of the 21st century. There is an abundance of cases confirming the importance of a responsible, attentive approach to information management, especially when the data in question is of a special nature (i.e. the 'sensitive' data referred to in Italy's data protection law – the 'Code' – No. 196/2003). A particularly apt example in this respect is offered by the reform of Section 110(1) of the Code, concerning the processing of personal data for scientific research in the medical, biomedical and epidemiological fields (see Section 6.1): namely, the removal of the obligation to consult the Garante in advance when it is not possible to obtain the data subjects' consent or where there are no other legal grounds for carrying out further processing for the purposes in question. Instead, data controllers must autonomously comply with the safeguards identified by the Garante in the resolution on commencement of the procedure for adopting the new code of conduct on processing for statistical or scientific research purposes. In particular, they are required to properly justify, within

mento, nonché pubblicare la valutazione di impatto svolta ai sensi dell'art. 35 del RGPD. Vi è, quindi, un forte spostamento dell'asse delle garanzie verso la responsabilizzazione individuale dei titolari che svolgono attività di ricerca; in questo, giovano evidentemente i contributi forniti dal Garante attraverso i molti provvedimenti adottati, anche nei primi mesi del 2024, in risposta alle istanze pregresse di consultazione preventiva, per le indicazioni operative in essi contenute: ricordiamo i requisiti che presiedono all'anonimizzazione dei dati quale trattamento dinamico da valutare alla luce del concreto utilizzo dei dati e del contesto di tale utilizzo, o le misure tecniche da implementare per assicurare il principio di esattezza (e quindi qualità) dei dati, o anche la valutazione di impatto specifica da dedicare al trattamento di dati genetici. Può dunque parlarsi di una versione "assistita", o aumentata, dell'*accountability* promossa dal RGPD, nel solco di una continuità innovata dai costanti apporti conoscitivi dell'Autorità resi attraverso il confronto con i titolari. Un altro esempio preclaro di questo *trend* è da rinvenirsi nella gestione delle complesse questioni inerenti al *telemarketing*, da sempre uno dei temi più caldi e difficili anche per la multiforme natura dei trattamenti svolti (cfr. cap. 11). Da un lato, è proseguita l'attività di contrasto al *telemarketing* indesiderato, aggravato dalle attività promozionali svolte mediante il ricorso a internet e ai *social media*, sfociata nell'adozione di numerosi provvedimenti correttivi e sanzionatori, e sono stati forniti puntuali riscontri e chiarimenti in risposta alle migliaia di segnalazioni pervenute per via telematica; qui le istruttorie condotte dall'Autorità hanno rivelato il lato oscuro dell'*accountability*, ossia la mancata assimilazione degli obblighi che gravano sul titolare del trattamento: scarsi o inefficaci i controlli sulla filiera che dovrebbe condurre dal contatto al contratto, lacunose le misure tecniche e organizzative, assenti i controlli sulle liste di contatti acquisite da soggetti terzi con informative e consensi

the research project, the ethical or organisational reasons preventing the use of consent as a legal basis for processing, and to publish the impact assessment carried out pursuant to Article 35 of the GDPR. This marks a clear shift in the setting of safeguards towards the individual accountability of data controllers conducting research activities. In this respect, the decisions adopted by the Garante – including those in the early months of 2024 – in response to requests for consultation offer valuable operational guidance. These include the requirements for data anonymisation, to be understood as a dynamic processing activity to be assessed in light of the actual use of the data and its context; the technical measures needed to uphold the principle of data accuracy (and thus quality); and the specific impact assessment to be carried out in the case of genetic data processing. One can therefore speak of an 'assisted' or augmented version of the accountability promoted by the GDPR, in the wake of continuity innovated through the Authority's ongoing contribution of knowledge and expertise which is the result of the dialogue with data controllers.Another prominent example of this trend can be found in the management of the complex issues surrounding telemarketing, which has always been one of the most sensitive and challenging areas – partly due to the multifaceted nature of the processing operations involved (see Chapter 11). On the one hand, efforts continued to combat unsolicited telemarketing, further complicated by promotional activities carried out through the Internet and social media. These efforts led to the adoption of numerous corrective and sanctioning measures, as well as the timely provision of responses and clarifications following the thousands of reports received electronically. In this context, the investigations conducted by the Authority revealed the dark side of accountability, i.e. a failure to internalise the obligations incumbent upon data controllers – characterised by poor or ineffective control over the chain leading from contact

privi dei requisiti di validità necessari. Particolarmente negativo il panorama risultante dal contrasto al *telemarketing* selvaggio nel settore delle forniture energetiche, dove il passaggio al mercato libero ha coinciso con un proliferare di società *multiutility* che hanno interpretato in modo disinvolto il perimetro delle attività promozionali. Al contempo, dall'altro lato, è stato avviato un tavolo di confronto con i principali fornitori del settore energetico per sensibilizzare sulle implicazioni connesse al trattamento dei dati personali della clientela (cfr. par. 14.3), nell'ottica di quella *accountability* "assistita" di cui si parlava poc'anzi; inoltre, alcuni provvedimenti correttivi e sanzionatori hanno costituito l'occasione per una rivisitazione complessiva, anche in termini interpretativi, dell'approccio adottato da importanti aziende, per esempio quanto ai presupposti per il *soft spam* (basato su una deroga al requisito del previo consenso *ex* art. 130, comma 4, d.lgs. n. 196/2003, non equiparabile quanto a *ratio* e conseguenze al legittimo interesse del titolare); lo stesso vale per un provvedimento adottato nei confronti di un importante operatore telefonico, con cui si è preso atto dell'evoluzione registrata nelle campagne di *marketing* per adattarsi ai requisiti di liceità definiti negli anni dal Garante, constatando positivamente il mutamento di approccio in direzione di una vera *accountability* – in particolare, avendo l'operatore privilegiato i contatti basati sulla manifestazione di un valido interesse da parte dell'utente, ossia le cd. "liste calde". Sempre in tema di *accountability*, il problema dei *data breach* offre un ulteriore spunto per ragionare sul filo della continuità, pur essendo notevolmente cresciuto il numero di violazioni comunicate annualmente al Garante (cfr. cap. 17). Molte di tali violazioni hanno riguardato grandi *database* pubblici e privati e le ispezioni condotte dall'Autorità (cfr. cap. 19) hanno evidenziato una persistente sottovalutazione dei rischi legati ai trattamenti con un'insufficiente o, in taluni casi, assente struttura organizzativa

to contract, inadequate technical and organisational measures, and a lack of controls on contact lists acquired from third parties, often accompanied by privacy notices and consent statements falling short of the necessary validity requirements. Particularly worrisome is the picture that emerged from the fight against wild telemarketing in the energy supply sector, where the transition to a liberalised market has gone hand in hand with the proliferation of multi-utility companies that have applied a cavalier approach to promotional activities. At the same time, exchanges were held with the main energy suppliers to raise awareness of the implications involved in the processing of customers' personal data (see Section 14.3), in line with the 'assisted' accountability paradigm referred to earlier. Moreover, the imposition of certain corrective and sanctioning measures served as an opportunity comprehensively reassessing the practices followed by major companies – including interpretative aspects. This was the case, for example, with regard to the conditions for soft spam (based on the derogation from the consent rule under Section 130(4) of the Code, which cannot be equated to the controller's legitimate interest in terms of either its rationale or consequences). The same applies to a decision adopted against a major telephone company, which confirmed an ongoing evolution in marketing campaigns towards compliance with the lawfulness requirements established over the years by the Garante. The decision positively noted a shift toward a model of genuine accountability, with the company having prioritised contacts with individuals who had clearly expressed an interest – namely, those included in so-called 'hot lists'. Still on the subject of accountability, the issue of data breaches offers a further opportunity to reflect on the thread of continuity, despite the significant increase in the number of breaches reported annually to the Garante (see Chapter 17). Many of these incidents affected large public and private databases, and inspections con-

e tecnica volta a prevenire e intercettare le violazioni in questione; significativamente, nel settore bancario la maggioranza di tali violazioni proveniva dall'interno dell'organizzazione del titolare (tipicamente per l'operato di dipendenti infedeli), mentre nell'ambito sanitario le minacce risultano provenire in modo prevalente dall'esterno: si tratta spesso di violazioni associate all'invio di messaggi ricattatori da parte degli autori della violazione, che utilizzano *ransomware* e confidano nella particolare delicatezza (e quindi nel valore intrinseco) dei dati carpiti. Va segnalato (in termini di *accountability*, ancora una volta, assistita) che, nel quadro di un provvedimento assunto nei confronti di una società interessata da una grave violazione di dati personali (cfr. cap. 13), l'incompletezza della notifica fornita al Garante ai sensi dell'art. 33 del RGPD è stata l'occasione per evidenziare i requisiti di una notifica corretta – nello specifico, la necessità che essa contenga tutte le informazioni che caratterizzano l'incidente informatico, così da consentire al Garante di esercitare un controllo accurato e indicare le misure utili a ripristinare un adeguato livello di protezione dei dati personali violati. Sempre in questo ambito, è necessario segnalare la continuità dell'azione di vigilanza svolta dal Garante particolarmente sulle grandi banche dati pubbliche (cfr. cap. 4), anche al fine di arginare il fenomeno degli accessi abusivi, con provvedimenti finalizzati a potenziare le misure di sicurezza tecniche e organizzative; negli ultimi anni si è assistito, peraltro, a un incremento dei casi di rivendita delle informazioni riservate presenti nelle banche dati pubbliche, attraverso meccanismi poco trasparenti di raccolta e reperimento dei dati da parte di soggetti privati. Tutto ciò ha condotto il Garante a costituire una *task force* con il compito di individuare specifiche azioni di controllo e a carattere preventivo, ancora una volta con il fine precipuo di accompagnare e assistere i titolari nell'esercizio della rispettiva *accountability*.

4. Come si è detto, è difficile non evocare

ducted by the Authority (see Chapter 19) revealed a persistent underestimation of the risks associated with processing operations, often accompanied by an inadequate – or downright absent – organisational and technical structure to prevent or detect such breaches. In particular, in the banking sector, most of these violations originated within the data controller's organisation (typically due to the actions of disloyal employees); conversely, in the healthcare sector, threats tend to come predominantly from outside: these are often breaches linked to ransomware attacks and blackmail attempts, in which perpetrators exploit the highly sensitive nature (and thus intrinsic value) of the data they steal. It is worth highlighting – again in terms of 'assisted' accountability – that a decision adopted by the Garante against a company affected by a serious personal data breach (see Chapter 13), shed light on the inadequacy of the notification submitted to the Garante pursuant to Article 33 of the GDPR. This served as an opportunity to clarify the requirements for a proper notification, emphasising that it must include all relevant details of the IT incident to enable the Garante to carry out a thorough assessment and recommend appropriate measures to restore an adequate level of protection of the personal data affected by the breach. In this context, the Garante's continued vigilance must also be emphasised in relation to large public databases (see Chapter 4), with a view to preventing unauthorised access by strengthening technical and organisational security measures. In recent years, however, there has been a growing number of cases involving the resale of confidential information contained in public databases, through opaque mechanisms of data collection and acquisition by private parties. This situation led the Garante to set up a dedicated task force in order to identify specific monitoring and preventive measures, again with the main purpose of guiding and assisting data controllers in fulfilling their accountability obligations.

il principio di responsabilizzazione con riguardo a qualsiasi aspetto del trattamento di dati personali, costituendo essa il perno del RGPD. Merita però dedicare un separato paragrafo alla tutela dei diritti degli interessati, anche perché essa, in ultima analisi, rappresenta una cartina di tornasole della bontà degli approcci messi in campo dai titolari e responsabili del trattamento. Assai ampia, infatti, è la casistica affrontata dal Garante in tema di diritti negati parzialmente o *in toto*; principalmente il diritto di accesso (art. 15 RGPD), in tutte le sue declinazioni, e il diritto all'oblio (art. 17 RGPD) continuano a essere quelli più spesso oggetto di doglianze da parte degli interessati. Persistono, in via generale, alcune difficoltà e incomprensioni concernenti l'accesso alle cartelle cliniche sanitarie, per l'intreccio fra diritto di accesso sancito dal RGPD e diritto di accesso documentale, e per questo il Garante ha ritenuto utile pubblicare alcune FAQ sul sito istituzionale per chiarire i limiti rispettivi e la diversa *ratio* (anche alla luce della sentenza resa dalla CGUE nella causa C-307/22 in tema di profondità e ambito del diritto di accesso di cui all'art. 15 RGPD) (cfr. par. 5.6). Significativi, in questo campo, anche gli sforzi profusi dall'Autorità per assistere interessati e titolari nella gestione del cd. oblio oncologico, alla luce dei compiti di vigilanza attribuiti dal legislatore all'Autorità; menzioniamo, in particolare, il modello unico di informativa a livello nazionale proposto dal Garante, e anche le FAQ intese a chiarire l'interrelazione fra oblio oncologico e diritti dei lavoratori pubblici e privati (cfr. par. 5.7). Molteplici i casi in cui il Garante è dovuto intervenire per porre rimedio all'illecita diffusione di dati, anche particolari, svolta da soggetti pubblici di grandi e piccole dimensioni, molto spesso avvenuta *online* in violazione del principio di minimizzazione di cui al RGPD, ovvero per ribadire i limiti dell'esercizio dell'accesso civico (anche generalizzato) di cui al d.lgs. n. 33/2013 (cfr. cap. 4). Non fa eccezione neppure la pubblicazione di sentenze

4. As previously mentioned, it is difficult not to evoke the principle of accountability when addressing any aspect of personal data processing, as it represents the linchpin of the GDPR. Nevertheless, it is worth devoting a specific paragraph to the protection of data subjects' rights, partly because this ultimately constitutes a litmus test for assessing the soundness of the approaches adopted by data controllers and processors. Indeed, the number of cases handled by the Garante concerning the partial or total denial of rights is particularly significant. Generally speaking, the right of access (Article 15 of the GDPR), in all its forms, and the right to be forgotten (Article 17 of the GDPR) continue to be the most frequent sources of concern with data subjects. Difficulties and misunderstandings persist in relation to access to health records, mainly due to the interplay between the right of access enshrined in the GDPR and the right to access public records. For this reason, the Garante considered it useful to publish specific FAQs on its website, aimed at clarifying the respective limits and rationales of these two rights (also in light of the judgement of the Court of Justice of the European Union in Case C-307/22 which addressed the depth and scope of the right of access under Article 15 of the GDPR) (see Section 5.6). Equally significant, in this field, were the efforts made by the Authority to support both data subjects and controllers in managing the right to be forgotten for cancer survivors, within the framework of its oversight responsibilities as conferred by recent legislation. In this regard, reference should be made to the national standardized privacy notice proposed by the Garante as well as the FAQs designed to clarify the interplay between the right to be forgotten for cancer survivors and the rights of public and private employees (see Section 5.7). In a number of cases, the Garante had to step in to remedy unlawful disclosures of personal data – including special categories of data – by both large and small public entities. These disclosures fre-

recanti dati particolari e giudiziari, come dimostra il procedimento avviato nei confronti della Corte di cassazione che è sfociato in un provvedimento di ammonimento (cfr. cap. 8). Notevolissimo, come di consueto, il numero di reclami e segnalazioni concernenti la diffusione di notizie in rete e su *social media* ritenuta illecita dagli interessati (cfr. cap. 9), soprattutto al fine di ottenere la deindicizzazione di contenuti da parte di motori di ricerca (*in primis*, Google); qui, come sempre, il Garante si è esercitato nella ricerca di un punto di equilibrio fra diritto di informare e di essere informati e diritto alla tutela della propria identità personale. Una novità, in negativo, in questo campo è legata alla sempre più frequente diffusione di materiale artefatto realizzato anche attraverso sistemi di IA (cd. *deep fake*), oggetto di segnalazioni al Garante in rapporto al fenomeno del *revenge porn* (cfr. cap. 10). Sempre in chiave di continuità, si è confermato assai rilevante il numero di provvedimenti adottati nell'ambito dei trattamenti relativi al rapporto di lavoro (cfr. cap. 14), pubblico e privato; particolarmente l'esercizio del diritto di accesso di cui all'art. 15 RGPD continua a trovare ostacoli legati a riscontri assenti o inidonei (talora puramente interlocutori), ovvero a presunte limitazioni quanto alla natura delle informazioni richieste (segreti aziendali) che non possono mai comportare il diniego a fornire all'interessato tutte le informazioni attraverso un adeguato bilanciamento degli interessi in gioco (per esempio, attraverso la cancellazione delle informazioni eccedenti non riferite all'interessato). Egualmente significativi gli interventi del Garante per assicurare un ricorso equilibrato a sistemi di riconoscimento facciale, o comunque a dispositivi biometrici, per rilevare la presenza in servizio, ben difficilmente conformi ai principi di liceità, minimizzazione, proporzionalità del trattamento e, quindi, non utilizzabili nell'ordinaria gestione del rapporto di lavoro. Tuttavia, occorre rilevare anche alcune novità, in positivo, relativamente

quently occurred online in breach of the data minimisation principle enshrined in the GDPR. In other cases, the Authority had to reaffirm the limits of FOIA-type access rights as regulated by Legislative Decree No. 33/2013 (see Chapter 4). Nor were exceptions made for the publication of court rulings containing special categories of data or judicial data, as shown by the proceedings initiated against the Court of Cassation which ultimately led to issuing a reprimand (see Chapter 8). As usual, the number of complaints and reports concerning the allegedly unlawful dissemination of information on the web and social media remained very high (see Chapter 9), most of them being aimed at the de-indexing of content by search engines (first and foremost, Google). In this area, as ever, the Garante sought to strike a balance between the right to inform and be informed and the right to protect one's personal identity. A negative development in this field relates to the increasingly frequent dissemination of fictitious contents, including those created through AI systems (so-called deep fakes), which have been reported to the Garante in connection with revenge porn cases (see Chapter 10). Still in terms of continuity, the number of decisions adopted in relation to processing operations in the employment context remained significant (see Chapter 14), both in the public and in the private sectors. In particular, the exercise of the right of access under Article 15 of the GDPR continues to encounter obstacles due to missing or inadequate responses (which are sometimes purely formal), or to limitations allegedly due to the nature of the information requested (e.g. trade secrets). However, these limitations can never justify a refusal to provide the data subject with all the information, which must instead be ensured by appropriately balancing the interests at stake (for instance, by erasing excessive information that is not related to the data subject). Also noteworthy were the Garante's interventions to ensure a balanced use of facial recognition

alla tutela dei diritti degli interessati, che dimostrano la sedimentazione, lenta ma continua, di approcci organizzativi e formativi necessari a evitare il ripetersi di violazioni – per esempio, in ambito bancario, relativamente all'esercizio del diritto di accesso ai dati di congiunti deceduti (art. 2-*terdecies*, Codice) (cfr. cap. 14). Significativo anche il fatto che delle numerose segnalazioni ricevute quanto al trattamento di dati personali nei sistemi di informazione creditizia (SIC), ben poche hanno condotto a evidenziare violazioni della normativa applicabile; lo stesso dicasi con riguardo al settore del recupero crediti. I provvedimenti a suo tempo adottati dal Garante, anche di indirizzo, e i codici di condotta già sottoscritti dalle principali organizzazioni di settore stanno dando in misura crescente i propri frutti. Vi sono poi alcune ulteriori iniziative di autodisciplina che indicano la volontà di procedere sulla strada di un'effettiva responsabilizzazione; fra queste, l'approvazione di alcuni codici di condotta avvenuta nel corso del 2024 ai sensi dell'art. 40 del RGPD (sviluppo e produzione di *software* gestionali, trattamenti effettuati dalle agenzie per il lavoro in fase pre-assuntiva) (cfr. capp. 14 e 15). Quest'ultimo codice, in particolare, riveste importanza per la necessità di accresciuta tutela in una fase assai delicata, ove sono possibili discriminazioni basate su un utilizzo improprio delle informazioni raccolte dalle più diverse fonti, compresi i *social media*. Nello stesso solco si muovono alcune iniziative di sensibilizzazione ed educazione promosse dal Garante, che hanno riscosso grande successo e plauso. Tra queste, la conclusione del progetto ARC-II merita di essere segnalata sinteticamente perché il progetto, di carattere internazionale, si focalizzava sull'apprestamento di strumenti di autoapprendimento e autovalutazione per le PMI, un settore da sempre bisognoso di grande attenzione e di essere "guidato" verso l'approccio di responsabilizzazione di cui più volte si è parlato (cfr. capp. 14 e 21).

5. Se ne è ragionato *supra* con riguardo

systems—or more generally, biometric devices— for monitoring staff attendance at work. These tools are highly unlikely to comply with the principles of lawfulness, data minimisation, and proportionality, and therefore cannot be used in the ordinary management of employment relationships. However, one should point to some positive developments in the protection of data subjects' rights, which demonstrate the slow but steady consolidation of organisational and training approaches necessary to prevent the recurrence of infringements – for example, in the banking sector, with regard to the exercise of the right of access to the data of deceased relatives under Section 2-*terdecies* of the Code (see Chapter 14). It is also significant that, among the numerous reports received concerning the processing of personal data in credit information systems, very few resulted into finding violations of the applicable legislation; the same applies to the debt collection sector. The decisions and guidance previously adopted by the Garante as well as the codes of conduct already entered into by the main trade organisations are increasingly yielding positive results.There are also further self-regulatory initiatives that indicate the resolve to pursue genuine accountability. Among these is the adoption, during 2024, of several codes of conduct pursuant to Article 40 of the GDPR (relating to the development and production of business management software, and processing carried out by employment agencies in the recruitment phase) (see Chapters 14 and 15). The latter code, in particular, is especially significant given the need for strengthened protection in a very sensitive phase, in which discrimination may occur due to the improper use of information gathered from a wide range of sources, including social media. In the same vein were awareness-raising and educational initiatives promoted by the Garante, which met with great success and praise. Among these, the conclusion of the ARC-II project deserves brief mention, as this international

alla ricerca di approcci coordinati per gestire l'impatto dell'IA in ogni campo, ma è comunque innegabile che si sia in presenza di una crescente internazionalizzazione di tutti i processi di trattamento. Ne danno evidenza l'accresciuto numero, nel 2024, di procedure di "sportello unico" ai sensi dell'art. 60 del RGPD per la gestione di reclami relativi a trattamenti transfrontalieri, che si fondano sui principi di cooperazione fra le autorità e sull'intervento del CEPD quale *ultima ratio* in caso di discordanze (art. 65 RGPD). Un sistema amministrativo pan-europeo che significativamente, e questa è una novità, ha registrato una riduzione dei casi di controversie tali da necessitare l'intervento del CEPD; ciò rappresenta la spia di un consenso sempre più condiviso fra le autorità europee di protezione dei dati (cfr. capp. 21 e 22), anche per la necessità di un approccio coordinato dinanzi alla pressione di grandi *player* multinazionali. Di rilievo è il ruolo che taluni di questi *player* hanno inteso assumere anche con riguardo a delicate attività di interesse pubblico quali quelle rimesse alla legislazione nazionale in materia elettorale (cfr. cap. 12); l'intreccio fra il (presunto) valore civico del servizio offerto, di promozione della partecipazione elettorale, e la (concreta) assenza di un fondamento giuridico legittimante l'intervento di un soggetto privato, mosso da fini primariamente di lucro ed estraneo al contesto nazionale, ha evidenziato la necessità di una vigilanza avvertita e, quindi, orientata in senso prospettico. *De iure condendo*, il futuro regolamento in materia procedurale che i legislatori europei stanno negoziando, quale integrazione delle norme contenute nel RGPD in materia di cooperazione, potrà sperabilmente dare ulteriore impulso in questa direzione, anche attraverso le indicazioni maturate dal CEPD sulla base delle esperienze applicative delle autorità nazionali di protezione dei dati. Del resto, il CEPD sempre più, e in misura particolarmente marcata nel 2024, si esercita nel fornire indirizzi interpretativi sull'applicazione

initiative focused on developing self-learning and self-assessment tools for SMEs – a sector that has always required particular attention and specific 'guidance' to implement the accountability-based approach that has been repeatedly mentioned here (see Chapters 14 and 21).

5. As previously discussed with regard to the search for coordinated approaches to manage the impact of AI in every sector, it is undeniable that there is a growing internationalisation of all processing activities. This is evidenced by the increased number, in 2024, of 'one-stop-shop' procedures under Article 60 of the GDPR for handling complaints concerning cross-border processing, which are based on the principles of cooperation between authorities and on the involvement of the EDPB as a last resort in cases of disagreement (Article 65 GDPR). This pan-European administrative system has significantly – and this is a new development – recorded a reduction in the number of disputes requiring intervention by the EDPB. This reflects an increasingly shared consensus among European data protection authorities (see Chapters 21 and 22), also driven by the need for a coordinated approach to withstand the pressure from major multinational players. Notably, some of these players also sought to play a role in sensitive activities of public interest, such as those governed by national legislation in the field of elections (see Chapter 12). The intertwining of the (alleged) civic value of the services offered – such as promoting electoral participation – and the (actual) absence of a legitimate legal basis for involving a private entity, primarily driven by profit and external to the national context, underscored the need for vigilant and forward-looking oversight. From a *de iure condendo* perspective, the future regulation on additional procedural rules currently being negotiated by EU legislators – intended to complement the cooperation provisions of the GDPR – may hopefully give further impetus in this direction, also drawing on the guidance provided by the

delle norme attraverso complessi pareri (art. 64, par. 2, RGPD) che hanno riguardato, non a caso, il riutilizzo di dati personali per l'addestramento e il *deployment* di modelli di IA, il riconoscimento facciale, i requisiti del consenso nei modelli di *business* basati sul paradigma del *consent or pay* (quest'ultimo legato chiaramente al tema della monetizzazione dei dati personali – cfr. par. 22.1). Insieme alle molteplici attività svolte dal Garante in altri consessi internazionali, *in primis* nel 2024 il G7 e l'annuale riunione delle autorità di protezione dati del G7 a cui si è già fatto cenno (v. *supra*, e capp. 16 e 21), ma anche OCSE e Consiglio d'Europa, e al numero davvero imponente di pronunce rese dalla CGUE a seguito di domande di rinvio pregiudiziale, la dimensione sovranazionale della protezione dei dati si conferma nel 2024 quale fonte primaria di indirizzi unitari e condivisi nella prospettiva di una lenta convergenza – anche rispetto alle iniziative di altri regolatori, quali le autorità per la tutela dei consumatori e della concorrenza – nonché corollario inevitabile della strategia digitale dell'UE nelle sue molteplici declinazioni (si pensi alle attività implementative, iniziate nel 2024, del *Digital Governance Act* e del *Digital Markets Act* – cfr. capp. 2, 21). Assicurare il rispetto delle regole e, soprattutto, dello spirito del RGPD sarà la vera sfida dei prossimi anni nel contesto dell'ambizioso obiettivo della Commissione europea di fare dell'UE un *leader* mondiale in termini di utilizzo e riutilizzo dei dati anche personali.

6. In questo scenario mutevole ma caratterizzato da alcuni punti fermi, come si è cercato di indicare finora, il ruolo del Garante assume in misura crescente le connotazioni di un'autorità non solo di controllo, intenta ad assicurare *ex post* l'osservanza delle normative che è chiamato a sovrintendere, ma anche di un'autorità proattiva che si confronta in modo costruttivo con le sfide eternamente nuove che volta per volta si presentano. Dai controlli remoti sul rispetto da parte dei

EDPB which reflects the implementation experiences of national data protection authorities.Indeed, the EDPB has increasingly, and particularly in 2024, been issuing interpretative guidance on the application of rules through complex opinions (under Article 64(2) GDPR), which have notably concerned the reuse of personal data for training and deploying AI models, facial recognition, and valid consent in business models based on 'Consent or Pay' (the latter being an issue that is clearly linked to the monetization of personal data – see paragraph 22.1). Alongside the many activities carried out by the Garante in other international for a – primarily the G7 and the annual meeting of the G7 data protection authorities already mentioned above (see Chapters 16 and 21), but also within the OECD and the Council of Europe – and in parallel with the very large number of rulings issued by the CJEU following requests for preliminary ruling, the supranational dimension of data protection continued in 2024 to be a primary source of unified and shared guidance, leading to a gradual convergence – also with respect to initiatives by other regulatory authorities such as consumer protection and competition authorities. It also stands as an inevitable corollary of the EU's digital strategy in its various facets: only consider the implementation activities connected with the Digital Governance Act and the Digital Markets Act which started in 2024 – see Chapters 2 and 21. Ensuring compliance with the rules and, above all, with the spirit of the GDPR will be the real challenge of the coming years, in the context of the ambitious goal set by the European Commission - namely, making the EU a global leader in the use and reuse of data, including personal data.

6. In this evolving scenario, where a few landmarks remain nevertheless unchanged as indicated so far, the role of the Garante is increasingly taking on the features not only of a supervisory authority – aiming to ensure *ex-post* compliance with the

siti web delle norme e delle indicazioni del Garante in tema di *cookie* (cfr. par. 12.2), una delle priorità di sempre, alle indicazioni fornite in tema di *web scraping* o di monetizzazione, delle quali si è già fatto cenno, fino alle attività di sensibilizzazione su questioni di grande interesse e delicatezza quali lo *sharenting* o l'uso avvertito delle tecnologie digitali da parte dei minori (dove permane il dibattito sull'individuazione di meccanismi in grado di assicurare la necessaria verifica dell'età) (cfr. cap. 24), il Garante non si è sottratto alla ricerca di soluzioni efficaci o, comunque, a un approccio dialettico che prevede il coinvolgimento degli *stakeholder* pubblici e privati: ne sono un chiaro indizio alcuni eventi pubblici finalizzati a una, se possibile, "democratizzazione" ulteriore del dibattito sui temi della *privacy* (quali lo *State of Privacy* 2024, o i *privacy tour*). Tutto questo passa necessariamente dal potenziamento delle risorse umane e strutturali dell'Autorità, che ha assunto notevole impulso nello scorso anno grazie al reclutamento di nuovo e qualificato personale, alla transizione verso il Polo strategico nazionale con il conseguente rafforzamento del perimetro di sicurezza dei trattamenti, alle iniziative di formazione interna ed esterna che si sono giovate anche delle piattaforme di *e-learning* messe a disposizione delle amministrazioni pubbliche e degli apporti di studio e ricerca interni. Per citare Tomasi di Lampedusa, "Se vogliamo che tutto rimanga com'è, bisogna che tutto cambi": e, dunque, garantire la continuità di princìpi e diritti senza rinunciare a confrontarsi con il nuovo è, forse, il migliore antidoto a un certo gattopardismo che, in momenti di rapido cambiamento, aspira a mantenere lo *status quo* nascondendolo sotto una patina superficiale di novità. In questo senso la vera scommessa continua a essere, anche per il Garante, quella di vivere nel tempo presente pur rimanendo saldamente radicato nell'*humus* costituzionale europeo dei diritti della persona.

regulations it oversees – but also of a proactive authority that engages constructively with the new challenges that arise from time to time. From remote checks of websites' compliance with the Garante's rules and guidance on cookies (see paragraph 12.2), one of the Authority's longstanding priorities, to the guidance issued on web scraping and monetization, as mentioned above, up to awareness-raising activities on topics of great interest and sensitivity such as sharenting or the knowledgeable use of digital technologies by minors (where the debate continues regarding effective age verification mechanisms) (see Chapter 24), the Garante has not shied away from seeking effective solutions or at least keeping up a dialogue with public and private stakeholders. This is clearly shown by some public events aimed at an even greater 'democratization' of the privacy debate (such as the 'State of Privacy 2024' and the 'Privacy Tours'). All of the above necessarily requires strengthening human and structural resources, which gained significant momentum last year thanks to the recruitment of new qualified staff, the transition towards the *Polo strategico nazionale* (National Strategic Hub) with the consequent reinforcement of the security of data processing, and internal and external training initiatives which also relied on e-learning platforms made available to public administrations as well as on the contributions provided by internal study and research activities.To quote the Italian writer Tomasi di Lampedusa, the author of 'The Leopard': 'If we want things to stay as they are, everything must change'. Thus, ensuring the continuity of principles and rights without renouncing to address innovation is perhaps the best antidote to resist the temptation which is rife in times of rapid change – that of applying a thin veneer of innovation whilst secretly holding on to the *status quo*. In this sense, the real challenge for the Garante is still that of engaging with the present while remaining deeply anchored in the European constitutional tradition of human rights.

I

IL QUADRO NORMATIVO E I RAPPORTI CON IL PARLAMENTO E ALTRE ISTITUZIONI

2 Principali novità normative in materia di protezione dei dati personali

Fra i numerosi provvedimenti normativi incidenti, a vario titolo e in diversa misura, sulla materia della protezione dei dati personali, si riportano di seguito i più significativi.

2.1. *Le leggi*

Legge di bilancio 2025

La l. 30 dicembre 2024, n. 207, recante il bilancio di previsione dello Stato per l'anno finanziario 2025 e bilancio pluriennale per il triennio 2025-2027 prevede alcune disposizioni di interesse in materia di protezione dati, tra le quali si segnalano le seguenti:

- il comma 74 dell'art. 1 che, per contrastare l'evasione in materia di pagamenti elettronici, dispone che la memorizzazione elettronica e la trasmissione telematica all'Agenzia delle entrate dei dati relativi ai corrispettivi giornalieri siano effettuate mediante strumenti tecnologici tali da garantire l'inalterabilità e la sicurezza dei dati, nonché la piena integrazione e interazione del processo di registrazione dei corrispettivi con il processo di pagamento elettronico. A tal fine, si precisa che lo strumento *hardware* o *software* mediante il quale sono accettati i pagamenti elettronici debba essere sempre collegato allo strumento mediante il quale sono registrati e memorizzati, in modo puntuale, e trasmessi, in modo aggregato, i dati dei corrispettivi, nonché i dati dei pagamenti elettronici giornalieri;
- il comma 78, dispone che con provvedimenti del direttore dell'Agenzia delle entrate, di approvazione della modulistica fiscale, vengano definite anche le modalità di indicazione del codice identificativo nazionale (CIN) nelle dichiarazioni fiscali e nella certificazione unica;
- il comma 212, che nel prevedere misure di semplificazione dei controlli per l'erogazione delle prestazioni assistenziali da parte dell'INPS, stabilisce che ai fini del riconoscimento ed erogazione dei benefici economici per i quali è richiesta l'esibizione di una fattura, l'Istituto acquisisca e verifichi, in interoperabilità, le informazioni disponibili nella banca di dati dell'Agenzia delle entrate relative alla fatturazione elettronica riferita ai servizi per i quali è concessa la prestazione economica;
- il comma 243, che istituisce presso la Presidenza del Consiglio dei ministri-Dipartimento per le politiche antidroga, il sistema nazionale di allerta rapida, quale strumento di coordinamento operativo delle informazioni di allerta funzionante anche attraverso un dispositivo informatico dedicato e finalizzato alla prevenzione e alla tutela della salute pubblica, in particolare mediante la prevenzione di fenomeni potenzialmente pericolosi correlati alla comparsa di nuove sostanze psicoattive o al consumo di sostanze stupefacenti già vietate;
- i commi 298 e 299, che istituiscono presso l'ISS il registro unico nazionale delle *Breast Unit*, con l'obiettivo di raccogliere tutti i dati provenienti dalle *Breast Unit* nel territorio nazionale e garantire la centralizzazione e l'analisi dei dati relativi alla diagnosi, al trattamento e al *follow up* del carcinoma mammario;

- i commi 317 e 318, che prevedono la dematerializzazione delle ricette mediche cartacee per la prescrizione di farmaci a carico del SSN, dei SASN (servizi territoriali per l'assistenza sanitaria al personale navigante, marittimo e dell'aviazione civile) e dei cittadini.

Legge concorrenza

La legge annuale per il mercato e la concorrenza, 16 dicembre 2024, n. 193, comprende varie disposizioni rilevanti sotto il profilo della protezione dei dati personali, in particolare nel settore assicurativo, introducendo norme in materia di portabilità dei dati delle scatole nere (art. 20) e di contrasto al fenomeno delle frodi assicurative, attraverso il conferimento alle imprese assicurative della facoltà di istituire un sistema informativo sui rapporti assicurativi non obbligatori (art. 21).

L'art. 20, comma 1, vieta, in particolare, l'inserimento di clausole che limitino il diritto dell'assicurato di disinstallare gratuitamente il dispositivo elettronico del veicolo alla scadenza del contratto. Il comma 2, invece, legittima l'assicurato a richiedere gratuitamente al fornitore dei servizi assicurativi telematici alcuni dati (registrati nella scatola nera) relativi alla percorrenza del veicolo negli ultimi dodici mesi, resi accessibili in un formato strutturato e leggibile.

L'art. 21, comma 1, stabilisce che le imprese di assicurazione, anche per il tramite della loro associazione, possano istituire un sistema informativo – alimentato dalle singole compagnie e sottoposto a vigilanza dell'IVASS – sui rapporti assicurativi per i rami diversi dalla responsabilità civile automobilistica, i cui dati possono essere utilizzati per finalità connesse alla liquidazione dei sinistri.

Il comma 2, demanda la disciplina delle modalità di alimentazione e accesso al sistema e delle tipologie di dati trattabili a un reg. dall'IVASS, sentiti il Garante e l'AGCM.

Si segnala infine l'art. 24, che disciplina l'accesso dei clienti domestici vulnerabili al servizio a tutele graduali, demandando all'ARERA la definizione delle modalità di attuazione di quanto ivi previsto, comprese quelle concernenti l'attestazione circa la sussistenza dei requisiti di vulnerabilità.

Codice della strada

La l. 25 novembre 2024, n. 177, recante interventi in materia di sicurezza stradale e delega al Governo per la revisione del codice della strada, presenta molteplici disposizioni di interesse, parte delle quali relative all'utilizzo di strumenti e dispositivi di controllo ai fini dell'accertamento delle violazioni. In particolare, si segnalano le seguenti:

- l'art. 1, che prevede la possibilità, per gli organi di polizia stradale, di sottoporre in determinate circostanze i conducenti ad accertamenti tossicologici analitici su campioni di fluido del cavo orale, nel rispetto della riservatezza personale degli interessati;

- l'art. 10, il quale prevede che:

a) la contestazione immediata della violazione non sia necessaria qualora accertata per mezzo di dispositivi o apparecchiature di rilevamento approvate od omologate ai sensi di appositi regolamenti tenuti a definire anche le condizioni per l'installazione e l'esercizio dei dispositivi di controllo, nonché per l'accesso alle banche di dati necessarie per il loro funzionamento. Ai fini dell'accertamento delle violazioni, la documentazione fotografica prodotta costituisce atto di accertamento, ai sensi e per gli effetti dell'art. 13 della l. 24 novembre 1981, n. 689;

b) i dispositivi possano accertare contemporaneamente due o più violazioni, tra quelle indicate, se approvati od omologati allo scopo, ferma restando l'utilizzabilità delle immagini per l'accertamento, mediante raffronto con banche dati esterne, di altre violazioni per le quali i dispositivi medesimi non siano stati specificamente approvati od omologati;

c) la contestazione immediata non sia necessaria quando le violazioni siano accertate

attraverso la semplice visione delle immagini riprese dagli impianti di videosorveglianza installati lungo le strade. In tali casi, l'accertamento deve essere effettuato direttamente nel momento in cui la violazione viene ripresa dagli impianti di videosorveglianza, con l'acquisizione e conservazione di un filmato avente data e orario certificati dall'operatore di polizia, oppure risultare dalla visione delle registrazioni effettuate nelle ventiquattro ore precedenti al momento dell'accertamento. Con decreto, acquisito il parere del Garante, sono determinate le modalità di acquisizione e conservazione delle registrazioni delle violazioni accertate.

La l. 9 agosto 2024, n. 114, reca modifiche al codice penale, al codice di procedura penale, all'ordinamento giudiziario e al codice dell'ordinamento militare, introducendo limitazioni all'acquisizione di comunicazioni tra imputato e difensore e novellando, in senso più restrittivo, la disciplina sulle intercettazioni.

Il testo della legge, all'art. 2, tiene conto delle indicazioni rese dal Garante nell'ambito dell'audizione tenutasi al Senato il 6 settembre 2023 (doc. web n. 9926529), in particolare sulla trascrizione delle intercettazioni e la tutela dei terzi.

In particolare, la novella dell'art. 1034 c.p.p. estende il divieto di acquisizione da parte dell'Autorità giudiziaria di ogni altra forma di comunicazione, diversa dalla corrispondenza, intercorsa tra l'imputato ed il proprio difensore, salvo sussista fondato motivo di ritenere che si tratti di corpo del reato. Si introduce, inoltre, l'obbligo per l'Autorità giudiziaria o per gli organi ausiliari delegati di interrompere immediatamente le operazioni di intercettazione quando risulta che la conversazione o la comunicazione rientrino tra quelle vietate.

L'art. 2, comma 1, lett. b), modifica il comma 2-*bis* dell'art. 114 c.p.p., introducendo il divieto di pubblicazione, anche parziale, del contenuto delle intercettazioni in tutti i casi in cui esso non sia riprodotto dal giudice nella motivazione di un provvedimento o utilizzato nel corso del dibattimento.

L'art. 2, comma 1, lett. c), modifica poi il comma 1 dell'art. 116 c.p.p., prevedendo il divieto di rilascio di copia delle intercettazioni, delle quali è vietata la pubblicazione, quando la richiesta sia presentata da un soggetto diverso dalle parti e dai loro difensori, salvo l'esigenza (motivata) di utilizzare i risultati delle intercettazioni in altro procedimento specificamente indicato.

L'art. 2, comma 1, lett. d), apporta alcune modifiche all'art. 268 c.p.p., disponendo il divieto di riportare nei verbali di trascrizione delle intercettazioni espressioni che consentano di identificare soggetti diversi dalle parti (n. 1) e l'obbligo di stralcio anche delle registrazioni e dei verbali che riguardano soggetti diversi dalle parti medesime (n. 2).

L'art. 2, comma 1, lett. e), interviene sull'art. 291 c.p.p. vietando d'indicare nella richiesta di misura cautelare, con riguardo alle conversazioni intercettate, i dati personali dei soggetti diversi dalle parti, salvo che ciò sia indispensabile per la compiuta esposizione.

Viene altresì introdotto all'articolo il comma 1-*novies*, nel quale si prevede che il verbale dell'interrogatorio della persona sottoposta alle indagini preliminari sia documentato "integralmente", a pena di "inutilizzabilità, mediante riproduzione audiovisiva o, se non disponibile, fonografica (art. 141-*bis*).

Di particolare interesse, infine, risulta l'art. 3, che nel recare modifiche all'art. 89-*bis* disp. att. c.p.p., relativo all'archivio delle intercettazioni, estende l'applicazione del comma 2, art. 89-*bis* anche ai dati personali relativi a soggetti diversi dalle parti, in modo da realizzare un necessario coordinamento normativo con le modifiche introdotte all'art. 268.

L'art. 89-*bis*, comma 2, prevede infatti che l'archivio digitale "è gestito con modalità

tali da assicurare la segretezza della documentazione relativa alle intercettazioni non necessarie per il procedimento, ed a quelle irrilevanti o di cui è vietata l'utilizzazione ovvero riguardanti categorie particolari di dati personali come definiti dalla legge o dal regolamento in materia. Il Procuratore della Repubblica impartisce, con particolare riguardo alle modalità di accesso, le prescrizioni necessarie a garantire la tutela del segreto su quanto ivi custodito".

Cybersicurezza e reati informatici

La l. 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e dei reati informatici, introduce disposizioni volte a conseguire una più elevata capacità di protezione e risposta di fronte alle emergenze cibernetiche.

In particolare, l'art. 1 prevede l'obbligo di notifica degli incidenti aventi impatto su reti, sistemi informativi e sistemi informatici, da parte delle p.a. centrali, le regioni e le province autonome di Trento e Bolzano, i comuni e le aziende sanitarie locali.

L'art. 9 – in linea con le indicazioni del Garante (v. audizione 22 marzo 2024, doc. web n. 9995952) – attribuisce alle strutture preposte all'attività di cybersicurezza nelle p.a. il compito di verificare che i programmi e le applicazioni informatiche di comunicazione elettronica rispettino le linee guida sulla crittografia, nonché quelle sulla conservazione delle *password* adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante e che non presentino vulnerabilità note, tali da rendere disponibili e intellegibili a terzi i dati cifrati.

L'art. 16 novella il delitto di cui all'art. 615-*ter* c.p. (accesso abusivo ad un sistema informatico o telematico), con l'aumento della cornice edittale per le ipotesi aggravate e l'introduzione di ulteriori condotte rilevanti. In particolare si qualifica come aggravata la condotta di chi sottrae, anche mediante riproduzione o trasmissione, ovvero renda inaccessibili al titolare, i dati, le informazioni o i programmi contenuti nel sistema informatico o telematico.

Contrasto al bullismo e al cyberbullismo

La l. 17 maggio 2024, n. 70, che delega il Governo ad adottare misure tese a prevenire e contrastare il fenomeno del bullismo e del cyberbullismo, interviene novellando la l. 29 maggio 2017, n. 71.

L'art. 1 in primo luogo introduce la definizione di bullismo, per tale intendendosi l'aggressione o la molestia reiterate, da parte di una singola persona o di un gruppo di persone, in danno di un minore o di un gruppo di minori, idonee a provocare sentimenti di ansia, timore, isolamento o emarginazione, attraverso atti o comportamenti vessatori, pressioni o violenze fisiche o psicologiche, istigazione al suicidio o all'autolesionismo, minacce o ricatti, furti o danneggiamenti, offese o derisioni.

Lo stesso articolo estende al bullismo il perimetro applicativo della l. 29 maggio 2017, n. 71, ponendo l'accento sulle azioni di carattere preventivo e privilegiando quelle di carattere formativo ed educativo, in una pluralità di ambiti (scolastico, sportivo, ecc.), anche attraverso il coinvolgimento degli esercenti la responsabilità genitoriale nell'orientamento al corretto utilizzo delle tecnologie, e prevedendo campagne informative di prevenzione e sensibilizzazione.

L'articolo prevede poi, nell'ambito del piano di azione integrato per il contrasto ai fenomeni di bullismo e del cyberbullismo, l'istituzione di un apposito tavolo tecnico, con possibilità per il Garante di collaborare alla predisposizione di periodiche campagne informative di prevenzione e di sensibilizzazione, anche a fini di diffusione della conoscenza dei sistemi di controllo parentale, avvalendosi dei principali *media*, degli organi di comunicazione e di stampa, nonché di soggetti privati.

La disposizione novella poi l'art. 5 della legge del 2017, imponendo – con clausola di salvaguardia per l'integrazione di estremi di reato – al dirigente scolastico che venga a conoscenza di atti di bullismo e cyberbullismo, realizzati anche in forma non

telematica, che coinvolgano a qualsiasi titolo studenti iscritti nel proprio istituto scolastico, di seguire le procedure previste dalle linee di orientamento ministeriale.

La novella conferma inoltre le disposizioni vigenti circa il procedimento in camera di consiglio e il regime delle spese, ma aggiunge che ogni provvedimento deve essere preso previo ascolto del minore (anche infradodicenne, se capace di discernimento), dei genitori o degli esercenti la responsabilità genitoriale.

L'art. 3, infine, reca una delega legislativa al Governo per l'adozione di disposizioni in materia di prevenzione e contrasto del bullismo e del cyberbullismo. Tra i princìpi e criteri direttivi della delega si segnalano: la promozione di iniziative tese a prevedere un servizio di sostegno psicologico agli studenti; la predisposizione di piattaforme di formazione e monitoraggio destinate alle scuole; il potenziamento del servizio per l'assistenza alle vittime mediante il numero pubblico "emergenza infanzia 114".

Legge di delegazione europea

La l. 21 febbraio 2024, n. 15, recante la delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – legge di delegazione europea 2022-2023 – contiene diverse disposizioni di interesse in materia di protezione dati, tra le quali si segnalano, in particolare, le seguenti:

- l'art. 3, recante delega legislativa per il recepimento della dir. (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del reg. (UE) 910/2014 e della dir. (UE) 2018/1972 e che abroga la dir. (UE) 2016/1148 (dir. NIS2). In particolare si segnala che, per quanto riguarda l'attuazione della NIS2, il decreto legislativo è tenuto a individuare i criteri in base ai quali un ente pubblico può essere considerato p.a. ai fini dell'applicazione delle disposizioni della direttiva e poi definire le esclusioni di particolari soggetti. In base alle nuove regole della direttiva, gli Stati membri devono definire entro il 17 aprile 2025 un elenco dei soggetti essenziali e importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio, da riesaminare e aggiornare ogni due anni;

- l'art. 4, recante delega legislativa per garantire l'integrale e compiuto adeguamento alla dir. (UE) 2016/343 sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali, novellando l'art. 114 c.p.p, relativamente al divieto di pubblicazione integrale o per estratto del testo dell'ordinanza di custodia cautelare finché non siano concluse le indagini preliminari ovvero fino al termine dell'udienza preliminare;

- l'art. 7, recante delega legislativa per il recepimento della dir. (UE) 2021/2167, relativa ai gestori di crediti e agli acquirenti di crediti e che modifica le dir. 2008/48/CE e 2014/17/UE, e dell'opportuno coordinamento tra la disciplina nazionale in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e quella di recepimento della medesima direttiva.

Nell'esercizio della delega, è previsto che il Governo garantisca la coerenza tra la disciplina nazionale di recepimento e il quadro normativo unionale in materia di tutela dei consumatori e dei debitori, nonché con le norme in materia di protezione dei dati personali;

- l'art. 17, recante delega legislativa per l'adeguamento della normativa nazionale alle disposizioni del reg. (UE) 2022/868 (cd. *Data Governance Act*). In particolare, si delega il Governo ad adottare – dopo aver acquisito il parere del Garante (successivamente reso il 12 settembre 2024, n. 571, doc. web n. 10105175) – uno o più decreti legislativi, tesi ad introdurre norme di coordinamento delle disposizioni unionali con il sistema normativo interno vigente nella materia, più contigua, della protezione dei dati personali, per evitare dubbi interpretativi o contrasti tra norme (con riguardo, tra

l'altro, ai presupposti di liceità per la trasmissione a terzi di dati personali a fini di riutilizzo e all'introduzione di norme di raccordo con il sistema sanzionatorio). In tale articolo il legislatore ha tra l'altro recepito buona parte delle indicazioni fornite dal Garante al Governo nel mese di marzo 2023, accogliendo alcuni criteri per l'esercizio della delega. L'articolo, tuttavia, al contrario di quanto richiesto dal Garante, non prevede l'indicazione dell'autorità competente (v. *infra,* quanto ai contenuti del decreto legislativo in questione);

- l'art. 19, recante delega legislativa per l'adeguamento alle disposizioni del reg. (UE) 2023/1114, relativo ai mercati delle cripto-attività e che modifica i reg. (UE) 1093/2010 e 1095/2010 e le dir. 2013/36/UE e 2019/1937/UE, cd. MiCAR (*Markets in Crypto-Assets Regulation*). In tale ambito, tra i criteri di delega (n. 8), si prevede che il Governo debba disciplinare la comunicazione tra l'Autorità giudiziaria, la Banca d'Italia e la CONSOB, secondo le rispettive competenze, dei dati in forma anonima e aggregata riguardanti le indagini penali intraprese e le sanzioni penali imposte in relazione alle violazioni previste dall'art. 111 del medesimo reg., ai fini della segnalazione all'Autorità bancaria europea (ABE) e alla *European securities and markets authority* (ESMA).

2.2. *I decreti-legge*

Lavoro e università

La l. 20 dicembre 2024, n. 199, ha convertito, con modificazioni, il d.l. 28 ottobre 2024, n. 160, recante disposizioni urgenti in materia di lavoro, università, ricerca e istruzione per una migliore attuazione del PNRR, il quale presenta tra gli articoli di interesse l'art. 1, comma 11, che rimette all'Ispettorato nazionale del lavoro (INL), nel rispetto della vigente normativa in materia di tutela dei dati personali, la definizione delle modalità tecniche per assicurare alle p.a. ed agli enti che erogano o gestiscono fondi pubblici la possibilità di accedere al Portale nazionale del sommerso, per le finalità di verifica nelle attività di propria competenza, rinviando a uno o più decreti ministeriali l'individuazione dei dati oggetto di condivisione nell'ambito del medesimo Portale, nonché dei soggetti abilitati ad accedervi.

Decreto flussi

La l. 9 dicembre 2024, n. 187, ha convertito, con modificazioni, il d.l. 11 ottobre 2024, n. 145, recante disposizioni urgenti in materia di ingresso in Italia di lavoratori stranieri, di tutela e assistenza alle vittime di caporalato, di gestione dei flussi migratori e di protezione internazionale, nonché dei relativi procedimenti giurisdizionali.

Il decreto, all'art. 1, introduce modifiche concernenti, in particolare, la disciplina dei procedimenti relativi al lavoro subordinato, anche a carattere stagionale e segnatamente a taluni profili di carattere procedurale, del d.lgs. n. 286/1998 (TUI), in materia di procedure di ingresso di cittadini stranieri, nel territorio nazionale, per motivo di lavoro.

Le modifiche prevedono la digitalizzazione di talune fasi del procedimento amministrativo, in attuazione di quanto previsto dall'art. 12, d.lgs. n. 82/2005 (CAD).

In particolare, relativamente al primo articolo si segnalano le seguenti previsioni:

- si estende ai visti nazionali l'obbligo di acquisizione dei dati biometrici, attualmente previsto per i soli visti Schengen in base al codice visti di cui al reg. UE 810/2009 (art. 1, comma 1, lett. a), n. 1);

- viene novellato l'art. 22, comma 2, TUI, prevedendosi, in relazione alla fase iniziale del procedimento di rilascio del nulla osta al lavoro subordinato, l'obbligo, per il datore di lavoro, di trasmettere allo sportello unico per l'immigrazione il certificato di idoneità alloggiativa, l'asseverazione di cui all'art. 24-*bis* del testo unico,

in originale digitale, nonché il domicilio digitale di cui agli artt. 6-*bis* e 6-*ter* del CAD volto ad assicurare la disponibilità, in capo allo sportello unico per l'immigrazione, di una PEC del datore di lavoro cui inviare e ricevere, con ogni valore legale, tutte le comunicazioni di interesse dell'amministrazione (art. 1, comma 1, lett. e), n. 1).

Particolare rilevanza assume l'art. 12, che introduce l'obbligo per il richiedente asilo di cooperare con le autorità ai fini dell'accertamento dell'identità e di esibire o produrre gli elementi disponibili relativi all'età, all'identità, alla cittadinanza, nonché al paese o ai paesi in cui ha soggiornato o è transitato in precedenza e consentendo, qualora sia necessario ai fini dell'acquisizione di tali elementi, l'accesso ai dispositivi o supporti elettronici o digitali in suo possesso (comma 1).

La novella prevede inoltre che il questore, in caso di inosservanza dell'obbligo di cooperazione da parte dello straniero, possa disporre, al solo fine di acquisire gli elementi relativi all'età, all'identità e alla cittadinanza, nonché ai paesi in cui ha soggiornato, che gli ufficiali o agenti di pubblica sicurezza procedano all'accesso immediato ai dati identificativi dei dispositivi elettronici e delle eventuali schede elettroniche o digitali in suo possesso, nonché all'accesso dei video e audio esclusi quelli comunicativi contenuti nei dispositivi mobili (anche di minori) a fini identificativi nell'ambito dei procedimenti per il riconoscimento della protezione internazionale, con convalida giudiziale e inutilizzabilità dei dati in sua assenza (art. 12, comma 2, lett. a)).

La l. 8 agosto 2024, n. 112, ha convertito, con modificazioni, il d.l. 4 luglio 2024, n. 92, recante misure urgenti in materia penitenziaria, di giustizia civile e penale e di personale del Ministero della giustizia.

Il decreto stabilisce, all'art. 6-*bis*, comma 1, che il Ministero della salute e il Ministero della giustizia conferiscano reciprocamente, tramite interoperabilità ai sensi del CAD, i dati conservati nelle banche dati relative ai flussi, rispettivamente, del Sistema informativo per le dipendenze (SIND) e del Sistema informativo per la salute mentale (SISM), nell'ambito del Nuovo sistema informativo sanitario (NSIS), e del Sistema informativo anagrafica penitenziaria SIAP/AFIS, limitatamente ai soggetti detenuti affetti da patologia da dipendenza o da patologia psichica diagnosticate, esclusivamente per finalità legate al costante monitoraggio dell'attività dei servizi dell'amministrazione penitenziaria e delle prestazioni del SSN, all'analisi dell'andamento delle misure e degli esiti dei programmi di trattamento, al supporto alle attività gestionali dei servizi dell'amministrazione penitenziaria, nonché all'emanazione delle direttive tecniche per l'intervento dei servizi dell'amministrazione penitenziaria, alla produzione di dati aggregati e di analisi statistiche e alla redazione di relazioni o rapporti richiesti dalle Camere o da organismi europei o internazionali.

I commi 2 e 3 qualificano quali titolari dei rispettivi trattamenti il Ministero della giustizia - Dipartimento per l'amministrazione penitenziaria, e il Ministero della salute - Direzione generale competente in materia di prevenzione sanitaria per le dipendenze e la salute mentale.

Il comma 4 richiama la disciplina nel cui rispetto deve essere effettuato il trattamento, mentre il comma 5 demanda a un decreto del Ministro della giustizia la definizione delle categorie di interessati, del responsabile del trattamento, dei soggetti cui possono essere comunicati i dati, delle operazioni di trattamento, nonché delle misure appropriate e specifiche per tutelare i diritti degli interessati.

Il comma 6 demanda ad altro decreto del Ministro della giustizia, di concerto con il Ministro della salute e sentito il Garante, l'individuazione, ai fini dell'interoperabilità dei sistemi e limitatamente ai trattamenti o alle categorie di trattamenti non occasionali di cui all'art. 5, comma 1, d.lgs. n. 51/2018, dei termini, delle modalità di conservazione

dei dati, dei soggetti legittimati ad accedervi, delle condizioni di accesso e dei relativi sistemi di autenticazione, delle modalità di consultazione, dei requisiti tecnici essenziali del flusso informativo, delle sue modalità procedurali e di ogni altra specifica tecnica necessaria ad assicurare autenticità, integrità e riservatezza dei dati medesimi, delle misure di sicurezza da approntare in relazione ai distinti fattori di rischio, delle modalità di predisposizione del documento di valutazione di impatto di cui all'art. 35 del RGPD, nonché delle modalità e delle condizioni per l'esercizio dei diritti di cui agli artt. 9, 10, 11 e 13, d.lgs. n. 51/2018.

Attuazione PNRR

La l. 29 aprile 2024, n. 56, ha disposto la conversione in legge, con modificazioni, del d.l. 2 marzo 2024, n. 19, recante ulteriori disposizioni urgenti per l'attuazione del PNRR.

Il decreto introduce disposizioni di varia natura per l'attuazione del PNRR, alcune delle quali rivestono particolare interesse in materia di protezione dati, tra cui quelle in materia di digitalizzazione (Capo V), e, in particolare, di delega per l'accesso ai servizi *online* della p.a., di Sistema di portafoglio digitale – sentito il Garante – e di Anagrafe nazionale dell'istruzione superiore (art. 20), di digitalizzazione dei servizi di trasporto merci e/o passeggeri (art. 20-*bis*) e di digitalizzazione e dematerializzazione documentale delle p.a. (art. 21), di informatizzazione dell'albo dei periti (art. 22), di notificazione tramite mezzi telematici (art. 25-*bis*), di casellario giudiziale, casellario giudiziale europeo, anagrafe delle sanzioni amministrative dipendenti da reato e relativi carichi pendenti (art. 26), in materia di sanità digitale (art. 42).

In particolare, quest'ultimo articolo disciplina il FSE, i sistemi di sorveglianza nel settore sanitario e governo della sanità digitale, al fine di rimodulare il ruolo svolto da AGENAS, quale Agenzia per la sanità digitale (ASD) per garantire che la Piattaforma nazionale di telemedicina (PNT) possa svolgere funzioni di governo della sanità digitale, di programmazione dello sviluppo della telemedicina, di ricerca, con l'utilizzo dell'IA, nonché di valutazione delle tecnologie sanitarie (*Health Technology Assessment* - HTA) relative ai dispositivi medici.

Altre disposizioni di interesse riguardano le modalità tecnologiche per la raccolta, l'elaborazione e l'analisi dei dati sanitari (definite tramite decreto ministeriale su cui è previsto il parere del Garante), al fine di assicurare l'aggiornamento del FSE (art. 43), e, soprattutto, le modifiche apportate all'art. 2-*sexies* del Codice (art. 44).

Viene introdotta, infatti, una nuova formulazione del comma 1-*bis* dell'art. 2-*sexies* del Codice, secondo cui i dati personali relativi alla salute sono trattati, in forma pseudonimizzata e anche mediante interconnessione, dal Ministero della salute, dall'Istituto superiore di sanità (ISS), dall'Agenzia nazionale per i servizi sanitari regionali (AGENAS), dall'Agenzia italiana del farmaco (AIFA), dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà (INMP), nonché, relativamente ai propri assistiti, dalle regioni e dalle province autonome.

Si aggiunge, inoltre, il comma 1-*ter*, che demanda a uno o più decreti ministeriali, da emanarsi su parere del Garante, la disciplina dell'interconnessione dei sistemi informativi tra le amministrazioni coinvolte, nonché le garanzie di sicurezza del trattamento.

Si novella, inoltre, la disposizione di cui all'art. 110 del Codice, sopprimendo l'obbligo di consultazione preventiva del Garante per il trattamento dei dati sulla salute a fini di ricerca medica, biomedica ed epidemiologica nei casi in cui non sia possibile informare gli interessati e acquisirne un valido consenso, demandando all'Autorità l'individuazione delle garanzie da osservare ai sensi dell'art. 106, comma 2, lett. d), del Codice.

2.3. *I decreti legislativi*

Controllo del denaro contante

Il d.lgs. 10 dicembre 2024, n. 211, recante adeguamento della normativa nazionale alle disposizioni del reg. (UE) 2018/1672, relativo ai controlli sul denaro contante in entrata nell'Unione o in uscita dall'Unione, sul cui schema il Garante ha reso parere il 26 settembre 2024 (cfr. par. 3.1.2), è stato adottato nell'esercizio della delega legislativa conferita al Governo dall'art. 15 della l. 21 febbraio 2024 n. 15 (legge di delegazione europea 2022-2023) (cfr. par. 2.1) e novella la l. 17 gennaio 2000, n. 7, recante la disciplina del mercato dell'oro, il d.P.R. 26 ottobre 1972, n. 633 al fine di eliminare i riferimenti all'ufficio italiano dei cambi (da tempo soppresso), nonché il d.lgs. 19 novembre 2008, n. 195, recante modifiche e integrazioni alla normativa valutaria.

In particolare, si dispone che lo scambio di informazioni tra l'Agenzia delle dogane e dei monopoli, la Guardia di finanza e le omologhe autorità competenti degli Stati UE avvenga attraverso il Sistema di informazioni doganali (SID) e che, qualora emergano indizi di attività criminose correlate a denaro contante, suscettibili di arrecare pregiudizio agli interessi finanziari dell'UE, le medesime informazioni siano trasmesse anche alla Commissione UE, alla Procura europea e a EUROPOL (lett. h).

Di particolare interesse risulta la lett. i) dell'art. 2, che introduce al d.lgs. n. 195/2008 l'art. 5-*bis*, recante norme in materia di trattamento dei dati personali, legittimandolo per le sole finalità di prevenzione delle attività criminose e consentendo l'accesso alle informazioni al solo personale debitamente autorizzato delle autorità competenti (salvi obblighi comunicativi previsti dal diritto interno), che ne garantiscono la sicurezza.

I commi 3 e 4 dell'art. 5-*bis* legittimano le autorità competenti a conservare i dati personali per un periodo di cinque anni dalla data in cui sono stati ottenuti, prorogabili una sola volta per un periodo non superiore a tre anni, al ricorrere di ipotesi indicate, con obbligo di cancellazione una volta decorso il termine.

Digital Governance Act

Il d.lgs. 7 ottobre 2024, n. 144, reca norme di adeguamento della normativa nazionale alle disposizioni del reg. (UE) 2022/868, relativo alla *governance* europea dei dati (DGA).

Il decreto, sul cui schema il Garante ha reso parere il 12 settembre 2024 (cfr. par. 3.1.2), è stato adottato nell'esercizio della delega prevista dall'art. 17 della l. 21 febbraio 2024, n. 15 (legge di delegazione europea 2022-2023) (cfr. par. 2.1). Per quanto di interesse, esso prevede la designazione di AgID quale autorità competente per i servizi di intermediazione dei dati e per la registrazione di organizzazioni per l'altruismo dei dati, nonché quale organismo competente per l'assistenza agli enti pubblici che concedono o rifiutano l'accesso al riutilizzo dei suddetti dati, individuandola come sportello unico per l'implementazione delle relative funzioni, nel rispetto delle disposizioni in materia di protezione dei dati personali e delle competenze del Garante, dell'ACN e dell'AGCM, disciplinando anche il regime sanzionatorio.

Disabilità

Il d.lgs. 3 maggio 2024, n. 62, costituisce esercizio della delega di cui all'art. 1, comma 5, lett. a), b), c), d) e h), l. 22 dicembre 2021, n. 227, relativa alla revisione e al riordino delle disposizioni in materia di disabilità.

Il decreto, sul cui schema il Garante ha reso parere il 22 febbraio 2024 (cfr. par. 3.1.2), mira a garantire alla persona disabile il riconoscimento della propria condizione, anche attraverso un procedimento valutativo "congruente, trasparente e agevole" che consenta "il pieno esercizio dei suoi diritti civili e sociali" e, in particolare, "il diritto alla vita indipendente e alla piena inclusione sociale e lavorativa", favorendo "l'effettivo e pieno accesso al sistema dei servizi, delle prestazioni, dei trasferimenti finanziari previsti e di ogni altra relativa agevolazione", nonché a promuovere l'autodeterminazione

della persona nel rispetto, tra gli altri, del principio di non discriminazione.

Il Capo II disciplina la procedura di accertamento della condizione di disabilità e quella di rivisitazione dei processi valutativi, anche ai fini dell'inclusione lavorativa, dell'individuazione degli elementi utili alla definizione della condizione di non autosufficienza e disabilità gravissima, nonché della definizione dei requisiti necessari per l'accesso ad agevolazioni fiscali, tributarie e relative alla mobilità (art. 5).

L'art. 6 scandisce le fasi del procedimento per la valutazione di base, attivato con la trasmissione del certificato medico introduttivo e concluso con l'acquisizione, al FSE, del certificato con validità illimitata nel tempo ovvero con indicazione del termine.

L'art. 8 prevede che il certificato medico introduttivo di base rappresenti il documento unitario in grado di avviare la sequenza procedimentale per l'accertamento di base della condizione di disabilità, da inserire, attraverso la trasmissione all'INPS, anche nel FSE.

L'art. 16, infine, ascrive all'INPS il compito di garantire l'interoperabilità delle banche dati esistenti alimentate da dati relativi a uno o più elementi del procedimento unitario di valutazione di base, nonché dai dati inerenti comunicazioni e informazioni relative alla conclusione del procedimento stesso.

In linea con i rilievi resi dall'Autorità il 22 febbraio 2024, si prevede il parere del Garante sulla determinazione del direttore generale INPS, da adottarsi per garantire l'interoperabilità delle banche dati esistenti, tra cui anche il FSE.

Comunicazioni elettroniche

Il d.lgs. 24 marzo 2024, n. 48, reca disposizioni correttive e di aggiornamento del d.lgs. 1° agosto 2003, n. 259, come modificato dal d.lgs. 8 novembre 2021, n. 207, di recepimento della dir. (UE) 2018/1972, istitutiva del codice europeo delle comunicazioni elettroniche.

Il decreto, adottato nell'esercizio della delega legislativa di cui all'art. 4, l. 22 aprile 2021, n. 53 (legge di delegazione europea 2019-2020), aggiorna il codice delle comunicazioni elettroniche di cui al d.lgs. 1° agosto 2003, n. 259, In merito alle disposizioni di interesse si segnalano:

- l'art. 1, comma 1, lett. a), che sopprime dalla definizione dell'ambito di applicazione del Codice il riferimento ai servizi di comunicazione elettronica a uso privato, apportando inoltre al comma 2, numerose modifiche alle definizioni o introducendone di nuove (tra le altre, quelle di *access point*, *call center*, codice di abilitazione e identificazione, Mac Address (*Media access control address*), radio digitale e SSID (*Service set identifier*);

- l'art. 1, comma 38, relativo alle procedure e agli obblighi per le imprese relativi all'identificazione degli utenti della telefonia mobile in sede di sottoscrizione dei contratti. In particolare, si prevede che il Ministero dell'interno e l'autorità nazionale di regolamentazione assicurino che i clienti siano identificati prima dell'attivazione, anche di singole componenti dei servizi, al momento della consegna o messa a disposizione della scheda elettronica (SIM) o della fornitura del profilo nel caso di eSIM digitale con obbligo per le imprese, nei casi di nuova attivazione e di portabilità del numero o cambio della SIM, di adottare tutte le necessarie misure affinché venga garantita l'acquisizione dei dati anagrafici del titolare del contratto, riportati su un documento di identità, nonché del tipo e del numero, acquisendone copia.

Inoltre, le medesime imprese devono assicurare il corretto trattamento dei dati acquisiti, fatto salvo il caso in cui per l'identificazione del cliente vengano utilizzati sistemi di identità digitale equipollenti ai documenti d'identità.

Riforma fiscale

- Concordato preventivo biennale. Il d.lgs. 12 febbraio 2024, n. 13, recante disposizioni in materia di accertamento tributario e di concordato preventivo biennale, sul cui schema il Garante ha reso parere l'11 gennaio 2024 (cfr. par. 3.1.2), è stato adottato

nell'esercizio della delega di cui all'art. 17 della l. 11 agosto 2023, n. 111 (delega al Governo per la riforma fiscale). Tra le disposizioni di interesse per la protezione dei dati, si segnalano le seguenti:

- l'art. 2, che dispone la razionalizzazione e il riordino organico delle norme che disciplinano le attività di analisi del rischio nel settore fiscale. Oltre a individuare gli scopi sottesi all'attività di analisi del rischio fiscale (prevenzione e contrasto dell'evasione fiscale, della frode fiscale e dell'abuso del diritto in materia tributaria, nonché stimolo dell'adempimento spontaneo e svolgimento dei controlli preventivi), la norma ribadisce la possibilità di utilizzare allo scopo, in maniera integrata, le informazioni presenti nelle banche dati di cui dispone l'Agenzia delle entrate, anche attraverso l'interconnessione con altri archivi pubblici gestiti da enti non appartenenti all'amministrazione finanziaria, esclusi tuttavia quelli nella disponibilità dell'Autorità giudiziaria (penale) o delle forze di polizia.
- l'art. 8, che impone all'Agenzia delle entrate, entro il 15 marzo di ciascun anno, di mettere a disposizione dei contribuenti o dei loro intermediari, anche mediante l'utilizzo delle reti telematiche, appositi programmi informatici per l'acquisizione dei dati necessari per l'elaborazione della proposta di concordato preventivo biennale, demandando l'individuazione delle modalità e dei dati da comunicare all'amministrazione finanziaria a uno specifico provvedimento del direttore dell'Agenzia delle entrate.
- l'art. 9, secondo cui la proposta di concordato dev'essere elaborata, tenuto conto dei dati dichiarati dal contribuente, sulla base di una metodologia che valorizzi, anche attraverso processi decisionali automatizzati, le informazioni già nella disponibilità dell'amministrazione finanziaria, così da limitare l'introduzione di nuovi oneri dichiarativi.

L'individuazione di tale metodologia, predisposta tenendo conto degli andamenti economici e dei mercati, delle redditività individuali e settoriali desumibili dagli indici sintetici di affidabilità fiscale, nonché dei limiti imposti dalla normativa di tutela dei dati personali, è demandata a uno specifico decreto del Ministro dell'economia e delle finanze, sentito il Garante.

Con il medesimo decreto dovranno essere individuate anche le specifiche cautele e le garanzie per i diritti e le libertà dei contribuenti, nonché le eventuali tipologie di dati esclusi dal trattamento, fermo restando che, ai fini dell'elaborazione della proposta di concordato, l'Agenzia delle entrate, oltre ai dati dichiarati dal contribuente, potrà acquisirne ulteriori dalle banche dati nella disponibilità dell'Amministrazione finanziaria e di altri soggetti pubblici, con l'eccezione di quelle soggette alla disciplina di cui al d.lgs. 18 maggio 2018, n. 51.

- Adempimento collaborativo. Il d.lgs. 5 agosto 2024, n. 108, reca invece disposizioni integrative e correttive in materia di regime di adempimento collaborativo, razionalizzazione e semplificazione degli adempimenti tributari e concordato preventivo biennale. Il decreto, sul cui schema il Garante ha reso parere il 4 luglio 2024 (cfr. par. 3.1.2), reca tra le disposizioni di interesse l'art. 2, il cui comma 4 estende agli altri soggetti incaricati della trasmissione telematica delle dichiarazioni la possibilità di rendere disponibile la dichiarazione precompilata; le modalità di accesso a tale dichiarazione saranno disciplinate con provvedimenti annuali dell'Agenzia delle entrate sottoposti al parere del Garante.

Il medesimo articolo, al comma 6, lett. b), impone all'Agenzia delle entrate, per quanto attiene ai contenuti conoscitivi relativi al cd. cassetto fiscale, di mettere a disposizione dei contribuenti, all'interno di un'apposita area riservata del sito, anche alcuni dati, atti e comunicazioni relativi al medesimo contribuente e che sono comunicati all'Agenzia da altri soggetti, secondo modalità già approvate dal Garante.

2

La lett. c) del medesimo comma sopprime, invece, il riferimento all'"importo complessivo" dei corrispettivi giornalieri anonimi di cui all'art. 2, comma 1, d.lgs. 5 agosto 2015, n. 127 da memorizzare e trasmettere telematicamente all'Agenzia delle entrate, consentendo così il ricorso a soluzioni s*oftware* installate su qualsiasi dispositivo che garantiscano la sicurezza e l'inalterabilità dei dati memorizzati e trasmessi, nonché la piena integrazione e interazione del processo di registrazione dei corrispettivi con il processo di pagamento elettronico, nel caso in cui l'operazione commerciale preveda tale modalità di pagamento.

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 in materia di protezione dei dati personali ha determinato un notevole incremento, di tipo qualitativo oltre che quantitativo, nell'attività consultiva del Garante (artt. 36, par. 4, e 57, par. 1, lett. c), cons. n. 96, RGPD; art. 28, par. 2, dir. UE 2016/680; art. 24, comma 2, d.lgs. n. 51/2018), contribuendo in tali sedi ad un più corretto bilanciamento dei diritti.

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

Nel 2024 sono stati numerosi i casi di consultazione del Garante su atti normativi primari, anche in sede di conversione di decreti-legge. Per tali forme di consultazione dell'Autorità è, infatti, sempre più frequente il ricorso allo strumento dell'audizione parlamentare, che offre anche la possibilità di un dialogo diretto, mediante il dibattito successivo alla relazione, tra le Commissioni parlamentari competenti e il Garante.

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

a) audizione dinanzi alla 4ª Commissione politiche dell'Unione europea del Senato, nell'ambito dell'esame del d.d.l. AS 1258 recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - legge di delegazione europea - 19 novembre 2024 (doc. web n. 10126639);

b) audizione dinanzi alla I Commissione affari costituzionali della Camera nell'ambito dell'esame del d.l. n. 145/2024 recante disposizioni urgenti in materia di ingresso in Italia di lavoratori stranieri, di tutela e assistenza alle vittime di caporalato, di gestione dei flussi migratori e di protezione internazionale, nonché dei relativi procedimenti giurisdizionali - 24 ottobre 2024 (doc. web n. 10066888);

c) audizione dinanzi alle Commissioni riunite 8ª Commissione ambiente e 10ª nell'ambito dell'esame del dd.l. AS 1146, recante disposizioni e delega al Governo in materia di IA - 24 luglio 2024 (doc. web n. 1003798);

d) audizione dinanzi alla II Commissione giustizia della Camera, nell'ambito dell'esame del d.d.l. AC 1974, recante modifiche all'art. 132 del Codice in materia di protezione dei dati personali, di cui al d.lgs. 30 giugno 2003, n. 196, concernenti l'acquisizione di dati relativi al traffico telefonico e telematico per esigenze di tutela della vita e dell'incolumità fisica del soggetto interessato - 18 luglio 2024 (doc. web n. 10036428);

e) audizione dinanzi alla 8ª Commissione ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica del Senato, nell'ambito dell'esame dei d.d.l. nn 1136, 1160 e 1166 recanti disposizioni in materia di tutela dei minori nella dimensione digitale – 10 luglio 2024 (doc. web n. 10034485);

f) audizione dinanzi alla Commissioni riunite I affari costituzionali e II giustizia della Camera nell'ambito dell'esame del d.d.l. AC 1660, recante disposizioni in materia di

sicurezza pubblica, di tutela del personale in servizio, nonché di vittime dell'usura e di ordinamento penitenziario - 16 maggio 2024 (doc. web n. 10014236);

g) audizione dinanzi alle Commissioni riunite I affari costituzionali e II giustizia della Camera, nell'ambito dell'esame del d.d.l. AC. 1717 Governo, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici - 22 marzo 2024 (doc. web n. 9995952).

Non sono mancate richieste di contributi anche nell'ambito dell'esercizio delle funzioni conoscitiva, di indirizzo e controllo delle Camere. Si segnalano, in particolare, quelli di seguito riportati:

a) audizione dinanzi alla XI Commissione lavoro della Camera, nell'ambito dell'indagine conoscitiva in materia di Rapporto IA - Lavoro – 7 maggio 2024 (doc. web n. 10011530);

b) audizione dinanzi alla Commissione XII affari della Camera, nell'ambito dell'esame delle risoluzioni Loizzo n. 7-00183 e Girelli n. 7-00183, in materia di raccolta e utilizzo dei dati sanitari - 13 febbraio 2024 (doc. web n. 9983067);

c) memoria resa alla X Commissione attività produttive, commercio e turismo della Camera, nell'ambito dell'indagine conoscitiva sull'IA: opportunità e rischi per il sistema produttivo italiano - 7 febbraio 2024 (doc. web n. 9982816).

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 formulati si segnalano, in particolare, i seguenti:

a) parere 12 dicembre 2024, n. 790, reso alla Presidenza del Consiglio dei ministri sulle proposte emendative n. 8.085 (Del Barba), n. 8.084 (De Bertoldi), 8.0154 (Tenerini), 8.0155 (Mazzella) e 8.0156 (Cannizzaro), presentate al d.d.l. di bilancio per il triennio 2025-2027 (AC 2112-*bis*) in materia di catasto edilizio urbano (doc. web n. 10097373). Gli emendamenti prevedevano l'aggiunta delle planimetrie delle unità immobiliari urbane tra gli elementi costitutivi del nuovo catasto edilizio urbano, attualmente circoscritti allo schedario delle partite, allo schedario dei possessori e alla mappa urbana. Al riguardo il Garante, pur non rilevando di per sé significative criticità sotto il profilo della protezione dei dati personali, ha ritenuto comunque opportuno segnalare cautela per evitare che l'ostensione di tali documenti potesse rivelare informazioni e scelte personali sulla disposizione interna delle unità immobiliari. In particolare, si è evidenziata la necessità di escludere le planimetrie dal regime di pubblicità previsto dall'art. 65, d.P.R. n. 1142/1949, per garantirne l'accessibilità solo a quanti vantino diritti reali sull'immobile o agli altri soggetti legittimati;

b) parere 5 dicembre 2024, n. 757, reso alla Presidenza del Consiglio dei ministri sulle proposte emendative n. 8.079 (Gebhard e altri), n. 8.080 (Barabotti e altri), 8.081 (Panizzut e altri), 8.082 (Bicchielli e altri), presentate al d.d.l. di bilancio per il triennio 2025-2027 (AC 2112-*bis*) riguardanti la disciplina del cinque per mille e la conoscibilità dei nominativi dei contribuenti da parte dei destinatari (doc. web n. 10097392). Gli emendamenti prevedevano modifiche all'art. 1, comma 154, l. 23 dicembre 2014, n. 190 (legge di stabilità 2015), per legittimare gli enti destinatari del contributo del cinque per mille a conoscere i nominativi dei contribuenti che lo consentono in sede di presentazione della dichiarazione dei redditi, mediante il modello predisposto dall'Agenzia delle entrate. Al riguardo, il Garante ha suggerito alcune integrazioni per chiarire le finalità della comunicazione dei nominativi da parte dell'Agenzia delle entrate e assicurare che i dati dei contribuenti non siano trattati per scopi ulteriori e incompatibili.

Il Garante, inoltre, si è soffermato sulle modalità semplificate di revoca del consenso e sull'informazione adeguata che i contribuenti devono ricevere in merito al trattamento dei loro dati personali;

c) parere 26 settembre 2024, n. 577, reso alla Presidenza del Consiglio dei ministri, su uno schema di decreto legislativo, adottato in attuazione della delega legislativa prevista dall'art. 17, l. 11 agosto 2023, n. 111 (delega al Governo per la riforma fiscale), volto ad adeguare la normativa interna alle disposizioni del reg. UE 2018/1672, in materia di controlli sui flussi di contante in entrata e in uscita dall'Unione e al reg. di esecuzione 2021/776 (doc. web n. 10071235) (oggi: d.lgs. 10 dicembre 2024, n. 211). Il provvedimento novella la l. 17 gennaio 2000, n. 7, recante la disciplina del mercato dell'oro e il d.P.R. 26 ottobre 1972, n. 633 per eliminare i riferimenti all'Ufficio italiano dei cambi, nonché il d.lgs. 19 novembre 2008, n. 195, recante modifiche e integrazioni alla normativa valutaria. Nel proprio parere il Garante, pur rilevando la coerenza del decreto rispetto ai principi e criteri direttivi della legge di delegazione ha evidenziato, tuttavia, la necessità di alcune modifiche e integrazioni, con riguardo al richiamo all'osservanza della normativa in materia di protezione dei dati personali; all'individuazione espressa dei titolari dei trattamenti; alla previsione del rinvio a una fonte secondaria, – da adottarsi previo parere del Garante – per la disciplina delle modalità di esercizio dei diritti degli interessati, delle misure di sicurezza dei dati, nonché delle modalità di realizzazione dei controlli;

d) parere 12 settembre 2024, n. 571, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo volto ad adeguare la normativa interna alle disposizioni del reg. (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022, relativo alla *governance* europea dei dati, e che modifica il reg. (UE) 2018/1724 (doc. web n. 10105175) (oggi: d.lgs. 7 ottobre 2024, n. 144). Il parere reca alcune osservazioni in ordine all'opportunità di alcune integrazioni all'articolato, con riferimento, tra l'altro, alla definizione delle forme e delle modalità di esercizio del coordinamento tra Garante, AgID e altre amministrazioni competenti in relazione alla materia trattata; all'individuazione delle informazioni da fornire agli interessati in ordine al riutilizzo dei loro dati; alla disciplina dei presupposti di liceità per la trasmissione a terzi dei dati personali a fini di riutilizzo; all'esclusione delle funzioni di controllo sul trattamento dei dati personali da quelle devolute agli organismi competenti di cui all'art. 7 del reg. (UE) 2022/868;

e) parere 2 agosto 2024, n. 477, reso alla Presidenza del Consiglio dei ministri, su uno schema di disegno di legge, recante disposizioni e delega al Governo in materia di IA (doc. web n. 10043532). Il parere prevede la necessità di alcune modifiche e integrazioni volte a migliorare la conformità delle disposizioni del disegno di legge alla normativa in materia di protezione dati, tenendo conto delle possibili sovrapposizioni tra la disciplina ivi contenuta, l'AI *Act* e la stessa normativa di protezione dati, prevedendo misure a salvaguardia dei minori (quali sistemi di *age verification*) e dei dati, individuando idonei presupposti di liceità per i trattamenti in ambito sanitario e a fini di ricerca, introducendo misure a garanzie dei lavoratori e facendo salvi i poteri del Garante, del quale si suggerisce la designazione quale autorità competente ai fini dell'art. 74, par. 8, della AI *Act,* nonché l'individuazione quale autorità per la tutela dei diritti fondamentali ai fini di cui all'art. 77, parr. 1 e 2, dell'AI *Act*;

f) parere 18 luglio 2024, n. 460, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo – adottato in attuazione dell'art. 5 l. 21 febbraio 2024, n. 15 (legge di delegazione europea 2022-2023) – recante attuazione della dir. (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la dir. 2008/114/CE del Consiglio (doc. web n. 10053427). Il parere rileva la necessità di alcune integrazioni e precisazioni volte a

garantire la piena conformità del provvedimento alla normativa vigente e a evitare dubbi interpretativi, con particolare riguardo alla disciplina della verifica dei precedenti penali – in relazione, segnatamente, alla previsione delle condizioni legittimanti le richieste di controllo, alle categorie di precedenti ritenuti rilevanti, nonché alla disciplina delle modalità e dei tempi di conservazione dei certificati del casellario giudiziale europeo, alla gestione degli incidenti rilevanti, al richiamo agli adempimenti previsti dagli artt. 33 e seguenti del RGPD e, se applicabile, dagli artt. 26 e seguenti, d.lgs. n. 51/2018, indipendentemente dalla rilevanza dell'incidente;

g) parere 4 luglio 2024, n. 400, reso alla Presidenza del Consiglio dei ministri, su uno schema di decreto legislativo recante disposizioni integrative e correttive in materia di regime di adempimento collaborativo, razionalizzazione e semplificazione degli adempimenti tributari e concordato preventivo biennale (doc. web n. 10039528) (oggi: d.lgs. 5 agosto 2024, n. 108). Il decreto, adottato nell'esercizio della delega legislativa prevista dall'art. 17, l. 11 agosto 2023, n. 111 (delega al Governo per la riforma fiscale) ha novellato la disciplina relativa al regime di adempimento collaborativo di cui al titolo III, d.lgs. 5 agosto 2015, n. 128, come novellato, tra gli altri, dal d.lgs. 12 febbraio 2024, n. 13 (in materia di accertamento tributario e di concordato preventivo biennale) (cfr. par. 2.3), sul cui schema il Garante ha reso parere l'11 gennaio 2024. In assenza di elementi di criticità, il Garante non ha formulato rilievi;

h) parere 22 febbraio 2024, n. 89, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo adottato ai sensi dell'art. 1, comma 5, lett. a), b), c), d) e h), l. 22 dicembre 2021, n. 227 recante la delega legislativa per la revisione e il riordino delle disposizioni vigenti in materia di disabilità (cfr. par. 2.3), recante definizione della condizione di disabilità, della valutazione di base, di accomodamento ragionevole, della valutazione multidimensionale per l'elaborazione e attuazione del progetto di vita individuale personalizzato e partecipato (doc. web n. 9995198) (oggi: d.lgs. 3 maggio 2024, n. 62).

Il decreto legislativo coordina le disposizioni legislative vigenti in materia di disabilità, funzionali a garantire alla persona con disabilità il riconoscimento della propria condizione (anche attraverso un procedimento valutativo) e a promuoverne l'autodeterminazione nel rispetto, tra gli altri, del principio di non discriminazione. Esso reca la disciplina del "procedimento valutativo di base" e dell'accomodamento ragionevole", nonché quella della "valutazione multidimensionale", tesa ad assicurare un "progetto di vita individuale personalizzato e partecipato" del disabile. Il parere si sofferma su tali procedimenti amministrativi, prevedendo per entrambi la necessità di integrazioni volte ad assicurare alle previsioni dei trattamenti la necessaria determinatezza, anche in ragione delle peculiarità dei dati personali coinvolti (art. 9 del RGPD);

i) parere 11 gennaio 2024, n. 3, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo in materia di procedimento accertativo, adottato nell'esercizio della delega legislativa prevista dall'art. 17, l. 11 agosto 2023, n. 111 (doc. web n. 9978230) (oggi: d.lgs. 12 febbraio 2024, n. 13). Il Garante ha al riguardo ritenuto che le modifiche introdotte, funzionali alla razionalizzazione del regime normativo e all'agevolazione dell'uso di tecnologie digitali, non richiedessero rilievi specifici, in ragione dell'assenza di particolari criticità.

3.1.3. I pareri sugli atti regolamentari

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

Nel periodo considerato, in particolare, l'Autorità si è espressa sui seguenti atti:

a) schema di regolamento del Ministro dell'ambiente e della sicurezza energetica recante criteri, modalità e requisiti per l'iscrizione, la permanenza e l'esclusione delle imprese iscritte nell'elenco dei soggetti abilitati alla vendita di gas naturale ai sensi dell'art. 17, comma 3, d.lgs. 23 maggio 2000, n. 164 (parere 27 novembre 2024, n. 725, doc. web n. 10100424). Lo schema di regolamento, che qualifica l'iscrizione e la permanenza nell'elenco dei soggetti abilitati quali condizioni necessarie per lo svolgimento dell'attività di vendita di gas naturale ai clienti finali, si inscrive nel quadro della riforma introdotta con decisione del Consiglio 5 dicembre 2023, volta a migliorare la trasparenza e a favorire la scelta dei fornitori da parte dei consumatori energetici nel libero mercato, nel rispetto di adeguati standard di legalità e solvibilità. Nel proprio parere, il Garante ha suggerito alcune modifiche e integrazioni all'articolato per elevare le garanzie di protezione dei dati personali trattati (in particolare quelli di cui agli artt. 10 del RGPD e 2-*octies* del Codice, avuto riguardo alla sussistenza dei requisiti di onorabilità in capo ad amministratori, legali rappresentanti e sindaci delle imprese di vendita), rilevando la necessità di riformulare l'art. 9, comma 4, prevedendo l'utilizzo del certificato selettivo di cui all'art. 28, d.P.R. n. 313/2002 e la limitazione dell'accesso alle informazioni al solo personale autorizzato, nonché di inserire all'art. 4, comma 5, un riferimento ai dati relativi alle misure di prevenzione trattati;

b) schema di decreto del Ministro della giustizia recante regolamento per la determinazione dei criteri e delle modalità di formazione e trasmissione telematica delle copie dei repertori e del registro somme e valori o della certificazione negativa e delle modalità di conservazione, ricerca e consultazione dei documenti e dei dati inseriti nell'archivio centrale informatico ai sensi dell'art. 65, l. 16 febbraio 1913, n. 89 (parere 21 novembre 2024, n. 724, doc. web n. 10097091). Il regolamento, parzialmente attuativo dell'art. 65, l. 16 febbraio 1913, n. 89, è volto a migliorare la gestione degli archivi notarili, regolando la trasmissione e la conservazione digitale delle copie dei repertori e dei registri nel rispetto delle disposizioni sulla protezione dei dati personali. Nel proprio parere, il Garante ha segnalato la necessità di alcune modifiche e integrazioni, relative, in particolare, alla disciplina della titolarità dei diversi trattamenti, definendo in maniera più puntuale l'ambito di competenza dei soggetti coinvolti e prevedendo in capo a costoro un obbligo di vicendevole informazione in merito a eventuali violazioni dei dati personali, ai profili di sicurezza, al coinvolgimento del Garante nella determinazione degli aspetti rilevanti (quali la formazione del fascicolo digitale e la sua trasmissione) rimessi alla disciplina da introdursi con le specifiche tecniche;

c) schema di decreto del Ministro della difesa recante regolamento di attuazione delle norme sull'esercizio della libertà sindacale del personale delle forze armate e delle forze di polizia a ordinamento militare di cui al d.lgs. 15 marzo 2010, n. 66, ai sensi degli artt. 1, comma 3, e 1475, comma 2, del medesimo decreto legislativo (parere 17 ottobre 2024, n. 610, doc. web n. 10071217). Il Garante ha ritenuto che lo schema di regolamento – adottato ai sensi degli artt. 1, comma 3, e 1475, comma 2, d.lgs. n. 66/2010 (recante codice dell'ordinamento militare) e introduttivo dell'art. 941-*quaterdecies*, relativo al diritto di assemblea – non presenti significative criticità in termini di protezione dei dati personali, pur meritando alcune integrazioni utili a garantire una maggiore completezza della disciplina. In particolare, il Garante ha segnalato la necessità di integrare l'art. 941-*quaterdecies*, imponendo un vincolo di conformità alla disciplina di protezione dei dati personali relativamente alle modalità di acquisizione della documentazione audiovisiva dell'attività svolta durante le assemblee del personale, richiamando i requisiti di validità del consenso e il previo rilascio all'interessato dell'informativa, demandando peraltro a un atto subordinato la previsione di misure tecniche e organizzative tali da garantire il trattamento dei dati relativi alla

causale inerente al permesso unicamente da parte del personale gerarchicamente sovraordinato competente e da quello deputato alla gestione del rapporto di lavoro;

d) schema di decreto del Ministro del lavoro e delle politiche sociali attuativo (e integrativo) dell'art. 27, commi 3 e 5, d.lgs. 9 aprile 2008, n. 81 e s.m.i. relativo all'individuazione delle modalità di presentazione della domanda per il conseguimento della patente per le imprese e i lavoratori autonomi operanti nei cantieri temporanei o mobili (parere 16 settembre 2024, n. 573, doc. web n. 10070301). Il decreto disciplina il rilascio della patente in formato digitale, i requisiti necessari, i presupposti per l'adozione dei provvedimenti cautelari di sospensione, i punteggi con i relativi criteri e meccanismi di attribuzione, la sospensione e la decurtazione dei crediti e i contenuti informativi della patente. Al riguardo, il Garante ha suggerito alcune integrazioni all'articolato, limitando la conoscibilità dei contenuti informativi della patente ai soli esiti relativi a eventuali provvedimenti di sospensione o definitivi e rendendo tassativo l'elenco dei soggetti potenzialmente legittimati all'accesso alle informazioni;

e) schema di decreto del Ministro delle infrastrutture e dei trasporti, avente natura regolamentare, attuativo dell'art. 39-*bis*, d.lgs. 18 luglio 2005, n. 171 e s.m.i. (codice della nautica da diporto), recante la disciplina dell'anagrafe nazionale delle patenti nautiche (parere 18 luglio 2024, n. 461, doc. web n. 10056306). Lo schema di regolamento disciplina la definizione dell'organizzazione e del funzionamento dell'anagrafe nazionale delle patenti nautiche, dei tipi di dati trattati, delle operazioni eseguibili, del motivo di interesse pubblico rilevante, delle forme di tutela degli interessati, delle misure tecniche di sicurezza, nonché delle modalità di accesso e trasmissione dei dati da parte dei soggetti tenuti, prevedendone forme di conoscibilità anche da parte di soggetti non appartenenti al novero di quelli individuati dall'art. 39-*bis*, comma 4, d.lgs. 18 luglio 2005, n. 171. A tale ultimo riguardo, il Garante ha evidenziato la necessità di riformulare la disposizione sull'accesso ai dati, circoscrivendo l'ambito dei soggetti legittimati unicamente a quelli stabiliti dal citato art. 39-*bis*, comma 4 e limitando l'accesso ai soli dati indispensabili per le loro finalità istituzionali;

f) schema di regolamento del Ministro delle imprese e del *made in Italy* predisposto ai sensi dell'art. 2, d.lgs. 8 novembre 2021, n. 185, attuativo della dir. (UE) 2019/1, che conferisce alle autorità garanti della concorrenza degli Stati membri poteri di applicazione più efficace e che assicura il corretto funzionamento del mercato interno (parere 21 marzo 2024, n. 174, doc. web n. 10010543). Lo schema di regolamento novella il d.P.R. 30 aprile 1998, n. 217, coordinandolo con la legge *antitrust*. Tra le modifiche previste si segnalano, tra le altre, la novella dell'art. 6 relativa all'avvio della fase istruttoria e quella dell'art. 13 in materia di accesso. Il Garante, oltre a fornire indicazioni sui termini di conservazione delle registrazioni delle audizioni (distinguendo se video o audio) e sulle modalità per assicurare il rispetto dei principi di cui all'art. 5 del RGPD, con particolare riguardo al canone di minimizzazione, ha proposto l'integrazione del regolamento con la previsione di un coordinamento tra le istruttorie del Garante e di AGCM, nei casi in cui i procedimenti *antitrust* involgano anche profili rilevanti in termini di protezione dati;

g) schema di decreto del Ministro della giustizia relativo all'attivazione dell'archivio delle intercettazioni (ADI) presso le infrastrutture interdistrettuali (parere 22 febbraio 2024, n. 90, doc. web n. 9995724). Lo schema di decreto, oltre a regolare l'attivazione dell'ADI definisce, al contempo, i tempi, le modalità e i requisiti di sicurezza della migrazione e del conferimento dei dati e dispone altresì che l'ADI – tenuto sotto la direzione e la sorveglianza del Procuratore della Repubblica – custodisca i verbali, gli atti e le registrazioni delle intercettazioni disposte dalle singole Procure. Lo schema di decreto perfeziona un percorso che ha già sancito l'istituzione delle infrastrutture

digitali centralizzate per le intercettazioni e la definizione dei requisiti tecnici per la gestione dei dati presso tali sistemi (sui cui schemi il Garante si è espresso con parere favorevole rispettivamente nei mesi di settembre e di dicembre 2023). Esso ha recepito tutte le indicazioni fornite in fase istruttoria dall'Autorità e prevede le ulteriori misure tecniche e organizzative di funzionamento del sistema già richieste dal Garante. Per tali ragioni, il parere reso è stato favorevole con la sola indicazione inerente l'esplicitazione, nel testo, del ruolo di titolare del trattamento dei dati svolto dalle Procure della Repubblica, per fugare possibili dubbi interpretativi e agevolare l'esercizio dei diritti da parte degli interessati;

h) schema di decreto del Ministro della giustizia relativo all'istituzione dell'archivio nazionale delle intercettazioni disposte dalla Procura europea - EPPO (parere 22 febbraio 2024, n. 91, doc. web n. 9999936). Lo schema di decreto disciplina le modalità di conservazione e consultazione dei dati contenuti nell'archivio e i soggetti legittimati all'accesso mediante le postazioni istituite presso le sedi di servizio dei Procuratori europei delegati. Potranno dunque accedere all'archivio nazionale il giudice che procede e i suoi ausiliari; il pubblico ministero e i suoi ausiliari, ivi compresi gli ufficiali di polizia giudiziaria delegati all'ascolto; i difensori delle parti assistiti, se necessario, da un interprete. L'archivio nazionale, tenuto sotto la direzione e la sorveglianza esclusive del Procuratore europeo o, nei casi previsti, del Procuratore europeo delegato, conserverà la versione integrale di tutti i verbali e di tutte le registrazioni delle intercettazioni eseguite nei procedimenti in cui la Procura europea ha esercitato la sua competenza, nonché ogni altro atto ad esse relativo. Nel rilasciare parere favorevole sullo schema di decreto, il Garante ha ritenuto comunque di richiedere – in analogia con i sistemi nazionali – l'introduzione misure tecnico-organizzative ulteriori, tese a garantire uniformità nei livelli di sicurezza del trattamento.

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

Per quanto riguarda i pareri chiesti al Garante su alcuni progetti di legge o schemi di regolamento di regioni o province autonome, si segnalano i seguenti:

1) parere sullo schema di regolamento relativo al trattamento dei dati personali, predisposto in attuazione dell'art. 14, l. p. 2 novembre 2022, n. 12, recante il Sistema provinciale per la politica attiva del lavoro e la realizzazione di interventi e servizi di pubblica utilità (cd. progettone) (parere 7 marzo 2024, n. 131, doc. web n. 10008202);

2) parere sulla proposta di modifica dell'art. 15, l. p. 27 luglio 2007, n. 13, relativo al Sistema informativo delle politiche sociali nella Provincia autonoma di Trento (parere 12 settembre 2024, n. 537, doc. web n. 10061517);

3) parere sulla proposta normativa della Provincia di Trento volta a novellare la l. p. 30 giugno 2017, n. 6 relativa alla pianificazione e gestione degli interventi in materia di mobilità sostenibile (parere 12 settembre 2024, n. 538, doc. web n. 10062327);

4) parere sullo schema di regolamento recante norme per il funzionamento del registro tumori della Regione Friuli Venezia Giulia (parere 31 ottobre 2024, n. 661, doc. web n. 10097356);

5) parere sulla proposta di legge della Provincia autonoma di Trento recante novella della l. p. 5 novembre 1991, n. 23 recante norme transitorie per l'esercizio delle funzioni in materia di igiene e sanità pubblica (parere 14 novembre 2024, n. 692, doc. web n. 10100374).

3.1.5. Segnalazioni

A seguito dell'approvazione definitiva del reg. europeo sull'IA, il Garante ha inviato al Parlamento e al Governo una segnalazione (nota 22 marzo 2024, doc. web n. 9996493)

relativa all'autorità competente ai sensi dell'art. 70 del reg. medesimo (cfr. cap. 16 e cap. 21).

In base alla disciplina unionale, le autorità di protezione dati sono le uniche destinatarie di un'espressa riserva di competenza in materia (v. l'art. 74, p. 8, oltre che le varie clausole di salvaguardia in favore della protezione dati) e, in quanto indipendenti, legittimate ad esercitare le funzioni di controllo in settori delicati come quello delle attività di contrasto (art. 5, p. 3).

Inoltre, la stretta interrelazione tra l'IA e la protezione dei dati personali, unitamente alla competenza già acquisita dall'Autorità in ordine ai processi decisionali automatizzati e alle caratteristiche d'indipendenza che ne connotano lo statuto, rendono il Garante un soggetto idoneo ai sensi dell'art. 70 del reg., in grado di esercitare le funzioni attribuite dal regolamento "in modo indipendente, imparziale e senza pregiudizi", salvaguardandone i principi di obiettività e garantendo l'applicazione e l'attuazione del reg. medesimo.

In tale ottica, la designazione dell'Autorità quale autorità nazionale di controllo in materia di IA permetterebbe altresì di assicurare un approccio normativo più armonizzato, contribuendo all'adozione di interpretazioni coerenti con le disposizioni in tema di trattamento dei dati e alla semplificazione dei meccanismi operativi, evitando in pari tempo conflitti di competenza e duplicazioni ingiustificate di oneri a carico di soggetti pubblici e privati.

Ferme restando le attribuzioni del Governo in ordine alla generale promozione e regolazione secondaria della materia, l'Autorità ha dunque suggerito di riflettere in ordine all'opportunità di una sua designazione quale autorità competente in materia di IA, anche sulla scorta della soluzione proposta al riguardo dal CEPD e dal Garante europeo con il parere congiunto 5/2021, nonché dei requisiti di competenza e indipendenza necessari per garantire un'attuazione del regolamento coerente con l'obiettivo di garantire un elevato livello di tutela dei diritti fondamentali nel ricorso all'IA (art. 1, p. 1).

3.1.6. Quesiti

Nell'anno di riferimento l'Autorità ha nuovamente fornito riscontro a un quesito sottoposto da una società di noleggio con conducente, relativa all'applicazione della disciplina di cui all'art. 11, comma 4, l. 15 gennaio 1992, n. 21, con particolare riguardo al contenuto del foglio di servizio di noleggio con conducente. In proposito, nel riportarsi integralmente a quanto già precisato nella Relazione 2023 (p. 30), si è dato conto dell'evoluzione della questione.

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

Anche nel 2024 il Garante ha fornito, su 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.

In particolare, l'Ufficio ha trasmesso al Governo riscontri sui profili di protezione dati sottesi alle seguenti interrogazioni parlamentari:

- n. 4-01713, relativa ai provvedimenti da adottare per formalizzare le procedure di controllo che garantiscano, prima della pubblicazione sui siti istituzionali dei *curricula* dei candidati alle elezioni, la veridicità delle informazioni ivi contenute, avuto riguardo all'iscrizione a un ordine professionale che prevede l'attribuzione di un titolo;
- n. 4-02334, relativa al sistema di videosorveglianza in uso presso la Casa di reclusione Opera di Milano e ai tempi di conservazione delle relative riprese.

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

Nell'anno di riferimento è proseguita l'attività di esame sulle leggi regionali, al fine di fornire alla Presidenza del Consiglio dei ministri eventuali elementi di valutazione circa la loro compatibilità con le disposizioni in materia di protezione dei dati personali, ai sensi dell'art. 127 della Costituzione.

In particolare, l'Autorità ha esaminato la l. 24 luglio 2024, n. 2 (assestamento del bilancio di previsione della Regione autonoma Trentino Alto Adige/Südtirol per gli esercizi finanziari 2024-2026), valutando la compatibilità degli artt. 1 e 5 – che introducono la nozione di "censimento dei gruppi linguistici" in luogo di quella relativa al "censimento ufficiale della popolazione" o "censimento generale della popolazione" – con la disciplina in materia di protezione dei dati personali.

Il Garante ha riscontrato la relativa richiesta del Governo ritenendo non eccedente la competenza della legislazione regionale ai sensi dei commi 1 e 2, lett. l), dell'art. 117 della Costituzione nonché assenti profili di criticità con riferimento alla protezione dati, anche in ragione della sussistenza di misure idonee ad assicurare modalità anonime di rilevazione dei dati in via telematica.

Di interesse, inoltre, l'analisi svolta sulla l.r. n. 18/2018 della Regione Sicilia.

Muovendo dalla procedura avviata dalla Commissione europea per la verifica del rispetto e della corretta applicazione del diritto unionale da parte della legge regionale – con riferimento all'obbligo ivi previsto di dichiarare, da parte dei soggetti espressamente indicati, l'eventuale appartenenza ad associazioni massoniche o similari – il Garante ha fornito riscontro alla Presidenza del Consiglio dei ministri - Dipartimento per gli affari europei, sostenendo la compatibilità della previsione regionale (di Regione, peraltro, ad autonomia speciale) in ordine al presupposto di liceità del trattamento (art. 9, p. 2, lett. g), RGPD), ma riservando alla legislazione statale esclusiva la normazione sulla protezione dei dati personali. Quanto alle possibili modalità alternative di adempimento dell'obbligo dichiarativo, pur sempre ipotizzabili, il Garante ha chiarito che occorre tener conto di quanto stabilito dall'art. 1, d.lgs. n. 33/2013, che qualifica la trasparenza – anche ai fini dell'individuazione del livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche – quale "accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche".

II

LE ATTIVITÀ PER SETTORE

4 Le amministrazioni pubbliche

4.1. *L'attività fiscale e tributaria*

Anche nel 2024 il Garante è stato chiamato a pronunciarsi in merito alla cd. dichiarazione dei redditi precompilata, con specifico riguardo alle tipologie di dati da trasmettere all'Agenzia delle entrate e alle modalità di accesso alla dichiarazione da parte degli interessati e degli altri soggetti autorizzati.

Dichiarazione dei redditi precompilata

L'Autorità si è espressa favorevolmente su un nuovo schema di decreto del MEF (provv. 24 gennaio 2024, n. 30, doc. web n. 9985697), con il quale sono state aggiornate, ai fini dell'elaborazione della dichiarazione dei redditi precompilata, le disposizioni attuative concernenti la trasmissione telematica "a regime" all'Agenzia delle entrate dei dati relativi alle erogazioni liberali detraibili e deducibili effettuate agli enti del terzo settore, alla luce delle modifiche normative intervenute rispetto a quanto stabilito nel precedente decreto 3 febbraio 2021 (sul quale il Garante aveva reso parere favorevole, cfr. provv. 14 gennaio 2021, n. 3, doc. web n. 9538552). In questo senso, è stata ridefinita la platea dei soggetti tenuti alla trasmissione dei dati, ampliandola agli ulteriori enti iscritti nel registro unico nazionale del terzo settore (RUNTS) che possono ricevere erogazioni detraibili o deducibili.

L'Autorità è stata poi consultata dall'Agenzia delle entrate in relazione allo schema di provvedimento del Direttore concernente le modalità tecniche di comunicazione alla Anagrafe tributaria dei predetti dati relativi alle erogazioni liberali. In particolare, lo schema prevede che gli enti del terzo settore, a partire dai dati relativi all'anno d'imposta 2023, trasmettano all'Agenzia delle entrate – in conformità alla normativa in materia di protezione dati e alle garanzie già previste nei provvedimenti del Direttore dell'Agenzia delle entrate adottati in passato in materia di trasmissione dei dati concernenti le erogazioni liberali a fini di dichiarazione dei redditi precompilata, e già vagliate dal Garante nei relativi provvedimenti (provv.ti 8 febbraio 2018, n. 66, doc. web n. 7772714 e 11 febbraio 2021, n. 42, doc. web n. 9556670) – le comunicazioni di cui al menzionato decreto del Ministro dell'economia e delle finanze, poi adottato il 1° marzo 2024, concernenti i dati relativi alle erogazioni liberali in denaro deducibili e detraibili, eseguite nell'anno precedente da persone fisiche, nonché i dati identificativi dei soggetti eroganti. Su tali basi, l'Autorità – considerando che i trattamenti di dati personali disciplinati nello schema di provvedimento, pur se riferiti a categorie particolari di dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, nonché lo stato di salute e la vita sessuale (art. 9 RGPD), fossero ammissibili, in particolare, in quanto necessari per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri – ha espresso, parere favorevole (provv. 22 febbraio 2024, n. 96, doc. web n. 9994654).

Sempre ai fini dell'elaborazione della dichiarazione dei redditi precompilata, il Garante ha espresso parere favorevole su uno schema di decreto del Ministro dell'economia e delle finanze concernente la trasmissione telematica all'Agenzia delle entrate dei dati riguardanti i proventi riconosciuti alle persone fisiche e ai condomìni, derivanti dalla cessione di energia risultata esuberante rispetto alle esigenze dell'abitazione del proprietario o del condominio, prodotta da impianti alimentati da fonti rinnovabili di potenza fino a 20 KW (provv. 12 dicembre 2024, n. 764, doc. web n. 10097432).

4

Sotto altro profilo, l'Autorità ha nuovamente vagliato le modalità con cui l'Agenzia delle entrate consente l'accesso alla dichiarazione 730 precompilata da parte del contribuente e degli altri soggetti autorizzati a partire dall'anno di imposta 2023 (provv. 24 aprile 2024, n. 236, doc. web n. 10018198). In particolare, il Garante ha reso parere favorevole sullo schema di provvedimento del Direttore dell'Agenzia, il quale, alla luce del novellato d.lgs. n. 175/2014, prevede che l'Agenzia delle entrate, a decorrere dal 2024, in via sperimentale, renda disponibile telematicamente, entro il 30 aprile di ciascun anno, la dichiarazione precompilata relativa ai redditi prodotti nell'anno precedente anche ai contribuenti titolari di redditi di lavoro autonomo e d'impresa e ai titolari di redditi che non possono essere dichiarati con il modello 730 (art. 1, comma 1-*bis*), e renda disponibili altresì a tutti i contribuenti, in modo analitico, le informazioni in proprio possesso, che possono essere confermate o modificate accedendo ad un'apposita area riservata del sito internet dell'Agenzia. Lo schema – oltre a integrare l'elenco degli oneri detraibili/deducibili e relativi rimborsi, trasmessi dai soggetti terzi, che sono utilizzati dall'Agenzia delle entrate per l'elaborazione della dichiarazione – prevede, in particolare: l'ampliamento della platea di destinatari della dichiarazione dei redditi precompilata ai contribuenti titolari di redditi di lavoro autonomo e d'impresa e ai titolari di redditi che non possono essere dichiarati con il modello 730; l'utilizzo dei dati trasmessi dall'INPS, relativi ai familiari a carico per i quali è stato riconosciuto l'assegno unico e universale a partire dall'anno di imposta 2023; l'accesso diretto, da parte del contribuente alla dichiarazione precompilata attraverso le funzionalità rese disponibili all'interno dell'area riservata, autenticandosi, come per gli scorsi anni, tramite le credenziali SPID, CNS o CIE o, per i soggetti titolati ad averle, con le credenziali rilasciate dall'Agenzia (ENTRATEL/FISCONLINE), con esclusione della possibilità di accedere tramite le credenziali rilasciate dall'INPS, in via di dismissione; nonché la possibilità di conferire, a regime, la delega ai CAF, da parte dei contribuenti mediante un documento informatico sottoscritto con firma elettronica avanzata, superando il regime sperimentale avviato nel 2023.

Nello schema di provvedimento vengono, in ogni caso, confermate le misure e le garanzie individuate negli anni passati per l'accesso alla dichiarazione dei redditi precompilata, anche sulla base delle indicazioni dell'Autorità.

Con riferimento, più in generale, agli accessi da parte dei soggetti autorizzati ai servizi *online*, il Garante ha inoltre espresso parere favorevole su uno schema di provvedimento del Direttore dell'Agenzia delle entrate recante "delega unica agli intermediari per l'utilizzo dei servizi *online* dell'Agenzia delle entrate e dell'Agenzia delle entrate - Riscossione", volto ad attuare l'art. 21 del d.lgs. 8 gennaio 2024, n. 1. Lo schema in esame, in particolare, disciplina il contenuto della delega (codice fiscale e dati anagrafici del delegante e dell'intermediario, i servizi *online* oggetto di delega o revoca, data di conferimento o di revoca della delega) e i servizi dell'Agenzia delle entrate - Riscossione delegabili; le modalità di conferimento e la durata della delega; le modalità di comunicazione all'Agenzia delle entrate dei dati relativi al conferimento della delega nonché le modalità di rinnovo, revoca e rinuncia della delega. Tale schema prevede un adeguato livello di sicurezza attraverso l'adozione di meccanismi di identificazione standard e di protocolli di comunicazione aggiornati, un sistema di profilazione, identificazione, autenticazione e autorizzazione dei soggetti abilitati alla consultazione, nonché il tracciamento degli accessi effettuati sui propri sistemi da parte di ciascun delegante e di ciascun intermediario delegato (provv. 12 settembre 2024, n. 539, doc. web n. 10062356).

Redditometro e concordato preventivo biennale

Il Garante è intervenuto nuovamente in materia di determinazione sintetica del reddito complessivo delle persone fisiche, con l'adozione di un parere sullo schema di decreto del Ministro dell'economia e delle finanze, attuativo dell'art. 38, comma 5, d.P.R. n. 600/1973, come modificato dall'art. 10, d.l. 12 luglio 2018 n. 87 (recante di-

sposizioni urgenti per la dignità dei lavoratori e delle imprese, convertito, con modificazioni, dalla l. 9 agosto 2018, n. 186). In particolare, lo schema – finalizzato a stabilire il contenuto induttivo degli elementi indicativi di capacità contributiva sulla base dei quali può essere fondata la determinazione sintetica del reddito o del maggior reddito complessivo delle persone fisiche applicabile agli accertamenti relativi ai redditi degli anni d'imposta, a decorrere dal 2016 – tiene conto delle prescrizioni rese dal Garante all'Agenzia delle entrate con il provv. 21 novembre 2013, n. 515 (doc. web n. 2765110), adottato a seguito di una richiesta di verifica preliminare formulata dalla stessa Agenzia delle entrate in tale ambito. In particolare, il cd. redditometro comporta la profilazione dei contribuenti (fondata sui dati personali presenti in Anagrafe tributaria, o comunque conosciuti dall'Agenzia, e sull'imputazione di altri elementi di carattere induttivo), nonché rilevanti conseguenze in capo agli interessati con l'attribuzione in via presuntiva della ricostruzione sintetica del reddito.

L'Autorità ha espresso, quindi, parere favorevole sullo schema (provv. 24 aprile 2024, n. 239, doc. web n. 10018219), risultando quest'ultimo conforme alla normativa in materia di protezione dei dati personali, con particolare riferimento alla individuazione delle tipologie di dati, alla logica utilizzata e alle conseguenze per gli interessati, ferma restando la necessità di svolgere future verifiche circa l'adeguatezza delle garanzie e delle misure che l'Agenzia delle entrate dovrà aver cura di adottare in tale contesto, anche in esito alla valutazione di impatto sulla protezione dei dati, nel solco di quanto ribadito dal Garante in pregressi provvedimenti.

Il d.lgs. 12 febbraio 2024, n. 13 (su cui il Garante si è espresso favorevolmente, seppure con alcune condizioni, con il provv. 11 gennaio 2024, n. 3, doc. web n. 9978230 - cfr. par. 2.3 *supra*) ha tra l'altro introdotto la possibilità di accedere al concordato preventivo biennale per i contribuenti di minori dimensioni titolari di reddito di impresa e di lavoro autonomo derivante dall'esercizio di arti e professioni.

Nel 2024, il Garante si è espresso su tre diversi schemi di decreto del MEF attuativi del citato d.lgs. n. 13/2024, concernenti l'applicazione del concordato preventivo biennale (provv.ti 6 giugno 2024, n. 36, doc. web n. 10025575; in via d'urgenza, 10 luglio 2024, n. 436, doc. web n. 10057102 e 25 luglio 2024, n. 439, doc. web n. 10057121). Gli schemi esaminati dal Garante hanno demandato all'Agenzia delle entrate, in qualità di titolare del trattamento, la definizione in concreto delle misure da adottare a tutela degli interessati nell'ambito della valutazione di impatto sulla protezione dei dati necessaria, in ragione dei rischi elevati presentati dal trattamento in esame, ai sensi dell'art. 35 del RGPD. L'Autorità ha valutato favorevolmente i predetti schemi, richiedendo alcune garanzie volte ad assicurare il rispetto dei principi di liceità, correttezza e trasparenza e di minimizzazione (art. 5, par. 1, lett. a) e c), RGPD), la limitazione del trattamento dei dati di cui all'art. 10 del RGPD a quelli riferibili alle condanne (o a sentenze di applicazione della pena su richiesta delle parti) per i soli reati di cui all'art. 11, comma 1, lett. b), d.lgs. n. 13/2024 (*id est* per i reati in materia di imposte sui redditi e sul valore aggiunto, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita), nonché una più accurata definizione dell'ambito di operatività di Sogei S.p.A., operante in qualità di responsabile del trattamento per conto dell'Agenzia delle entrate. Parimenti, è stata rilevata la necessità di integrare la valutazione di impatto sulla protezione dei dati, dovendo la stessa prevedere, prima dell'avvio del trattamento, l'adozione di garanzie e meccanismi adeguati ad assicurare il pieno rispetto del principio di esattezza dei dati e un elevato livello di trasparenza al fine di incrementare la fiducia dei contribuenti nei confronti dell'utilizzo di tale nuovo strumento.

Banca dati della Regione Friuli Venezia Giulia sull'imposta locale immobiliare

Il Garante ha espresso parere favorevole sullo schema di regolamento per l'istituzione, l'organizzazione e il funzionamento della banca dati regionale dell'imposta locale im-

mobiliare autonoma (ILIA) ai sensi dell'art. 17, l.r. 14 novembre 2022, n. 17 della Regione Friuli-Venezia Giulia. Tale banca dati è volta a consentire all'amministrazione regionale di valutare l'impatto delle scelte di politica tributaria in materia di imposta locale sugli immobili. In tale contesto, i dati caricati dai comuni, soggetti attivi dell'imposta, vengono sottoposti a una procedura di pseudonimizzazione per consentire alla Regione, titolare del trattamento, il raggiungimento delle finalità perseguite senza l'identificazione diretta degli interessati. Lo schema tiene conto delle indicazioni fornite dall'Autorità finalizzate ad assicurare, in particolare, la corretta individuazione dei ruoli ricoperti dai diversi soggetti a vario titolo coinvolti (Regione, comuni, società Insiel S.p.A.), l'indicazione delle tipologie di dati oggetto di trattamento e dei tempi di conservazione degli stessi, l'adozione di un'efficace procedura di pseudonimizzazione, nel rispetto dei principi di limitazione della finalità, minimizzazione e protezione dei dati fin dalla progettazione e per impostazione predefinita, nonché le misure tecniche e organizzative idonee a garantire la riservatezza, l'integrità e la disponibilità dei dati (tra cui, in particolare, le procedure di autenticazione informatica, l'utilizzo di canali di trasmissione protetti e l'implementazione di una politica di *backup*) (provv. 12 settembre 2024, n. 540, doc. web n. 10062397).

Provvedimenti correttivi

Il Garante ha censurato nonché sanzionato l'Agenzia delle dogane e dei monopoli che, sulla base di una circolare, aveva acquisito, e successivamente comunicato a una società, informazioni riguardanti la posizione debitoria personale del rappresentante legale nell'ambito dello svolgimento dei controlli per verificare i requisiti per il rinnovo alla stessa di una concessione di distribuzione e vendita dei generi di monopolio (con la conseguenza che il personale preposto ne aveva potuto prendere conoscenza). L'Autorità ha evidenziato, in particolare, che la disciplina normativa di settore di rango primario e secondario prevede che i controlli in merito alle fattispecie debitorie vengano svolti esclusivamente nei riguardi delle imprese concessionarie (cfr. art. 19, l. 22 dicembre 1957, n. 1293; art. 2, comma 4-*ter*, decreto MEF 21 febbraio 2013, n. 38), rappresentando, in ogni caso, che le circolari amministrative possono contenere specificazioni e disposizioni di dettaglio in merito al trattamento dei dati personali soltanto nei limiti di quanto stabilito da norme di legge o di regolamento. Nel caso di specie, l'Agenzia, pur a fronte di una normativa che prevede che le informazioni sulla posizione debitoria siano riferite alle imprese (v. art. 80, d.lgs. 18 aprile 2016, n. 50), aveva trattato e comunicato a terzi anche i dati personali relativi ai debiti contratti dal rappresentante legale della società istante, quale privato cittadino e separato centro di imputazione di obbligazioni, in maniera non conforme ai principi di liceità, correttezza e trasparenza, di minimizzazione dei dati, di *privacy by design* e *by default*, nonché in assenza di un idoneo presupposto normativo, in violazione degli artt. 5, par. 1, lett. a) e c), 6 e 25 del RGPD e dell'art. 2-*ter* del Codice. In seguito, l'Agenzia ha rivisto le proprie circolari, limitando i controlli a carico della figura del legale rappresentante a ipotesi del tutto residuali (provv. 12 dicembre 2024, n. 765, doc. web n. 10101204).

Il Garante ha adottato un provvedimento correttivo e sanzionatorio nei confronti dell'Agenzia delle entrate - Riscossione (AdeR), a seguito di un reclamo con il quale era stata lamentata la notifica di due atti di pignoramento presso terzi, soggetti privati con i quali il reclamante aveva stipulato un contratto di locazione ad uso abitativo successivamente oggetto di disdetta già nell'agosto 2016, con riguardo ad un immobile peraltro alienato poi nell'ottobre 2016. In particolare, al momento della notifica dei due atti di pignoramento non sussisteva da tempo più alcun rapporto giuridico del reclamante con i terzi pignorati in questione, né con il bene oggetto di locazione, con la conseguenza che AdeR aveva illecitamente comunicato ai soggetti pignorati dati e informazioni ad esso riferiti. La base giuridica dei trattamenti effettuati da AdeR per

finalità di riscossione, perseguendo un rilevante compito di interesse pubblico, è rinvenibile nella disciplina di settore del diritto nazionale (spec. art. 72-*bis*, d.P.R. n. 602/1973). Dall'accertamento compiuto è emerso, tuttavia, che AdeR aveva illecitamente comunicato a soggetti terzi i dati personali riferiti al reclamante, in quanto tali soggetti erano stati erroneamente qualificati quali terzi debitori dello stesso sulla base di due inesatti presupposti, ossia la vigenza del contratto di locazione anzitempo stipulato, e la permanenza della proprietà, in capo al reclamante, del bene immobile precedentemente locato. Inoltre, le previsioni contenute nella circolare interna si sono rivelate inadeguate e insufficienti in ordine, in particolare, alle verifiche da effettuare sui contratti di locazione prima di avviare una procedura esecutiva e, più in generale, quanto alle misure adottate al fine di assicurare il pieno rispetto del principio di esattezza nel trattamento dei dati effettuato nell'ambito dei pignoramenti che, nel caso in esame, avrebbero evitato l'indebita comunicazione a terzi di dati relativi alla situazione debitoria del reclamante, con potenziale pregiudizio alla sua reputazione, in violazione dei principi di liceità, correttezza e di esattezza di cui agli artt. 5, par. 1, lett. a) e d), e 6, par. 1, lett. e), RGPD, nonché dell'art. 2-*ter* del Codice (provv. 19 dicembre 2024, n. 798, doc. web n. 10103672).

4.2. *Previdenza, assistenza e altri benefici*

Nel 2024 il Garante è stato chiamato a pronunciarsi su diversi provvedimenti attuativi delle disposizioni normative in materia di riconoscimento delle misure di sostegno economico nei confronti di persone in difficoltà, quali l'assegno di inclusione (ADI), il supporto per la formazione e il lavoro (SFL), nonché il relativo Sistema informativo per l'inclusione sociale e lavorativa (SIISL).

ADI e SFL

L'Autorità ha espresso parere favorevole sullo schema di decreto del Ministro del lavoro e delle politiche sociali avente ad oggetto l'approvazione delle linee guida per la definizione dei Patti per l'inclusione sociale, rivolte ai professionisti incaricati di eseguire la valutazione multidimensionale dei nuclei familiari beneficiari dell'assegno di inclusione (ADI) convocati dai servizi dei comuni o degli ambiti territoriali sociali competenti in materia di contrasto alla povertà. In particolare il Garante non ha formulato osservazioni sul predetto schema il quale, oltre a prefiggersi (tra l'altro) di assicurare omogeneità nei criteri di valutazione dei bisogni dei nuclei familiari beneficiari dell'ADI, ha definito i criteri e le indicazioni seguiti dagli operatori preposti allo svolgimento dei compiti propri delle professioni cui questi appartengono, nel rispetto degli obblighi stabiliti dalla vigente disciplina normativa e deontologica cui sono assoggettati. L'Autorità ha ricordato, in termini generali, che gli enti competenti a gestire e fornire i servizi di carattere sociale sono titolari dei trattamenti dei dati personali in questione, e che, pertanto, restano fermi in capo a essi gli adempimenti necessari ad assicurare la conformità alla disciplina in materia di protezione dei dati personali nel relativo contesto (come, ad es., le istruzioni alle persone autorizzate che agiscono sotto la loro autorità o l'analisi dei rischi per i diritti e le libertà fondamentali degli interessati e l'adozione delle adeguate misure tecniche e organizzative per mitigarli) (provv. 8 febbraio 2024, n. 60, doc. web n. 9992965).

Nell'ambito delle politiche di coesione, l'Autorità si è pronunciata favorevolmente sullo schema di disciplinare dell'INPS, attuativo dell'art. 4, commi 5 e 8, del decreto del Ministro del lavoro e delle politiche sociali 13 dicembre 2023 (su cui il Garante si era pronunciato con provv. 12 dicembre 2023, n. 597, doc. web n. 10000877), in materia di verifiche operate dall'INPS sul possesso dei requisiti per l'accesso ad ADI e

SFL. Lo schema ha tenuto conto delle indicazioni fornite dal Garante nel corso delle interlocuzioni intercorse al fine di rendere conformi i trattamenti disciplinati alla normativa in materia di protezione dei dati personali. In particolare, in relazione alle ipotesi di scambi informativi tra l'INPS e le amministrazioni competenti (comuni, Ministero dell'interno, ACI, Agenzia delle entrate, Ministero della giustizia e Ministero dell'istruzione e del merito) sono state verificate le basi giuridiche che legittimano tali flussi di dati personali e i dati oggetto di trattamento sono stati limitati a quelli strettamente necessari ad effettuare le verifiche previste dalla legge, in parte anche secondo un modello di comunicazione già vagliato dal Garante in passato (cfr. provv. 26 novembre 2020, n. 231, doc. web n. 9492971). Lo stesso vale anche per i flussi relativi alla verifica delle condizioni di svantaggio o l'inserimento in programmi di cura e assistenza; sono state, inoltre, definite le procedure per lo scambio tempestivo di informazioni tra l'INPS e le altre amministrazioni in caso di violazioni di dati personali (provv. 12 settembre 2024, n. 541, doc. web n. 10063523).

SIISL e strumenti di IA

Il d.l. 7 maggio 2024, n. 60, nel modificare il d.l. 4 maggio 2023, n. 48, ha introdotto rilevanti disposizioni in riferimento al Sistema informativo per l'inclusione sociale e lavorativa (SIISL), in particolare ampliando la platea di soggetti ivi iscritti anche ai percettori della nuova prestazione di assicurazione sociale per l'impiego (NASPI) e dell'indennità di disoccupazione per i lavoratori con rapporto di collaborazione coordinata e continuativa (DIS-COLL), nonché stabilendo che il SIISL utilizzi strumenti di IA per l'abbinamento ottimale delle offerte e delle domande di lavoro ivi inserite (cfr. artt. 25 e 26). In attuazione delle anzidette disposizioni, il Ministero del lavoro e delle politiche sociali ha sottoposto all'Autorità lo schema di decreto attuativo ove, per effetto dell'accoglimento delle indicazioni fornite dal Garante nel corso delle interlocuzioni informali intercorse, sono state assicurate talune garanzie, quali, tra le altre: una puntuale definizione delle tipologie di dati trattati nonché delle banche dati pubbliche dalle quali tali informazioni originano; il trattamento dei soli dati personali degli interessati necessari al raggiungimento della specifica finalità di selezione, reclutamento e assunzione; il conferimento dei dati di contatto al SIISL da parte degli interessati nonché la loro messa a disposizione per le imprese e i centri per l'impiego solo a seguito di autorizzazione resa dai medesimi; le misure per gli interessati in merito alle operazioni di consultazione ed esportazione dei *curricula vitae* da parte delle imprese. Anche per quanto concerne i trattamenti di dati personali da effettuarsi mediante strumenti di IA (connessi, in particolare, alla generazione e all'utilizzo di un "indice di affinità" basato su un modello di calcolo algoritmico), sono state introdotte specifiche garanzie, fermo restando, in ogni caso, l'obbligo in capo al titolare del trattamento di adottare, a valle della valutazione d'impatto svolta anche tenendo conto delle eventuali opinioni dei soggetti a vario titolo coinvolti nel trattamento in esame, misure tecniche e organizzative adeguate in relazione alle particolari caratteristiche dei trattamenti medesimi, nonché processi di verifica della qualità dei modelli di calcolo alla base degli strumenti di IA impiegati, documentando adeguatamente, in rapporti periodici, le metriche utilizzate, le attività svolte, le eventuali criticità riscontrate e le misure di conseguenza adottate nonché la messa a disposizione dell'Autorità, in caso di specifica richiesta, degli esiti di tali verifiche. Inoltre, l'Autorità si è riservata di effettuare apposite verifiche, in considerazione dei compiti e poteri attribuiti dal RGPD per assicurare il rispetto della disciplina in materia di protezione dei dati personali, anche quando i trattamenti prevedono l'utilizzo di strumenti di IA (provv. 13 novembre 2024, n. 662, doc. web n. 10079136).

Vigilanza in materia di lavoro e legislazione sociale

Altro schema di decreto del Ministro del lavoro e delle politiche sociali su cui il Garante è stato consultato è quello concernente i controlli in materia di lavoro e

legislazione sociale, in attuazione dell'art. 7, comma 3, d.l. 4 maggio 2023, n. 48. Tale disciplina prevede che il personale ispettivo dell'Ispettorato nazionale del lavoro (INL), compreso il personale ispettivo del Comando carabinieri per la tutela del lavoro operante presso l'INL, e la Guardia di finanza, al fine di consentire un efficace svolgimento dell'attività di vigilanza sulla sussistenza di circostanze che comportano la decadenza dal beneficio e di rafforzare i controlli di prevenzione e contrasto del caporalato, dello sfruttamento lavorativo e del lavoro sommerso e irregolare, nonché su altri fenomeni di violazione in materia di lavoro e legislazione sociale, abbiano accesso a tutte le informazioni e le banche dati, sia in forma analitica che aggregata, trattate dall'INPS, già a disposizione del personale ispettivo dipendente dal medesimo Istituto. Nel proprio parere, l'Autorità ha fissato alcune condizioni affinché fossero anzitutto definite le specifiche finalità perseguite da ciascuno dei soggetti abilitati e le tipologie di dati personali cui possono accedere. Il Garante ha inoltre richiesto la previsione di misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi degli interessati laddove siano oggetto di trattamento le categorie particolari di dati personali di cui agli artt. 9 e 10 del RGPD, di misure idonee ad assicurare la correttezza e la trasparenza dei trattamenti effettuati da INL e Guardia di finanza nonché di misure specifiche per la prevenzione e rilevazione degli accessi non autorizzati e per la gestione degli incidenti di sicurezza (provv. 17 ottobre 2024, n. 611, doc. web n. 10073780).

Portale nazionale del sommerso

L'Autorità è stata chiamata a pronunciarsi anche sullo schema di decreto del Ministro del lavoro e delle politiche sociali, attuativo dell'art. 10, d.lgs. 23 aprile 2004, n. 124, che prevede la creazione, presso l'INL, del Portale nazionale del sommerso (PNS) ove, al fine di consentire una efficace programmazione dell'attività ispettiva nonché di monitorare il fenomeno del lavoro sommerso su tutto il territorio nazionale, confluiscano le risultanze dell'attività di vigilanza svolta dall'INL e dal personale ispettivo dell'INPS, dell'INAIL, dell'Arma dei Carabinieri e della Guardia di finanza avverso violazioni in materia di lavoro sommerso nonché in materia di lavoro e legislazione sociale. Il PNS viene altresì reso accessibile alle p.a. e agli enti che erogano o gestiscono fondi pubblici. Considerato che i trattamenti di dati personali previsti presentavano rischi elevati per i diritti e le libertà degli interessati (riguardando, in particolare, dati personali, su larga scala, relativi anche a interessati vulnerabili nel contesto in cui svolgono la propria attività lavorativa), e rilevato che il testo non disciplinava gli elementi essenziali del trattamento, il Garante ha richiesto, pur esprimendo parere favorevole sullo schema, quale condizione, l'introduzione di una disciplina di dettaglio al riguardo, con particolare riferimento a: le tipologie di dati personali trattati (sia con riferimento a quelli che alimentano il PNS che a quelli che vengono messi a disposizione di ciascuno dei soggetti abilitati ad accedere) e i relativi tempi di conservazione; le misure appropriate e specifiche in relazione al trattamento di categorie particolari di dati e di dati relativi a condanne penali e reati (al fine di assicurare l'accesso selettivo); le misure tecniche e organizzative per garantire un livello di sicurezza adeguato ai rischi; i flussi di dati personali tra il PNS e la Piattaforma per la gestione delle azioni di *compliance* e per il contrasto al lavoro sommerso, rilasciata dall'INPS; i ruoli assunti dai soggetti coinvolti nei trattamenti di dati personali (provv. 18 novembre 2024, n. 723, doc. web n. 10095723).

Regolamento ISEE

È stato, inoltre, sottoposto all'Autorità lo schema di d.P.C.M. avente ad oggetto le modifiche al d.P.C.M. 5 dicembre 2013, n. 159, in materia di ISEE (su cui il Garante aveva reso parere con provv. 22 novembre 2012, n. 361, doc. web n. 2174496), al fine di recepire una serie di novelle normative intervenute al riguardo. L'Autorità ha espresso parere favorevole in ragione della conformità del predetto quadro giuridico

4

Provvedimenti correttivi nei confronti dell'INPS

alla disciplina sulla protezione dei dati personali, anche tenuto conto del fatto che le modifiche apportate non hanno inciso sulle garanzie relative ai trattamenti di dati personali effettuati in tale ambito (provv. 9 maggio 2024, n. 290, doc. web n. 10019850).

L'Autorità ha adottato un provvedimento correttivo nei confronti dell'INPS in relazione alle violazioni dei dati personali verificatesi nell'ambito della erogazione delle prestazioni previste dal d.l. 17 marzo 2020, n. 18 (misure di sostegno economico connesse all'emergenza epidemiologica da COVID-19). Tali violazioni erano state determinate dal *caching* delle informazioni personali del servizio di *Content Delivery Network* (CDN) e nei web *server* dell'INPS nonché dall'errata configurazione del sistema di autorizzazione della procedura *bonus baby sitting*, e avevano comportato l'accesso, da parte di utenti terzi, ai dati personali riferiti ad alcuni interessati, in alcuni casi alle domande delle prestazioni richieste. Con riferimento a tali condotte, l'Autorità ha accertato la violazione degli artt. 5, par. 1, lett. a), 12 e 34 del RGPD, avendo l'INPS fornito tardivamente agli interessati coinvolti informazioni adeguate sulle violazioni dei dati personali occorse (cfr. al riguardo il provv. 14 maggio 2020, n. 86, doc. web n. 9344061). L'Autorità ha rilevato, altresì, criticità concernenti i profili relativi alla sicurezza del trattamento, in violazione dell'art. 5, parr. 1, lett. f), e 2, e degli artt. 25 e 32 del RGPD, anche con riferimento alla mancata adozione, da parte dell'Istituto, di misure adeguate a rilevare e gestire tempestivamente le violazioni dei dati personali. Considerati l'eccezionalità del momento in cui i fatti erano avvenuti (si trattava del pieno periodo emergenziale da COVID) e il relativo carico di incombenze gravante sul predetto Istituto per assicurare a milioni di cittadini la tempestiva erogazione di contributi economici, nonché tenuto conto che il medesimo Istituto si era prontamente attivato al fine di porre rimedio alle violazioni ed al contempo attenuarne il danno subìto dagli interessati, il Garante ha ritenuto di dover ammonire l'INPS per le violazioni riscontrate (provv. 17 luglio 2024, n. 475, doc. web n. 10057648).

Altro provvedimento correttivo è stato adottato dall'Autorità nei confronti dell'INPS in relazione al reclamo con cui i genitori adottivi di una minore avevano censurato l'invio, al genitore biologico della predetta minore, di due comunicazioni riguardanti la prestazione di invalidità civile di cui la stessa era beneficiaria.

Ciò aveva comportato la rivelazione al predetto genitore biologico del cognome acquisito dalla minore con l'intervenuta adozione, quale elemento che avrebbe potuto consentire di risalire all'identità dei genitori adottivi della stessa nonché la decadenza della prestazione di invalidità civile di cui la minore era beneficiaria. In particolare, l'Autorità ha comminato all'ente previdenziale una sanzione pecuniaria amministrativa (provv. 19 dicembre 2024, n. 821, doc. web n. 10110135), sul presupposto che il trattamento di dati personali della minore, anche relativi alla sua salute, fosse stato effettuato in maniera non conforme al principio di esattezza e in assenza delle misure appropriate e specifiche necessarie per garantire un'adeguata riservatezza dei dati personali (della minore e della sua famiglia adottiva) assicurando, al contempo, un livello di tutela adeguato al rischio di divulgazione dei dati a soggetti non autorizzati, nonché in maniera non conforme al principio di liceità, correttezza e trasparenza, in ragione del riscontrato contrasto con le disposizioni del vigente quadro normativo di settore che prevede la cessazione dei rapporti con la famiglia d'origine e il divieto di fornire a quest'ultima informazioni relative al rapporto di adozione (cfr. artt. 27, comma 3, e 28, comma 3, l. 4 maggio 1983, n. 184), in violazione dell'art. 5, par. 1, lett. a), d) e f), dell'art. 9, par. 2, lett. g), e dell'art. 32 del RGPD, nonché dell'art. 2-*sexies* del Codice.

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

Anche nel 2024 il Garante ha interagito con il Ministero dell'istruzione e del merito e le istituzioni scolastiche nel corso di incontri e contatti volti a fornire chiarimenti e indicazioni sulla corretta applicazione della disciplina in materia di protezione dei dati personali.

In tale ambito, particolare rilievo ha assunto il provv. 20 febbraio 2024, n. 84 (doc. web n. 10054523) con il quale il Garante ha espresso, in via d'urgenza, parere favorevole, sottoposto a condizione, sullo schema di decreto del predetto Ministero avente ad oggetto "la disciplina sul trattamento dei dati personali effettuato dal Ministero dell'istruzione e del merito e dagli Istituti tecnologici superiori (ITS *Academy*) nell'ambito dell'Anagrafe nazionale dell'istruzione (ANIST) riguardante gli studenti iscritti ai percorsi degli ITS *Academy* e della Banca dati nazionale per il monitoraggio quantitativo e qualitativo del sistema terziario di istruzione tecnologica, nel rispetto di quanto previsto dall'articolo 11, comma 3, del decreto ministeriale 30 novembre 2023, n. 227" (sul quale il Garante ha espresso parere favorevole con provv. 16 novembre 2023, n. 525, doc. web n. 9966592, v. Relazione 2023, p. 41), corredato dal relativo allegato tecnico, che ne costituisce parte integrante.

Lo schema di decreto in parola stabilisce il funzionamento della Sezione ITS *Academy* di ANIST, le modalità di accesso a tale sezione e gli utenti abilitati ad accedere; i dati contenuti nella Sezione ITS di ANIST e della banca dati nazionale, i soggetti coinvolti nel trattamento dei dati, le fonti dei dati e i sistemi di alimentazione; i servizi per il rilascio di certificazioni resi disponibili dalla richiamata sezione; le misure tecnico-informatiche di adeguamento della banca dati nazionale e le relative modalità di raccordo con la sezione; i tempi di conservazione dei dati trattati nella Sezione ITS *Academy* di ANIST e nella BDN. Lo schema di decreto ha tenuto conto delle molteplici osservazioni fornite nel corso delle interlocuzioni informali e delle riunioni con i rappresentanti del Ministero, avviate già nel 2023, al fine di rendere conformi i trattamenti ivi disciplinati alla normativa in materia di protezione dei dati personali, nel rispetto dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita. Tali osservazioni avevano riguardato molteplici profili connessi all'architettura funzionale sopra ricordata; in questa sede si ricordano, in particolare, la specificazione delle finalità perseguite e delle attività di trattamento effettuate tramite la Sezione ITS *Academy* dell'ANIST e la BDN; la precisa individuazione delle categorie di soggetti cui è consentito l'accesso alle informazioni ivi presenti, delle tipologie di dati personali e delle fonti che alimentano la Sezione ITS *Academy* dell'ANIST e la BDN; la descrizione delle tecniche di pseudonimizzazione adottate e le misure tecniche e organizzative intese a garantire la separazione e conservazione dell'informazione aggiuntiva; l'adeguamento delle procedure di autenticazione degli utenti del Ministero al medesimo livello di robustezza di quelle utilizzate dalle altre tipologie di utenti; l'individuazione, nell'ambito delle procedure di autenticazione informatica per l'accesso alla Sezione ITS *Academy*, dei soli dati necessari a questo fine (codice fiscale, cognome e nome); l'esplicitazione dei servizi web resi disponibili ai diversi soggetti coinvolti nel trattamento dei dati personali mediante la Piattaforma digitale nazionale dati (PDND); l'individuazione dei ruoli assunti dagli ITS *Academy* e dal Ministero in relazione ai trattamenti sottesi alle attività di rilascio dei certificati dei titoli di studio; l'individuazione delle specifiche tecniche e delle modalità operative di alimentazione della Sezione ITS *Academy* dell'ANIST e della BDN, nonché delle misure tecniche e organizzative adeguate ad assicurare la tutela dei diritti degli interessati.

Nell'esprimere il parere, l'Autorità ha in particolare rilevato che devono essere

mantenute distinte le operazioni di trattamento che INDIRE svolge, mediante la BDN, per il perseguimento delle proprie finalità da quelle che svolge per conto del Ministero, in qualità di suo responsabile del trattamento e ha pertanto espresso parere favorevole a condizione che lo schema medesimo e l'allegato tecnico fossero modificati prevedendo che i dati personali, riferiti a ciascuna categoria di soggetti componenti la struttura organizzativa degli ITS *Academy,* siano trattati da INDIRE in qualità di responsabile del trattamento, per conto del Ministero dell'istruzione e del merito, nell'ambito delle finalità di accreditamento di cui al d.m. 4 ottobre 2023, n. 191.

Servizio digitale *Knowledge area*

Il Garante ha espresso parere favorevole sullo schema di decreto del Ministero dell'istruzione e del merito che disciplina il trattamento dei dati personali effettuato dal medesimo Ministero nell'ambito dell'abilitazione di nuove utenze ai fini dell'accesso all'area privata della Piattaforma e del servizio digitale *Knowledge area* e, in particolare: l'individuazione di nuovi utenti che possono accedere all'interno della Piattaforma (studenti non frequentanti che sosterranno l'esame di Stato da privatisti presso un'istituzione scolastica, studenti che abbiano conseguito il diploma a partire dall'anno scolastico 2023/2024 e genitori/esercenti la responsabilità genitoriale dei predetti soggetti) e che possono fruire dei servizi erogati tramite la Piattaforma medesima; il trattamento dei dati personali effettuato nell'ambito del servizio di nuova introduzione denominato *Knowledge area* e i ruoli *privacy* dei soggetti coinvolti nel trattamento (Ministero, istituzioni scolastiche, Sogei S.p.A.); le modalità di alimentazione del servizio *Knowledge area* e l'individuazione dei tempi di conservazione dei dati personali oggetto di trattamento.

Anche tale schema di decreto aveva recepito le osservazioni informalmente fornite al Ministero allo scopo di garantire la conformità dei trattamenti ivi disciplinati alla normativa in materia di protezione dei dati personali. Tali osservazioni avevano riguardato, in particolare: l'individuazione dettagliata delle procedure di identificazione e autenticazione informatica per accedere all'area privata della Piattaforma nonché delle misure tecniche e organizzative adeguate ad assicurare la tutela dei diritti degli interessati con riferimento agli specifici trattamenti posti in essere; la previsione dell'obbligo, in capo ai titolari del trattamento a vario titolo coinvolti (Ministero e istituzioni scolastiche), di informazione reciproca e tempestiva in caso di violazioni di sicurezza o di qualsiasi minaccia intervenuta nei trattamenti effettuati all'interno della Piattaforma unica e dei relativi servizi digitali, che comportino un rischio per la sicurezza e per i diritti e le libertà degli interessati, nonché la specificazione dei diversi tempi di conservazione dei dati personali trattati e delle relative finalità di trattamento (provv. 6 giugno 2024, n. 334, doc. web n. 10036855).

Anagrafe nazionale dell'istruzione

Il Garante ha espresso parere favorevole sullo schema di decreto del Ministero dell'istruzione e del merito concernente "la disciplina sul trattamento dei dati personali e sulle specifiche tecniche dei servizi resi disponibili dall'Anagrafe nazionale dell'istruzione" corredato dal relativo allegato tecnico che ne costituisce parte integrante (provv. 26 settembre 2024, n. 578, doc. web n. 10064145).

Lo schema di decreto disciplina il trattamento dei dati personali effettuato dal Ministero nell'ambito dell'Anagrafe nazionale dell'istruzione (ANIST) di cui all'art. 62-*quater* del CAD e i relativi servizi fruibili tramite il suddetto portale con particolare riferimento: alla definizione delle specifiche tecniche dei servizi resi disponibili tramite il Portale ANIST e la Piattaforma digitale nazionale dati di cui all'art. 50-*ter* del CAD (PDND) ai cittadini e alle p.a.; il funzionamento di ANIST, le relative modalità di alimentazione, i dati personali ivi contenuti e i soggetti coinvolti nel trattamento; i servizi erogati ai cittadini e alle p.a. disponibili sul Portale ANIST e le relative modalità di accesso; l'individuazione dei tempi di conservazione dei dati personali oggetto di trattamento.

Anche tale schema di decreto ha recepito le osservazioni formulate nel corso delle interlocuzioni informali e delle riunioni con i rappresentanti del Ministero quali, in particolare: l'individuazione dettagliata delle categorie degli utenti che accedono ai servizi erogati ANIST; la specificazione delle tipologie dei dati personali a cui ciascuna categoria di utente può accedere; la descrizione della procedura di verifica del legame di genitorialità prevista nel caso di accesso da parte dell'utente genitore/esercente la responsabilità genitoriale; l'individuazione del ruolo assunto dai soggetti coinvolti nel trattamento, con riferimento ai servizi di messa a disposizione delle certificazioni scolastiche; la specificazione dei tempi di conservazione dei documenti digitali contenenti le certificazioni richieste dagli utenti, nonché l'indicazione della procedura, mediante il servizio di assistenza tecnica, che l'utente genitore/esercente la responsabilità genitoriale di uno o più utenti minorenni non conviventi, è tenuto a seguire nel caso in cui voglia accedere ai servizi.

Il Garante ha esaminato una pluralità di reclami, segnalazioni e richieste di parere, riguardanti tematiche relative al trattamento di dati personali degli alunni da parte degli istituti scolastici, con particolare riferimento alla pubblicazione di dati personali su siti web istituzionali e alla comunicazione a terzi dei predetti dati, in assenza di una base giuridica idonea e in violazione dei principi applicabili al trattamento.

Trattamenti di dati personali di alunni

In tale ambito, il Garante ha irrogato una sanzione amministrativa pecuniaria nei confronti di un istituto scolastico che aveva pubblicato decine di determinazioni dirigenziali riguardanti le assenze dal servizio di una docente e di altro personale scolastico (provv. 24 gennaio 2024, n. 35, doc. web n. 9987578 cfr. 13.3).

In un altro caso il Garante ha censurato il comportamento di una scuola che aveva inviato, in diverse occasioni, comunicazioni contenenti il calendario delle riunioni del gruppo di lavoro operativo per l'inclusione scolastica (GLO), organizzate dall'istituto e recanti l'indicazione delle iniziali del nome e cognome di tutti gli alunni coinvolti, distinti per classe, a tutti i docenti, genitori, alunni e personale medico sanitario invitati a partecipare, rendendo di fatto identificabili gli studenti interessati. Il Garante ha chiarito che, considerata la definizione di dato personale e di dato relativo alla salute (art. 4, punti 1 e 15, RGPD), la convocazione di una riunione del GLO, prevista dalla normativa di settore in materia di disabilità, rappresenti di per sé una informazione relativa allo stato di salute degli alunni per i quali tale riunione viene convocata. L'istruttoria ha inoltre rilevato che la prassi seguita dall'istituto, pur prevedendo l'uso delle sole iniziali, non era stata sufficiente a garantire l'anonimato degli alunni, configurando così una comunicazione illecita di dati personali anche relativi alla salute. Il Garante ha ricordato che "la prassi seguita da alcune amministrazioni di sostituire il nome e cognome dell'interessato con le sole iniziali è di per sé insufficiente ad anonimizzare i dati personali contenuti negli atti e documenti pubblicati *online*. Inoltre, il rischio di identificare l'interessato è tanto più probabile quando, fra l'altro, accanto alle iniziali del nome e cognome permangono ulteriori informazioni di contesto che rendono comunque identificabile l'interessato (…)" (v. provv. 15 maggio 2014, n. 243, doc. web n. 3134436). Le informazioni relative alla convocazione del GLO, recanti l'indicazione del nominativo o delle iniziali del nome e cognome dell'alunno, possono essere comunicate solo ai genitori dello studente interessato, ai docenti della classe di appartenenza di quest'ultimo e ai soggetti individuati dalla normativa di settore, coinvolti nell'intervento terapeutico e formativo seguito dall'alunno stesso. Per questi motivi, l'Autorità ha rilevato che l'istituto aveva effettuato un trattamento di dati personali in violazione degli artt. 5, 6, 9 del RGPD e 2-*ter* e 2-*sexies* del Codice e ha adottato un provvedimento sanzionatorio (provv. 27 novembre 2024, n. 728, doc. web n. 10097324).

Considerazioni in parte simili hanno condotto il Garante a comminare una sanzione amministrativa pecuniaria nei confronti di un istituto scolastico che aveva inviato a soggetti terzi alcune *e-mail* contenenti i piani educativi individualizzati (PEI) riferiti ad alunni con disabilità. L'istruttoria ha rilevato che le comunicazioni, inviate in più occasioni, riportavano i nominativi degli alunni interessati e le date degli incontri previsti con le famiglie, rendendo così identificabili gli studenti coinvolti e conoscibili le informazioni relative al loro stato di salute. Anche in questo caso, il Garante ha evidenziato che il riferimento al PEI, previsto dalla normativa di settore in materia di disabilità, rappresenta di per sé una informazione relativa allo stato di salute dell'alunno al quale tale documento viene riferito e che esso, elaborato e approvato dal GLO per l'inclusione scolastica, contiene informazioni che possono essere fornite solo a specifici soggetti (genitori dello studente, docenti della classe di appartenenza e soggetti normativamente coinvolti nell'intervento terapeutico e formativo). Nel corso dell'istruttoria è stato, inoltre, rilevato che le richiamate *e-mail*, inviate dall'istituto, recavano in chiaro gli indirizzi di posta elettronica dei destinatari. A tal proposito il Garante ha ribadito che l'invio di messaggi di posta elettronica "con *mailing list* in chiaro costituisce di fatto una comunicazione di dati personali (quelli relativi agli altri indirizzi di posta) a terzi, ossia ai molteplici destinatari" della *e-mail*. Il Garante ha quindi stabilito che la scuola, mediante l'invio delle *e-mail* aveva effettuato una "comunicazione" di dati personali e di categorie particolari di dati personali, in violazione degli artt. 5, 6, 9 del RGPD e 2-*ter* e 2-*sexies* del Codice (provv. 12 dicembre 2024, n. 767, doc. web n. 10099052).

Il Garante ha invece censurato, con un ammonimento, la condotta di una scuola che aveva inviato a tutti i genitori degli alunni di una classe, tramite registro elettronico, un messaggio di posta elettronica contenente un provvedimento, emesso dai servizi di igiene e sanità pubblica della ASL, riguardante la positività al COVID-19 di un alunno. Il Garante anche in questo caso ha chiarito che lo stato di positività al COVID-19 rappresenta una informazione relativa allo stato di salute dell'alunno. Sebbene l'invio della predetta comunicazione non avesse determinato una diffusione di dati personali, la conoscibilità dei dati è avvenuta in favore di un novero, determinato o determinabile, di soggetti, ossia di tutti i genitori della classe, dando luogo ad una comunicazione illecita dei dati personali anche relativi alla salute dell'interessato in violazione degli artt. 5, par. 1, lett. a), 6 e 9 del RGPD nonché 2-*ter* e 2-*sexies* del Codice (provv. 4 luglio 2024, n. 403, doc. web n. 10039592). Un ulteriore ammonimento è stato comminato ad una scuola, a seguito di un reclamo riguardante l'avvenuta somministrazione di taluni *test* nell'ambito di un progetto di ricerca scientifica condotto da una università. In particolare agli alunni della scuola primaria (di età compresa tra i 7 e gli 8 anni) erano stati sottoposti questionari ed erano stati effettuati colloqui individuali finalizzati a valutare le competenze sociali ed emotive, oltre a raccogliere informazioni relative alla loro vita sessuale.

Nel corso dell'istruttoria è emerso che l'istituto scolastico aveva effettuato la raccolta e la conservazione dei dati personali degli alunni per la realizzazione dell'iniziativa di ricerca scientifica, operando per conto dell'università in assenza di designazione ai sensi dell'art. 28 del RGPD, nonché in assenza di una idonea base normativa che ne legittimasse il ruolo concretamente svolto di autonomo titolare, in violazione, quindi, degli artt. 6 e 9 del RGPD. Il Garante ha inoltre chiarito che i dati trattati, seppur oggetto di una qualche forma di pseudonimizzazione o codifica (i *test* non riportavano il nominativo degli alunni ma un numero progressivo, che sembrava coincidere con la posizione dell'alunno nell'elenco della classe, unitamente alla prima lettera del nome e del cognome di ciascun alunno), non potevano essere considerati anonimi ma conservavano la natura di dato personale.

Al riguardo il Garante ha evidenziato che la codifica dei *test* non era tale da escludere la re-identificabilità degli interessati e che, materialmente, i *test* erano stati detenuti dalla scuola; quest'ultima pertanto aveva erroneamente negato la restituzione dei questionari sul falso presupposto della natura anonima degli stessi, in violazione dell'art. 15 del RGPD. Il Garante, considerato che la vicenda aveva avuto luogo pochi mesi dopo l'entrata in vigore del RGPD, che il trattamento dei dati da parte della scuola si era concretizzato unicamente nella raccolta e nella conservazione dei *test* senza accesso diretto al loro contenuto e che la mancata restituzione dei questionari ai genitori degli alunni che ne avevano fatto richiesta era stata determinata da un errore da parte dell'istituto scolastico, dovuto alla convinzione che i *test* fossero anonimi, ha ritenuto sufficiente ammonire il titolare del trattamento (provv. 7 marzo 2024, n. 135, doc. web n. 10008526).

In relazione alla somministrazione di tali *test* si veda anche il provvedimento assunto dal Garante nei confronti dell'università (provv. 7 marzo 2024, n. 136, doc. web n. 10008585).

4.4. *Trasparenza e pubblicità dell'azione amministrativa*

Nel corso dell'anno il Garante ha esaminato numerose questioni riguardanti il tema della protezione dei dati personali con riferimento alle esigenze di trasparenza e di pubblicità dell'azione amministrativa che, per chiarezza espositiva, saranno di seguito trattate in relazione alla pubblicazione di dati personali *online* e all'accesso a informazioni e documenti detenuti dalla p.a. tramite l'istituto dell'accesso civico generalizzato (art. 5, comma 2, d.lgs. n. 33/2013).

4.4.1. Pubblicazioni standardizzate

Schemi standard di pubblicazione redatti dall'ANAC

Si segnala il parere reso su quattordici schemi standard di pubblicazione predisposti da ANAC – riguardanti gli artt. 4-*bis*, 12, 13, 19, 20, 23, 26, 27, 29, 31, 32, 35, 36, 39 e 42, d.lgs. n. 33/2013 – ai sensi dell'art. 48, commi 1 e 3, d.lgs. n. 33/2013 (provv. 22 febbraio 2024, n. 92, doc. web n. 9996090). Gli schemi hanno tenuto conto delle osservazioni fornite dall'Ufficio relativamente a:

- limitare la pubblicazione dei dati di contatto utilizzabili dal cittadino per qualsiasi richiesta inerente ai compiti istituzionali a quelli dell'ufficio e non alla persona;
- indicare, con riferimento alla pubblicazione dei dati delle persone vincitrici di concorsi pubblici (e degli idonei vincitori a seguito di scorrimento della graduatoria) il nome e cognome, ed eventualmente la data di nascita (ad es., in caso di omonimia), nonché la posizione in graduatoria (escludendo quindi altre informazioni non necessarie come il luogo di nascita, il codice fiscale, la residenza, ecc.);
- oscurare i dati personali eventualmente presenti nell'oggetto (e nei documenti pubblicati *online* in via facoltativa) degli accordi stipulati dall'amministrazione con soggetti privati o con altre amministrazioni pubbliche;
- omettere i nominativi e i dati identificativi di persone fisiche destinatarie di benefici economici se dalla pubblicazione è possibile ricavare informazioni relative allo stato di salute o alla situazione di disagio economico-sociale degli interessati;
- pubblicare gli atti degli organismi indipendenti di valutazione o dei nuclei di valutazione, procedendo all'indicazione in forma anonima dei dati personali eventualmente presenti come previsto dall'articolo citato;
- in relazione alla pubblicazione delle informazioni relative alla *class action*, escludere la pubblicazione dei nomi delle parti, laddove si tratti di persone fisiche.

Il Garante ha inoltre chiesto ad ANAC di modificare lo schema standard di pubblicazione relativo:

- all'art. 4-*bis* (Trasparenza nell'utilizzo delle risorse pubbliche), coerentemente con quanto previsto dagli artt. 26 e 27, d.lgs. n. 33/2013;
- all'art. 20 (Obblighi di pubblicazione dei dati relativi alla valutazione della *performance* e alla distribuzione dei premi al personale), allo scopo di dare indicazione esclusivamente di dati opportunamente aggregati in conformità ai criteri indicati nel parere.

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

Sanzioni per illecita diffusione di dati sulla salute

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

In particolare, si menziona un caso in cui il Garante ha sanzionato un comune per aver pubblicato determinazioni riguardanti la liquidazione di contributi economici per agevolare i trasferimenti di soggetti sottoposti a trattamenti chemioterapici/radioterapici o dialitici e/o comunque in terapie salvavita continuative, con indicazione del relativo codice fiscale e del codice IBAN su cui accreditare le somme (provv. 6 giugno 2024, n. 362, doc. web n. 10032683).

Diffusione illecita di dati personali

Diversi sono stati gli interventi che hanno portato anche all'adozione di specifiche sanzioni o ammonimenti nei confronti di soggetti pubblici titolari del trattamento, per aver diffuso *online* dati personali in assenza di un'idonea base normativa in violazione dell'art. 2-*ter*, commi 1 e 3, del Codice e dell'art. 6, par. 1, lett. c) ed e); par. 2 e par. 3, lett. b), RGPD nonché del principio di minimizzazione di cui all'art. 5, par. 1, lett. c), RGPD. In particolare è stata dichiarata l'illiceità del trattamento effettuato da alcuni enti locali per aver pubblicato sul sito web istituzionale:

- una deliberazione della giunta con la quale era stata approvata la costituzione in giudizio dell'ente in un procedimento penale e il conferimento dell'incarico al difensore di fiducia, con indicazione in chiaro delle iniziali della controparte e del relativo coinvolgimento nel procedimento penale per il reato di furto beni pubblici. In tale contesto, pur tenendo conto della volontà del comune, titolare del trattamento, di non rendere identificabile il soggetto interessato sostituendo il nominativo con le iniziali del nome e cognome, è stato rilevato che tale accorgimento – unitamente alle informazioni e ai dati di contesto contenuti nella delibera pubblicata *online* quali ad es., la descrizione del reato contestato – non era idoneo a eliminare del tutto il rischio che il soggetto interessato potesse essere identificato da conoscenti e altri soggetti in ambito locale (considerando il ristretto contesto territoriale di riferimento riferito a un comune di circa 2.500 abitanti) (provv. 17 ottobre 2024, n. 614, doc. web n. 10079511);
- una deliberazione della giunta che riportava in chiaro dati del soggetto interessato (nominativo, residenza, data e luogo di nascita), nonché la circostanza di avere presentato una petizione/proposta popolare con la quale si chiedeva l'intervento dell'amministrazione comunale per intraprendere le azioni necessarie per la realizzazione di un impianto sportivo polivalente (provv. 13 novembre 2024, n. 664, doc. web n. 10082729);
- alcune determinazioni dirigenziali che riportavano in chiaro i dati personali delle guardie ecologiche volontarie (quali nominativo, *e-mail*, numero di cellulare, rimborsi ricevuti e IBAN su cui accreditare le somme) nonché dei soggetti sanzionati per violazioni delle leggi di competenza (quali nominativo e importo della sanzione ricevuta) (provv. 26 settembre 2024, n. 607, doc. web n. 10077313).

4.4.3. Accesso civico

Come già accaduto in passato, il Garante ha invitato le amministrazioni a rivalutare l'accoglimento di istanze di accesso civico che contrastavano con le limitazioni previste dall'art. 5-*bis,* comma 2 ovvero comma 3, d.lgs n. 33/2013.

Limitazioni *ex* art. 5-*bis*, comma 3, d.lgs. n. 33/2013

In diverse occasioni è stata ribadita la sussistenza di casi di esclusione dell'accesso civico laddove l'istanza aveva avuto a oggetto dati sulla salute. A parte casi generali (v. ad es., provv.ti 12 settembre 2024, n. 558, doc. web n. 10062415; 27 luglio 2024, n. 471, doc. web n. 10061292), si evidenziano le fattispecie seguenti:

- equo indennizzo: una delicata questione ha riguardato l'accesso civico alle indennità liquidate a militari e, in particolare, alle determinazioni di concessione di equo indennizzo e di ogni altro beneficio economico concessi, a qualsiasi titolo, a carico del bilancio dello Stato in conseguenza dell'attentato al contingente italiano impiegato nell'ambito dell'operazione "Antica Babilonia" a Nassiryia (Iraq) del 12 novembre 2003. Dall'istruttoria è emerso che sia nel caso di equo indennizzo che in quello di concessioni di speciali benefici (quali l'assegno vitalizio, la speciale elargizione e lo speciale assegno vitalizio) si tratta di provvedimenti in cui sono riportati dati sanitari (verbale della commissione medico ospedaliera, parere del comitato di verifica con relativa patologia/infermità) in relazione ai quali pertanto l'accesso civico è escluso ai sensi dell'art. 5, comma 3, d.lgs. n. 33/2013 (provv. 29 dicembre 2024, n. 831, doc. web n. 10107774);

- dati su vaccinazioni: analogamente, merita di essere citato un caso concernente l'accesso a dati riguardanti informazioni sui vaccini o contenute nell'anagrafe vaccinale, sul quale in passato il Garante si è più volte pronunciato. L'Autorità ha in particolare valutato un'istanza di accesso civico presentata a una regione ed avente a oggetto i dati vaccinali di coloro a cui erano state somministrate una o più dosi del vaccino anti COVID-19 e quelli dei soggetti deceduti. Più nel dettaglio tali dati erano stati richiesti aggregati per regione, provincia, mese, anno, sesso, fascia di età quinquennale, numero di dose, eventuale decesso, causa del decesso. Il Garante ha al riguardo evidenziato che i dati richiesti erano riferiti a soggetti vaccinati trattati su larga scala e alle dosi di vaccino effettuate, il cui numero poteva essere idoneo a rivelare – nel caso ad esempio dell'effettuazione di una sola dose o del mancato completamento del ciclo vaccinale – l'esistenza di possibili casi di esonero successivo o differito connessi a situazioni di morbilità, pregresse o attuali, temporanee o permanenti (con la conseguente riconducibilità alle categorie particolari di dati personali di cui all'art. 9 del RGPD) oppure ad altre convinzioni personali. Per tali motivi, è stato ritenuto necessario effettuare un'adeguata valutazione circa il rischio di re-identificabilità dei soggetti interessati (fra cui minori e soggetti deboli) tramite l'ostensione dei dati richiesti, anche in ragione del possibile incrocio dei dati con altre fonti, banche dati o dati statistici idonei a fornire informazioni ulteriori sugli stessi assistiti (provv. 19 febbraio 2024, n. 82, doc. web n. 9996647). Il Garante ha anche ritenuto di non potersi discostare dal diniego e dalle valutazioni già effettuate dalla regione sulla quale peraltro, in base al principio di *accountability*/responsabilizzazione del titolare del trattamento, ricade l'onere della valutazione in concreto sulla legittimità del trattamento (art. 5, par. 2, e 24 del RGPD), tenendo conto anche della possibilità per il soggetto istante (ma, dato il regime di pubblicità propria dell'accesso civico, anche per soggetti terzi) di incrociare e raffrontare i dati ottenuti con altre informazioni ausiliarie già conosciute o contenute in ulteriori banche dati o in dati statistici (su analoga questione v. anche provv.ti 19 febbraio 2024, n. 83, doc. web n. 9999918; 3 maggio 2024, n. 265, doc. web n. 10061232; 30 maggio 2024, n. 332, doc. web n. 10104889).

Limitazioni *ex* 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, ritenendo sussistere il limite derivante dalla protezione dei dati personali di cui all'art. 5-

4

bis, comma 2, lett. a), d.lgs. n. 33/2013. Ciò con particolare riferimento a:

- dati di tipo giudiziario: nello specifico, un'istanza di accesso civico concernente gli atti "presupposti" a una delibera di giunta avente a oggetto l'affidamento di un incarico professionale a un avvocato esterno al comune, con espresso mandato a proporre denuncia-querela nei confronti di un cittadino che aveva caricato dei commenti *online* su un *social network*, ritenuti non veritieri e offensivi e diffamatori nei confronti dell'amministrazione comunale. Al riguardo, è stato evidenziato che i dati personali del soggetto nei confronti del quale l'amministrazione aveva deciso di proporre denuncia/querela erano dati delicati di tipo giudiziario, in quanto afferenti a una fattispecie di reato e oggetto, di conseguenza, delle ulteriori garanzie previste per i dati riguardanti "condanne penali e reati" (art. 10 del RGPD, art. 2-*octies*, del Codice). Per tale motivo si è concordato con il diniego dell'accesso opposto dall'amministrazione, tenendo anche conto che i documenti richiesti contenevano informazioni e dati personali, che si riferivano a fatti e circostanze che erano risultate essere in una fase ancora preliminare meritevole di una protezione adeguata (provv. 3 ottobre 2024, n. 608, doc. web n. 10075926);
- copia degli elaborati della prova scritta e della prova pratica del concorso pubblico: conformemente ai precedenti orientamenti del Garante, si è concordato con il diniego dell'amministrazione, evidenziando di non poter accordare neanche un accesso civico parziale per il rischio di re-identificazione dei soggetti controinteressati. (provv. 27 novembre 2024, n. 726, doc. web n. 10100342. Sul tema dei documenti dei concorsi pubblici v. anche provv. 27 dicembre 2024, n. 825, doc. web n. 10108107);
- copia del documento contenente il nominativo del dipendente e la volontà di essere trasferito presso un altro ente pubblico: è stato precisato che l'ostensione di tale documento determina un'interferenza ingiustificata e sproporzionata nei diritti e libertà del dipendente, in quanto la generale conoscenza della volontà di voler cambiare ruolo o datore di lavoro può determinare conseguenze sul piano relazionale e professionale del controinteressato sia all'interno che all'esterno dell'ambiente lavorativo, in violazione del principio di minimizzazione dei dati, arrecando un pregiudizio concreto alla tutela della protezione dei dati personali (provv. 13 agosto 2024, n. 480, doc. web n. 10068091);
- informazioni sulle presenze di dipendenti: il Garante è tornato su questo argomento, già oggetto di precedenti pareri, esaminando un caso di accesso civico, fra l'altro, a informazioni contenute negli statini dei componenti del Consiglio centrale della rappresentanza militare in cui erano indicati orari di servizio (inizio e fine attività); attività informativa e permessi divisa per singoli giorni, comunicazioni di assenza con indicazione dei motivi. Al riguardo, è stato ribadito che si tratta di informazioni di carattere personale che, per motivi individuali del militare dipendente, non sempre si desidera portare a conoscenza di soggetti estranei e la cui ostensione appare eccedente e contraria al principio di minimizzazione dei dati (art. 5, par. 1, lett. c, RGPD) anche rispetto all'oggetto dell'istanza di accesso civico presentata nel caso in esame (provv. 24 gennaio 2024, n. 54, doc. web n. 9977461);
- verbali contenenti le valutazioni comparative del personale finalizzate all'attribuzione di incarichi di responsabilità o elevata qualificazione: al riguardo, si segnalano diversi pareri resi sull'argomento nei quali si è concordato con il rifiuto opposto dall'amministrazione all'istanza di accesso civico generalizzato (provv.ti 19 settembre 2024, n. 575, doc. web n. 10105106; 5 febbraio 2024, n. 59, doc. web n. 9986254; 8 gennaio 2024, n. 1, doc. web n. 10109748). In generale, è stato ribadito che le valutazioni comparative riportano dati e informazioni personali di natura delicata riferiti a tutti i dipendenti oggetto di valutazione e riguardanti, fra l'altro, le caratteristiche individuali relative, ad

esempio, alla preparazione professionale e alla migliore o minore attitudine a svolgere un determinato incarico quale un ruolo di elevata qualificazione (che costituiscono aspetti valutabili nella selezione dei partecipanti). Anche considerando che qualsiasi esame è diretto a verificare e a stabilire le prestazioni individuali di una specifica persona (sent. CGUE 20 dicembre 2017, C-434/16, punto n. 39), un eventuale accesso civico ai documenti richiesti (verbali o documenti contenenti le valutazioni comparative dei partecipanti alla selezione), in quanto riferiti ai singoli dipendenti e riguardanti anche informazioni di carattere attitudinale, avrebbe potuto esporre gli interessati a difficoltà relazionali con i colleghi di lavoro e creare ingiustificati pregiudizi da parte degli utenti esterni (provv. 5 febbraio 2024, n. 59, doc. web n. 9986254, cit.);

- elenco dei partecipanti e *curricula* di coloro che hanno solo presentato la candidatura, ma non sono stati selezionati per un incarico istituzionale (provv. 22 febbraio 2024, n. 124, doc. web n. 9995366). Il Garante ha nuovamente ricordato che la normativa in materia di trasparenza non prevede obblighi di pubblicità dei dati personali riferiti ai singoli partecipanti a una selezione pubblica. Nel caso in esame, è stato pertanto evidenziato che la conoscibilità della partecipazione a una selezione pubblica e la connessa volontà/disponibilità a cambiare lavoro, ruolo, datore di lavoro pubblico o privato può determinare conseguenze sul piano relazionale e professionale dei controinteressati, soprattutto considerando che nel caso in esame si era trattato di persone che non avevano superato la selezione. In relazione, inoltre, ai *curricula* dei soggetti che non erano stati selezionati per gli incarichi banditi, è stato evidenziato che, in generale, i dati e le informazioni personali contenuti nel *curriculum vitae* sono molteplici e la relativa ostensione può consentire l'accesso, a seconda di come è redatto il *curriculum*, a numerose informazioni di carattere personale che non sempre si desidera portare a conoscenza di soggetti estranei; pertanto un eventuale accoglimento di un'istanza di accesso civico all'elenco dei partecipanti non selezionati e al relativo *curriculum* può effettivamente arrecare ai soggetti interessati, a seconda delle ipotesi e dell'utilizzo dei dati da parte dei terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-*bis,* comma 2, lett. a), d.lgs. n. 33/2013;

- documenti contenuti nella CILA: in conformità ai precedenti orientamenti, il Garante ha ribadito che l'ostensione dei dati in parola (ovvero, oltre al dato anagrafico, eventuali informazioni relative alla proprietà immobiliare, all'effettuazione di interventi edilizi, alla scelta di una specifica impresa, all'effettuazione di un illecito amministrativo), anche in questo caso, può determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei soggetti coinvolti, in violazione del principio di minimizzazione dei dati (art. 5, par. 1, lett. c, RGPD) e un pregiudizio concreto alla tutela della protezione dei dati personali di cui all'art. 5-*bis*, comma 2, lett. a), d.lgs. n. 33/2013 (provv. 24 gennaio 2024, n. 55, doc. web n. 9981555; in materia di titoli edilizi v. anche provv. 24 aprile 2024, n. 241, doc. web n. 10018263).

In altri casi, il Garante ha invece rilevato l'insussistenza delle limitazioni in questione. Si menziona il parere reso su una fattispecie complessa in cui, fra l'altro, il Garante ha rappresentato che non poteva essere opposto alcun motivo di protezione dei dati personali in relazione alla ostensione dell'entità del rimborso a carico del comune (e liquidato dalla società di assicurazione) delle spese legali affrontate dal sindaco, tenuto in considerazione il regime di pubblicità e trasparenza rafforzato richiesto per coloro che rivestono incarichi di indirizzo politico in relazione ai compensi percepiti (art. 14, d.lgs. n. 33/2013) e dell'attenuata aspettativa di confidenzialità in capo a coloro che rivestono incarichi pubblici quali gli amministratori di un ente locale (provv. 20 giugno 2024, n. 366, doc. web n. 10060992).

Rilevatori di violazioni del codice della strada

4.5. *Mobilità e trasporti*

4.5.1. Regolamentazione e trattamenti effettuati a livello centrale

L'Autorità si è espressa con parere favorevole in merito allo schema di decreto del Ministro delle infrastrutture e dei trasporti, di concerto con il Ministro dell'interno, relativo alle modalità di collocazione e uso dei dispositivi o mezzi tecnici di controllo, finalizzati al rilevamento a distanza delle violazioni delle norme di comportamento di cui all'art. 142, d.lgs. 16 dicembre 1992, n. 285. Lo schema di decreto ha individuato la titolarità del trattamento dei dati raccolti mediante tali sistemi in capo all'amministrazione da cui dipende l'organo di polizia stradale che procede all'accertamento. L'all. B del medesimo schema ha previsto, in particolare, che le fotografie o le immagini che costituiscono fonte di prova per gli illeciti accertati non devono essere inviate al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione della violazione; l'accesso alla documentazione fotografica o dei video, infatti, deve essere reso disponibile a richiesta del destinatario del verbale, nel rispetto delle norme sull'accesso ai dati personali ai sensi dell'art. 25 della l. n. 241/1990 e sul diritto di accesso ai dati personali ai sensi degli artt. 12 e 15 del RGPD, garantendo, in ogni caso, che siano opportunamente oscurati o resi non riconoscibili i soggetti e le targhe di eventuali altri veicoli. In sede redazionale i Ministeri procedenti hanno tenuto conto delle osservazioni rese dal Garante nel corso delle interlocuzioni intercorse al fine di conformare i trattamenti disciplinati alla normativa in materia di protezione dei dati personali. Sono stati, pertanto, dettagliati i ruoli ricoperti dai soggetti coinvolti nel trattamento dei dati personali derivanti dall'utilizzo dei dispositivi di controllo ed è stata prevista la necessità di regolare i rapporti con i soggetti terzi, affidatari di attività complementari alla gestione amministrativa dei procedimenti sanzionatori, ai sensi dell'art. 28 del RGPD.

È stato, altresì, precisato che i dispositivi e sistemi, pur potendo effettuare un continuo monitoraggio del traffico, devono memorizzare le immagini solo in caso di infrazione, nel rispetto del principio di "minimizzazione dei dati" di cui all'art. 5, par. 1, lett. c), RGPD e che è consentito l'impiego di dispositivi o sistemi di rilevamento della velocità che effettuano la ripresa frontale del veicolo solo se provvisti di una funzione che oscura automaticamente le parti di immagini che permettono di identificare le persone che vi si trovano a bordo. Infine, è stato previsto che le immagini rilevate devono essere fruibili solo per l'accertamento e la contestazione degli illeciti stradali, nel rispetto del principio di "limitazione della finalità" di cui all'art. 5, par. 1, lett. b), RGPD.

Infine, nel rispetto dei principi di "integrità e riservatezza" e di "responsabilizzazione" (artt. 5, parr. 1, lett. f) e 2; 24, 25 e 32 del RGPD), è stata espressamente indicata la necessità di adottare misure tecniche e organizzative al fine di assicurare un adeguato livello di sicurezza dei trattamenti, incluse misure utili ad evitare l'accesso non autorizzato ai dati e alle risultanze fotografiche o video delle infrazioni al codice della strada (provv. 11 gennaio 2024, n. 2, doc. web n. 9983228).

Parere NCC

L'Autorità si è espressa con parere favorevole in merito allo schema di d.P.C.M., su proposta del Ministro delle infrastrutture e dei trasporti e del Ministro delle imprese e del *made in Italy*, da adottare ai sensi dell'art. 17, comma 3, l. n. 400/1988, recante la disciplina dell'attività delle piattaforme tecnologiche di intermediazione che intermediano tra domanda e offerta di autoservizi pubblici non di linea. Tale schema di decreto si inserisce in una attività di riforma del settore dei servizi taxi e noleggio con conducente e, pertanto, è stato oggetto di esame congiunto con lo schema di decreto del medesimo Ministero, recante le modalità di attivazione del registro informatico pubblico nazionale

istituito presso il CED del Dipartimento per i trasporti e la navigazione del Ministero delle infrastrutture e dei trasporti", "le specifiche tecniche nonché le relative modalità di accesso e di registrazione al medesimo registro da parte dei titolari di licenza per il servizio taxi (…) e dei titolari di autorizzazione per il servizio di noleggio con conducente (…)" e lo schema di decreto, di concerto con il Ministero dell'interno, recante "le modalità di tenuta e compilazione del foglio di servizio elettronico ai fini dello svolgimento del servizio di noleggio con conducente" (…) (cd. decreto FDSE). Gli schemi esaminati hanno tenuto conto delle indicazioni fornite dal Garante nel corso delle interlocuzioni con il Ministero delle infrastrutture e dei trasporti, concernenti, in particolare, la puntualizzazione dei ruoli ricoperti dai soggetti coinvolti nel trattamento dei dati personali, la definizione dei tempi di conservazione dei dati personali, nel rispetto del principio di "limitazione della conservazione" di cui all'art. 5, par. 1, lett. e), RGPD, in particolare per quanto concerne la documentazione di ogni contratto concluso con gli utenti per servizi taxi o servizi NCC e i dati del RENT, la necessità di adottare misure tecniche e organizzative al fine di assicurare un adeguato livello di sicurezza dei trattamenti, nel rispetto dei principi di "integrità e riservatezza" (artt. 5, parr. 1, lett. f) e 2 e 32 del RGPD) integrando, in particolare le misure previste nei relativi allegati tecnici del decreto RENT e decreto FDSE nonché l'individuazione puntuale, nel decreto RENT, delle informazioni oggetto di registrazione nel RENT, concernenti i contratti di durata di cui all'art. 3, comma 2, nel rispetto del principio di "minimizzazione" (art. 5, par. 1, lett. c), RGPD), e prevedendo, altresì, nell'all. 1) lett. c) del decreto FDSE che, con riferimento ai contratti di durata stipulati dal vettore NCC, le informazioni che il predetto vettore è tenuto a fornire ai fini della registrazione sull'applicazione informatica riguardano i "dati" (seppur non dettagliati ma che, per coerenza, devono essere considerati coincidenti con le medesime informazioni oggetto di registrazione nel RENT), anziché la copia integrale dei contratti stessi. Tuttavia, in considerazione del permanere di alcune residuali osservazioni sotto il profilo dei tempi di conservazione dei dati personali con riferimento al decreto FDSE, l'Autorità ha formulato delle osservazioni in merito all'opportunità che si rendano conformi i tempi di conservazione previsti dall'art. 7, lett. l) ed m) al termine di due anni previsto dall'art. 3, come modificato dall'art. 1, comma 153, della l. 24 dicembre 2007, n. 244, del d.l. 30 settembre, n. 203, nel rispetto del predetto principio di limitazione della conservazione (provv. 23 maggio 2024, n. 328, doc. web n. 10019934).

Registro unico degli ispettori di revisione (RUI)

Il Ministero delle infrastrutture e dei trasporti ha trasmesso all'Autorità, ai fini dell'acquisizione del relativo parere, lo schema di decreto della Direzione generale della motorizzazione concernente la disciplina del trattamento dei dati personali effettuato dal Ministero nell'ambito della nuova versione informatica del registro unico degli ispettori di revisione (RUI) – istituito ai sensi dell'art. 4, comma 1, del d.m. 11 dicembre 2019, quale elenco informatico di registrazione degli ispettori e delle informazioni ad essi associati, ivi compreso l'archivio delle annotazioni disciplinari e delle sanzioni – con particolare riferimento alle modalità di implementazione, funzionamento e aggiornamento dello stesso. Lo schema di decreto, tenuto conto delle osservazioni rese dal Garante nel corso delle interlocuzioni intercorse con il Ministero, ha in particolare descritto nel dettaglio i dati acquisiti nel RUI, relativi agli esiti degli eventuali procedimenti sanzionatori riguardanti gli ispettori autorizzati ed ha circoscritto il trattamento dei dati relativi ai predetti provvedimenti al solo esito degli stessi (ossia la sospensione o la revoca) nel rispetto del principio di minimizzazione di cui all'art. 5 del RGPD. Inoltre, ha individuato le modalità di identificazione e autenticazione informatica degli utenti abilitati ad accedere, in tempo reale in modalità telematica, al RUI, nonché le garanzie e le misure di sicurezza, appropriate e specifiche, finalizzate a

tutelare i diritti fondamentali e gli interessi delle persone fisiche i cui dati sono trattati nel RUI, in ossequio al principio di integrità e riservatezza e agli obblighi di sicurezza (artt. 5, par. 1, lett. f), e 32 del RGPD), nonché specificato i diversi tempi di conservazione dei dati personali trattati, nel rispetto del principio di "limitazione della conservazione" (art. 5, par. 1, lett. e), RGPD). Su tali basi, il Garante ha espresso parere favorevole (provv. 18 luglio 2024, n. 462, doc. web n. 10057148).

Registro unico telematico dei veicoli fuori uso (RVFU)

É stato inoltre sottoposto all'Autorità lo schema di decreto direttoriale del Ministero delle infrastrutture e dei trasporti, volto a disciplinare, nell'ambito del registro unico telematico dei veicoli fuori uso (RVFU) – istituito presso il CED della Direzione generale per la motorizzazione – l'attribuzione di funzioni e compiti ai soggetti coinvolti nel trattamento dei dati personali, nonché la definizione dei periodi di conservazione e delle misure tecniche e organizzative necessarie per garantire la tutela dei dati medesimi. Lo schema di decreto ha disciplinato, ai fini dell'alimentazione, della tenuta, dell'aggiornamento e del mantenimento del registro, nonché della produzione del certificato di rottamazione, il trattamento dei dati personali acquisiti dal predetto Ministero direttamente dalla persona fisica cui gli stessi si riferiscono, ovvero per il tramite degli operatori professionali (es. concessionari, centri di raccolta obbligati al popolamento e all'aggiornamento del registro). Anche in questo caso lo schema ha tenuto conto delle osservazioni rese dall'Autorità nel corso delle interlocuzioni intercorse con il Ministero, finalizzate a conformare i trattamenti ivi disciplinati alla normativa in materia di protezione dei dati personali, con particolare riguardo al principio di integrità e riservatezza e agli obblighi di sicurezza (artt. 5, par. 1, lett. f), e 32 del RGPD). Ciò con particolare riferimento a taluni profili, quali (tra gli altri) l'individuazione delle modalità di identificazione e autenticazione informatica degli utenti abilitati ad accedere al registro, nonché l'implementazione di garanzie e misure di sicurezza appropriate e specifiche. L'Autorità ha quindi espresso parere favorevole, evidenziando la necessità di integrare lo schema, in particolare, specificando i soggetti legittimati ad accedere al registro per visionare i dati per finalità di tutela dell'ordine pubblico e indagine giudiziaria, nonché introducendo un doppio fattore di autenticazione per l'accesso alla VPN del Ministero da parte degli operatori professionali, al fine di assicurare una maggiore robustezza delle modalità di autenticazione informatica al registro (provv. 17 ottobre 2024, n. 656, doc. web 10079489).

Sospensione della patente

L'Autorità ha avviato un'istruttoria in merito ad un reclamo presentato nei confronti del Ministero dell'interno - Prefettura di Roma e di una ASL, relativo al trattamento dei dati personali del reclamante posto in essere nell'ambito degli accertamenti conseguenti alla sospensione della patente, nonché relativamente all'esercizio del diritto di cancellazione dei propri dati formulato dal reclamante ai sensi dell'art. 17 del RGPD. In tale contesto, in considerazione del fatto che la violazione aveva riguardato un solo interessato, che la stessa era avvenuta in un contesto organizzativo particolarmente critico, anche dal punto di vista temporale, che il titolare del trattamento aveva prestato piena collaborazione all'Autorità nel corso dell'istruttoria, e che a seguito della stessa, aveva provveduto a sensibilizzare la struttura interessata sulla protezione dei dati, è stato rivolto un ammonimento al Ministero dell'interno, per aver tardivamente riscontrato l'istanza, in violazione dell'art. 12 del RGPD (provv. 26 settembre 2024, n. 587, doc. web n. 10066215).

4.5.2. Mobilità in ambito locale

Nel corso dell'istruttoria originata da un reclamo, l'Autorità ha rilevato che nell'informativa fornita da un comune, riportata nei verbali di contestazione di violazioni stradali, erano stati menzionati riferimenti non aggiornati in merito alla

normativa sulla protezione dei dati personali e non erano state indicate le modalità di accesso, da parte degli interessati, ad un'informativa completa di "secondo livello" nella quale poter acquisire gli ulteriori elementi previsti dagli artt. 13 e 14 del RGPD, tra cui i dati di contatto del responsabile della protezione dei dati, i soggetti coinvolti nel trattamento dei dati personali, l'indicazione dei diritti riconosciuti agli interessati ai sensi degli artt. da 15 a 22 del RGPD, le modalità di esercizio degli stessi, nonché il diritto di proporre reclamo all'Autorità. Il comune aveva rappresentato di aver provveduto, a seguito della richiesta d'informazioni dell'Autorità, ad integrare il *format* di informativa "di primo livello" presente nei verbali di accertamento e di aver adottato un'informativa estesa, pubblicata sul proprio sito web istituzionale. Tuttavia, l'informativa stratificata era risultata ancora carente di alcuni elementi obbligatori a norma degli artt. 13 e 14 del RGPD (modalità di esercizio dei diritti riconosciuti agli interessati ai sensi degli artt. da 15 a 22 del RGPD, nonché il diritto di proporre reclamo all'Autorità) non essendo tali elementi ancora adeguatamente menzionati almeno nell'informativa di "secondo livello". In aggiunta, l'Autorità ha accertato che la predetta informativa non risultava essere facilmente raggiungibile da parte degli interessati nell'ambito della navigazione sul sito web istituzionale. Per tali ragioni l'Autorità ha sanzionato il comune, titolare del trattamento, per violazione degli artt. 5, par. 1, lett. a), 12 e 13 del RGPD, ingiungendo al medesimo, ai sensi dell'art. 58, par. 2, lett. d), RGPD, di adottare le misure idonee a rendere, per quanto concerne i trattamenti di dati personali effettuati ai fini dell'accertamento di violazioni al codice della strada, l'informativa di secondo livello completa degli ulteriori elementi obbligatori previsti dagli artt. 13 e 14 del RGPD (nei termini sopra indicati) e facilmente reperibile e accessibile da parte degli interessati, provvedendo alla cancellazione di eventuali informative obsolete e/o duplicate e alla valutazione di riorganizzare il proprio sito web istituzionale evitando percorsi di navigazione multipli per raggiungere la predetta informativa nonché la cd. *click fatigue* per gli interessati (provv. 27 novembre 2024, n. 727, doc. web 10097307).

4.6. *Trattamenti in ambito locale*

4.6.1. Ambiente

A seguito di un'istruttoria, originata da un reclamo presentato nei confronti di un comune e del gestore del servizio locale di raccolta dei rifiuti e da una notifica di violazione dei dati personali, ai sensi dell'art. 33 del RGPD, inviata dal medesimo comune, l'Autorità ha adottato due provvedimenti sanzionatori. In particolare, nel reclamo era stata rappresentata la ricezione di una comunicazione a mezzo della quale il comune aveva informato gli interessati di essere venuto a conoscenza, per il tramite del predetto gestore, di una possibile illegittima diffusione, mediante *social media*, di dati personali particolari, relativi alle abitazioni di residenza di soggetti che avrebbero necessitato di una particolare tutela legata all'emergenza epidemiologica da COVID-19. Nel riscontrare le richieste di informazioni avanzate dall'Autorità, sia il comune che il gestore avevano evidenziato che la predetta diffusione era stata cagionata da un'acquisizione fraudolenta di un documento interno da parte di un operatore del predetto gestore, con conseguente imputabilità della condotta al gestore del servizio locale di raccolta rifiuti. Tuttavia, nell'ambito dell'istruttoria era emerso che tra il comune e il gestore del servizio locale non era stato inizialmente stipulato un contratto o altro atto giuridico che vincolasse quest'ultimo in qualità di responsabile del trattamento al titolare del trattamento, avendo il comune ritenuto, in un primo momento, il gestore quale autonomo titolare dei trattamenti dei dati personali sottesi

alla gestione dei rifiuti urbani ed avendo provveduto a stipulare il relativo atto giuridico ai sensi dell'art. 28 del RGPD solo in un momento successivo all'avvio dell'istruttoria. Sul punto, l'Autorità ha ribadito che la gestione dei rifiuti urbani rientra tra le attività istituzionali affidate agli enti locali, titolari del trattamento, che possono essere svolte da soggetti terzi – responsabili del trattamento – in nome e per conto del titolare, disciplinando il rapporto ai sensi dell'art. 28 del RGPD. La mancata stipula di un contratto o atto giuridico con il gestore aveva comportato l'omessa definizione di istruzioni funzionali a garantire una maggiore conformità dei trattamenti effettuati alla normativa sulla protezione dati quali l'avvenuta illecita diffusione di dati e la violazione del principio di responsabilizzazione di cui agli artt. 5, par. 2 e 24 del RGPD. Tale principio, come chiarito nelle linee guida 07/2020 in merito alle figure di titolare del trattamento e di responsabile del trattamento ai sensi del RGPD, adottate dal Comitato il 7 luglio 2021, pone in capo al titolare del trattamento l'obbligo di garantire ed essere in grado di dimostrare che "il trattamento è effettuato conformemente al Regolamento" anche sotto il profilo della definizione dei ruoli svolti dai vari soggetti coinvolti in un'attività di trattamento di dati personali e la conseguente ripartizione delle responsabilità. In aggiunta, sotto il profilo dell'adozione delle misure di sicurezza tecniche e organizzative, seppur il RGPD pone in capo anche al responsabile del trattamento specifici obblighi in materia (art. 32 del RGPD – cfr. *infra*), resta fermo che il titolare è il soggetto sul quale ricade una "responsabilità generale" sui trattamenti effettuati (art. 5, par. 2 cd. *accountability* e art. 24 del RGPD) anche quando questi siano effettuati da altri soggetti "per suo conto" (cons. 81, artt. 4, punto 8) e 28 del RGPD. Per tali ragioni l'Autorità ha sanzionato il comune, titolare del trattamento, per la violazione degli artt. 5, par. 2, 24 e 28 del RGPD. Il gestore del servizio locale di raccolta e smaltimento rifiuti è stato, invece, sanzionato per la diffusione illecita di dati personali relativi alla salute, in quanto trattamento ultroneo rispetto a quelli inerenti alla gestione del servizio locale e privo di idonea base giuridica. In aggiunta, essendo stata la predetta diffusione cagionata anche dalla mancata adozione, da parte del responsabile del trattamento, di misure tecniche e organizzative idonee a garantire un'adeguata sicurezza dei dati personali, l'Autorità ha ribadito che taluni obblighi previsti dalla normativa in materia di protezione dei dati personali gravano anche sul responsabile del trattamento. Al riguardo, infatti, ai sensi dell'art. 32 del RGPD anche il responsabile del trattamento deve, in ragione dell'esperienza e delle competenze nello specifico settore in cui opera, adottare misure tecniche ed organizzative adeguate. Pertanto, l'Autorità ha sanzionato il gestore del servizio, per violazione degli artt. 5, par. 1, lett. a) e f), 9 e 32 del RGPD, e dell'art. 2-*septies*, par. 8 del Codice, nel testo vigente all'epoca dei fatti (provv.ti 22 febbraio 2024, n. 103, doc. web n. 9999973 e n.104, doc. web n. 10006915).

4.6.2. Diffusione di dati personali sui social network

L'Autorità ha sanzionato un comune per avere pubblicato, su una propria pagina Facebook, un *post* corredato da una mappa dalla quale si evincevano, con una certa chiarezza, le abitazioni delle persone affette da coronavirus e in quarantena, contrassegnati da pallini rossi o gialli, nonché ulteriori *post* in cui erano stati pubblicati – sebbene oscurando, in modo non completo o adeguato – i dati identificativi degli interessati e i dati relativi alla salute, contenuti nei referti dei tamponi di un numero ridotto di interessati. Nell'ambito dell'istruttoria, era altresì emerso che il predetto comune non aveva comunicato all'Autorità i dati di contatto del RPD né aveva dato riscontro all'invito formulato dal Garante a fornire ogni informazione utile in merito. Per tali ragioni l'Autorità, nel rammentare, che neanche la normativa d'urgenza adottata in

relazione all'epidemia da COVID-19 aveva derogato il divieto di diffusione dei dati relativi alla salute, ha sanzionato il comune per violazione degli artt. 5, par. 1, lett. a), 6, par. 1 lett. c) ed e), 9 e 37, par. 7 del RGPD, e degli artt. 2-*ter*, 2-*sexies*, 2-*septies*, par. 8 e 157 del Codice (nel testo vigente all'epoca dei fatti) ingiungendo, altresì, al suddetto comune, ai sensi dell'art. 58, par. 2, lett. d) del RGPD, di cessare l'ulteriore diffusione dei *post* in parola e di fornire all'Autorità un riscontro adeguatamente documentato in ordine alle iniziative intraprese al fine di dare attuazione a quanto ordinato, nonché alle eventuali misure poste in essere per assicurare la conformità del trattamento alla normativa in materia di protezione dei dati personali (provv. 24 gennaio 2024, n. 34, doc. web n. 9986304; v. anche par. 4.7). A seguito dell'adozione del predetto provvedimento, il comune non ha fornito alcun riscontro all'Autorità entro i termini indicati; l'Autorità ha inoltre accertato che i *post* oggetto di contestazione risultavano ancora pubblicati sulla medesima pagina Facebook. Pertanto, il Garante ha adottato un ulteriore provvedimento correttivo e sanzionatorio, sanzionando il comune per la violazione degli artt. 58, par. 2, lett. d), RGPD e 157 del Codice, per aver omesso di ottemperare, entro il termine indicato, alle prescrizioni impartitegli dall'Autorità e per aver omesso di fornire alla stessa un riscontro adeguatamente documentato in merito alle iniziative intraprese al fine di dare attuazione a quanto ordinatogli e ingiungendo nuovamente al comune di cessare l'ulteriore diffusione dei dati personali pubblicati e di comunicare all'Autorità le misure adottate (provv. 20 giugno 2024, n. 377, doc. web n. 10105123).

In un altro caso, l'Autorità ha provveduto ad ammonire un comune all'esito di un'istruttoria, originata da un reclamo concernente la comunicazione di dati personali dell'interessato, a mezzo stampa e durante un convegno pubblico, da parte del Sindaco del comune. In particolare, l'Autorità ha rilevato l'assenza di una base giuridica per la predetta comunicazione e la violazione dei principi di "liceità, correttezza e trasparenza" nonché di "minimizzazione" di cui all'art. 5, par. 1, lett. a) e c), RGPD. Considerate le circostanze del caso concreto, in particolare il fatto che la comunicazione in esame era avvenuta in un contesto di contestazione dell'operato dell'ente locale e, dunque, era stata funzionale a difendere le scelte dell'amministrazione comunale, l'Autorità ha ritenuto sufficiente adottare un provvedimento di ammonimento nei confronti del comune, per violazione degli artt. 5, par. 1, lett. a) e c) e 6 del RGPD (provv. 20 giugno 2024, n. 376, doc. web n. 10039570).

L'Autorità ha, inoltre, ammonito un comune per avere diffuso alcuni dati personali di un interessato (nome, cognome e indirizzo PEC) mediante la pubblicazione sulla propria pagina Facebook di un *post*, contenente la risposta del Sindaco a una segnalazione dell'interessato già inviata all'indirizzo PEC di quest'ultimo. Sul punto, l'Autorità ha rilevato l'assenza di una base giuridica per la predetta diffusione *online* e ha colto, altresì, l'occasione per ricordare le specifiche indicazioni – tuttora valide – fornite dall'Autorità alle amministrazioni sulle cautele da adottare per la diffusione di dati personali *online* con il provvedimento generale 15 maggio 2014, n. 243, recante 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» doc. web n. 3134436. Nell'ambito della medesima istruttoria era emerso, altresì, che il comune non aveva fornito un idoneo riscontro all'interessato a seguito dell'esercizio dei diritti di cui agli artt. da 15 a 22 del RGPD. A seguito di espressa richiesta del Garante di fornire riscontro alle richieste formulate dall'interessato, il comune ha dato successivamente seguito a tale istanza comunicando all'interessato, in particolare, la rimozione del *post*. In considerazione delle circostanze del caso concreto, l'Autorità ha ritenuto sufficiente adottare un provvedimento

di ammonimento per violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) ed e), parr. 2 e 3, lett. b), 12, par. 3 e 17 del RGPD e dell'art. 2-*ter*, commi 1 e 3, del Codice (provv. 19 dicembre 2024, n. 800, doc. web n. 10104692).

4.6.3. Servizi ai cittadini

All'esito di una complessa istruttoria l'Autorità ha adottato un provvedimento sanzionatorio nei confronti di un comune. In particolare, l'istruttoria era stata avviata a seguito di notizie stampa concernenti la presenza, presso un cimitero comunale, di una sezione dedicata alla sepoltura di feti (inclusi prodotti abortivi o prodotti del concepimento), con l'indicazione, nella maggior parte dei casi, del medesimo nome, seguito da cognomi delle donne che avevano interrotto la gravidanza. Il Garante ha evidenziato che la normativa di riferimento è il d.P.R. 285/1990, a cui, nel caso di specie, si aggiunge la normativa regionale di riferimento, che disciplina tre casistiche distinte: i "nati morti", per i quali la sepoltura è sempre prevista; i "prodotti abortivi", che si collocano tra le 20 e 28 settimane, oppure oltre le 28 settimane di gestazione – purché non dichiarati "nati morti" – per i quali la sepoltura è prevista su richiesta dei "parenti o chi per essi", da presentare alla ASL entro 24 ore, oppure, trascorso il predetto termine, su richiesta della struttura sanitaria (art. 7, comma 2); i "prodotti del concepimento", di età inferiore alle 20 settimane, che possono essere sepolti solo su richiesta dei "genitori", in assenza della quale, sono considerati rifiuti speciali ospedalieri e destinati alla termodistruzione (art. 7, comma 3). Nel secondo e nel terzo caso, l'autorizzazione al trasporto e al seppellimento è rilasciata dalla Asl. Nello specifico, oggetto dell'istruttoria svolta dall'Autorità è stata la diffusione dei dati riportati sulle sepolture e rinvenibili, altresì, sul portale *online* dei servizi cimiteriali del comune, relativi ai prodotti abortivi o del concepimento per i quali i parenti non avevano richiesto la sepoltura né indicato i dati da riportare sul cippo, lapide o altro supporto.

In tali casi, il Garante ha evidenziato che l'indicazione del cognome della donna o del marito o del compagno, accanto al prenome convenzionalmente attribuito al feto, unitamente alla data dell'interruzione di gravidanza (riportato come data di nascita e morte coincidente), poteva consentire, mediante raffronto, incrocio con altre fonti, o informazioni di contesto in possesso di terzi, l'identificazione della donna che aveva effettuato l'interruzione di gravidanza. Rileva a tale fine il fatto che, per stabilire l'identificabilità di una persona è opportuno considerare "tutti i mezzi" di cui, non solo il titolare del trattamento, ma anche soggetti terzi, possono ragionevolmente avvalersi per identificare detta persona fisica; per accertare la ragionevole probabilità di utilizzo di tali mezzi occorre considerare l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione (cfr. anche cons. 26, 84, 89, 93 e 95 del RGPD). L'Autorità ha pertanto rilevato l'illiceità del trattamento *de quo* effettuato in assenza di una base normativa e in violazione del divieto di diffusione dei dati sulla salute (artt. 5, 6 e 9 del RGPD e degli artt. 2-*ter*, 2-*sexies* e 2-*septies*, comma 8, del Codice (nel testo vigente all'epoca dei fatti).

Il Garante ha ribadito infatti che l'informazione relativa all'interruzione di gravidanza rientra a pieno titolo tra i dati relativi alla salute (artt. 4, par. 1, n. 15, e 9, nonché considerando 35 del RGPD), trattandosi comunque di un evento connesso ad una "prestazione di servizi di assistenza sanitaria" (art. 4, par. 1, n. 15, RGPD, nonché tra i vari, provv.ti 27 aprile 2023, n. 163, doc. web n. 9900808; n. 164, doc. web n. 9900826 e n.165, doc. web n. 9900503). Nel corso della medesima istruttoria l'Autorità ha evidenziato, altresì, in particolare che l'attribuzione di un nome e un cognome è contemplata unicamente nel caso dei "nati morti" per i quali è prevista la formazione dell'atto di nascita (artt. 29 e ss. del d.P.R. n. 396/2000) e l'autorizzazione

alla sepoltura è rilasciata dall'ufficiale dello stato civile, con rinvio alle disposizioni relative, in generale, ai "defunti" (artt. 7, comma 1, e 6 del d.P.R. n. 285/2000). Per i prodotti abortivi e del concepimento non è prevista registrazione nei registri di stato civile, l'autorizzazione alla sepoltura è rilasciata dall'azienda sanitaria competente e le norme che disciplinano tale autorizzazione non prevedono l'indicazione di un nome e di un cognome (art. 7, commi 2, 3 e 4 del citato d.P.R. n. 285/2000). Né il comune può ritenersi esonerato dalla necessità di effettuare una propria valutazione in ordine alle modalità di trattamento dei dati che riceve dalle aziende e dalle strutture sanitarie, al fine della sepoltura dei feti, rientrando le attività dei servizi cimiteriali tra i compiti di interesse pubblico specificamente ad esso attribuiti dalla legge e rivestendo pertanto il ruolo di titolare in relazione ai trattamenti di dati personali connessi allo svolgimento di tali compiti. Di conseguenza, in applicazione del principio di responsabilizzazione (artt. 5, par. 2, e 24 del RGPD), allorché il comune riceva dall'azienda sanitaria la relativa documentazione, è tenuto a trattare i dati nel rispetto dei principi applicabili al trattamento dei dati personali previsti dal RGPD, e in particolare a quelli di "liceità, correttezza e trasparenza", "limitazione delle finalità", "minimizzazione dei dati" ed "esattezza" (art. 5, par. 1, lett. a), b), c) e d), RGPD). Per tali ragioni, l'Autorità ha provveduto a sanzionare il comune per violazione degli artt. 5, par. 1, lett. a), b), c) e d), 6 e 9, RGPD nonché degli artt. 2-*ter*, 2-*sexies* e 2-*septies*, comma 8 del Codice, come vigenti all'epoca dei fatti ordinando altresì al comune, ai sensi degli artt. 58, par. 1, lett. a), RGPD e 157 del Codice, di confermare che, a seguito delle misure adottate sul proprio portale dei servizi cimiteriali *online* fossero consultabili unicamente le ubicazioni di nati morti, nonché dei prodotti abortivi o del concepimento per cui risultasse agli atti del comune la richiesta espressa di sepoltura in forma singola e del nome da parte dei parenti (provv. 19 dicembre 2024, n. 799, doc. web n. 10104750).

4.6.4. Utilizzo da parte di enti locali di applicazioni informatiche e altri strumenti tecnologici

A seguito di un'istruttoria, avviata sulla base di notizie di stampa, l'Autorità ha adottato un provvedimento sanzionatorio nei confronti di un comune che aveva messo a disposizione dei cittadini un'applicazione informatica per presentare generiche segnalazioni in merito a reati, non attribuiti a specifici soggetti considerati quali presunti autori, al fine di consentire alla Polizia locale di avere contezza, su base aggregata, delle zone della città maggiormente interessate da fenomeni criminali e organizzare servizi mirati di prevenzione dei reati. Il Garante ha ravvisato l'illiceità di tali trattamenti di dati, sul presupposto che le polizie locali non hanno una competenza generale in materia di pubblica sicurezza. Il comune, anche in ragione dell'errata impostazione del rapporto con l'azienda fornitrice di tale applicazione ai fini dell'attribuzione dei ruoli previsti dal RGPD, non aveva, inoltre, assicurato la necessaria trasparenza nei confronti degli interessati e, più in generale, non aveva individuato le necessarie misure volte ad attuare i principi di protezione dei dati e soddisfare i requisiti previsti dal RGPD, agendo, così, in maniera non conforme ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, nonché di responsabilizzazione, in violazione degli artt. 5, par. 1, lett. a) e par. 2 (in combinato disposto con l'art. 24), 6, 13, 25 e 28 del RGPD, nonché 2-*ter* del Codice. L'azienda fornitrice, in veste di responsabile del trattamento, è stata, invece, a sua volta sanzionata per non aver regolato correttamente i rapporti con il titolare del trattamento (provv.ti 4 luglio 2024, n. 405, doc. web n. 10050298 e n. 406, doc. web n. 10050707; v. anche provv.ti 20 giugno 2024, n. 374, doc. web n. 10028498 e n. 375, doc. web n. 10029393, cfr. par. 4.11).

4.6.5. Trattamenti effettuati dal difensore civico

Si segnala, infine, il parere reso dal Garante alla Regione Valle d'Aosta sullo schema di regolamento per la disciplina dei criteri e delle modalità del trattamento dei dati personali di cui alla l.r. 28 agosto 2001, n. 17 (disciplina del funzionamento dell'ufficio del difensore civico. Abrogazione della l.r. 2 marzo 1992, n. 5 - istituzione del difensore civico) (provv. 21 marzo 2024, n. 175, doc. web n. 10010558). Con tale provvedimento sono state fornite indicazioni utili anche per altri trattamenti effettuati da difensori civici di altre regioni. In particolare, si segnalano le considerazioni effettuate per escludere, nel caso in esame, la contitolarità del trattamento fra difensore civico e consiglio regionale. A tali conclusioni si è pervenuti alla luce delle circostanze concrete relative al rapporto tra le parti secondo un'analisi sostanziale (e non meramente formale), che tiene conto, fra l'altro, dell'influenza effettivamente esercitata sulle finalità e sui mezzi del trattamento e, in particolare, della specifica disciplina regionale che, da un lato, mantiene distinte competenze e funzioni del Consiglio regionale e del difensore regionale e, dall'altro, attribuisce autonome funzioni al difensore regionale. Tali competenze e funzioni sono inoltre esercitate dal difensore civico – secondo quanto previsto dalla legge regionale – in piena libertà e indipendenza, senza sottoposizione ad alcuna forma di controllo gerarchico e funzionale da parte del Consiglio regionale che non può dunque influire sul trattamento dei dati personali.

4.7. *Il RPD in ambito pubblico*

Nel corso del 2024 l'Autorità ha adottato alcuni provvedimenti sanzionatori nei confronti di province e comuni, nell'ambito dell'indagine, avviata nel 2023, volta a verificare il rispetto dell'obbligo di comunicazione dei dati di contatto del RPD di cui all'art. 37, par. 7, RGPD (provv.ti 11 gennaio 2024, n. 6, doc. web n. 9979112; n. 7, doc. web n. 9979128; n. 8, doc. web n. 9979152; n. 9, doc. web n. 9979171; provv.ti 14 novembre 2024, n. 697, doc. web n. 10085757; n. 698, doc. web n. 10085732).

Nell'ambito del medesimo filone istruttorio, il Garante ha altresì sanzionato un ente in quanto, oltre a non aver effettuato né la pubblicazione né la comunicazione al Garante dei dati di contatto del RPD, aveva comunque designato lo stesso RPD solo dopo oltre tre anni e mezzo dall'entrata in vigore del RGPD, in violazione, dunque dell'art. 37, parr. 1 e 7, RGPD medesimo; inoltre, a mezzo dello stesso provvedimento l'Autorità ha rilevato la violazione dell'art. 38, parr. 2 e 6, RGPD, avendo accertato che l'incarico di RPD era stato affidato a un soggetto già titolare di altri incarichi di responsabile di più servizi di un'amministrazione, comportando così l'impossibilità che il soggetto in questione potesse adempiere ai compiti propri del RPD in maniera piena, effettiva e completamente autonoma, a causa dell'assenza delle risorse necessarie, soprattutto in termini di tempo, e all'esercizio di funzioni che avevano dato, o comunque avrebbero potuto dare adito, a un conflitto di interessi (provv. 11 aprile 2024, n. 199, doc. web n. 10013391).

In merito ad analoghi profili il Garante ha adottato un provvedimento sanzionatorio nei confronti di un ordine professionale per non avere il medesimo adeguatamente comunicato all'Autorità e per avere omesso di pubblicare sul proprio sito web istituzionale i dati di contatto del RPD in violazione dell'art. 37, par. 7, RGPD. Il Garante ha, altresì, accertato la violazione dell'art. 38, par. 6, RGPD, per avere nominato RPD un membro del consiglio direttivo presente alla deliberazione di tale nomina ed in assenza di adeguate misure volte a prevenire i rischi di conflitti d'interessi. Da ultimo, è stato sottolineato che l'ordine professionale è soggetto all'obbligo di designazione del RPD

ai sensi dell'art. 37, par. 1, lett. a), RGPD e che, in ogni caso, anche nel caso di nomina su base volontaria, trovano applicazione i requisiti di cui agli artt. 37-39 per quanto concerne la nomina stessa, lo *status* e i compiti del RPD esattamente come nel caso di una nomina obbligatoria (provv. 22 febbraio 2024, n. 102, doc. web n. 10006478).

Profili inerenti al ritardo nella designazione del RPD da parte di un soggetto pubblico (rispetto alla data del 25 maggio 2018 in cui è entrato in vigore il RGPD) e all'omessa pubblicazione e comunicazione all'Autorità dei dati di contatto del RPD, sono stati trattati anche in altri provvedimenti (v. provv.ti 24 gennaio 2024, n. 34, doc. web n. 9986304; 8 febbraio 2024, n. 61, doc. web n. 9994597; 23 maggio 2024, n. 301, doc. web n. 10030785; 12 dicembre 2024, n. 768, doc. web n. 10102355) (cfr. parr. 4.6.2, 4.8, 13.13).

4.8. *Ordini professionali*

A seguito di un reclamo, il Garante ha censurato la condotta di un ordine degli architetti, pianificatori, paesaggisti e conservatori, che, dopo aver ricevuto una segnalazione in merito al presunto utilizzo improprio del titolo di architetto da parte di una professionista iscritta all'albo come pianificatrice, aveva inviato una nota di riscontro indirizzata non solo al soggetto segnalante e al proprio consiglio di disciplina ma anche alla professionista segnalata, rendendo così noti a quest'ultima il nome, il cognome e gli indirizzi di posta elettronica del soggetto segnalante e, pertanto, anche la circostanza che lo stesso avesse presentato detta segnalazione all'ordine. È stato, inoltre, accertato che l'ordine aveva pubblicato sul proprio sito web istituzionale un verbale di riunione del proprio consiglio, in cui, nel dar conto della medesima segnalazione, venivano riportati in chiaro i dati personali relativi sia alla professionista segnalata (titolo; nome e cognome; vicenda segnalata) sia a un consigliere comunale – omonimo del soggetto segnalante ed erroneamente identificato con quest'ultimo – che era in realtà del tutto estraneo alla vicenda. Ravvisata l'illiceità dei trattamenti in questione il Garante ha adottato un provvedimento sanzionatorio nei confronti dell'ordine per violazione degli artt. 5, par. 1, lett. a) e d), e 6, RGPD, nonché 2-*ter* del Codice (provv. 23 maggio 2024, n. 301, doc. web n. 10030785).

Il Garante ha poi adottato quattro provvedimenti sanzionatori nei confronti di altrettanti ordini delle professioni infermieristiche, in relazione a vicende tra loro connesse e oggetto di un medesimo reclamo. Dall'istruttoria era emerso che tali ordini avevano condiviso tra loro informazioni relative a istanze di accesso civico e segnalazioni presentate dal reclamante e dalla moglie di questi. Inoltre, i medesimi ordini professionali, agendo in qualità di contitolari del trattamento, ancorché senza aver previamente stipulato l'accordo richiesto dall'art. 26 del RGPD, avevano inviato una nota congiunta all'Arma dei carabinieri, datore di lavoro del reclamante, in merito all'opportunità di tali istanze e segnalazioni e alla complessiva condotta del reclamante. Uno degli ordini coinvolti aveva, inoltre, informato di tali vicende anche la Federazione nazionale degli ordini delle professioni infermieristiche, comunicando alla stessa i dati personali del reclamante e della coniuge. Un altro ordine, aveva, invece, acquisito informazioni relative alla professione svolta dal reclamante interrogando un motore di ricerca e consultando documenti pubblicamente disponibili su internet, così ponendo in essere trattamenti di dati non necessari ai fini dei procedimenti amministrativi di propria competenza. L'Autorità ha ravvisato l'assenza dei necessari presupposti di liceità di tali trattamenti di dati personali e la mancanza di trasparenza nei confronti degli interessati, ed ha censurato il mancato o inadeguato riscontro ad istanze di esercizio dei diritti

presentate dal medesimo reclamante (provv.ti 12 settembre 2024, n. 544, doc. web n. 10064226; n. 545, doc. web n. 10064103; n. 546, doc. web n. 10064766 e n. 547, doc. web n. 10065732).

In un altro caso, una federazione nazionale di ordini di professioni sanitarie è stata destinataria di un provvedimento di ammonimento, per aver informato l'autore di un esposto a carico di un presidente di un ordine territoriale dell'avvio dell'azione disciplinare e dell'esito della stessa in maniera non conforme e in violazione degli artt. 5, par. 1, lett. a) e 6 del RGPD, nonché 2-*ter* del Codice (provv. 13 novembre 2024, n. 665, doc. web n. 10084436).

4.9. *Amministrazione digitale*

4.9.1. Attività consultiva in materia di digitalizzazione della pubblica amministrazione

Affinché la digitalizzazione delle procedure amministrative nei rapporti tra cittadino e p.a. avvenga nel pieno rispetto dei diritti e delle libertà degli individui, anche nel 2024 il Garante ha proseguito la propria attività consultiva sugli atti volti a digitalizzare i servizi pubblici.

Gli interventi sono stati volti ad assicurare che i sistemi informatici siano progettati e realizzati nel rispetto dei più rigorosi standard in materia di protezione dei dati personali, garantendo la riservatezza, l'integrità e l'esattezza dei dati, con misure tecniche e organizzative adeguate, ed evitando l'ingiustificata duplicazione di servizi e informazioni.

Regolamento *cloud*

L'Autorità ha esaminato lo schema di regolamento per le infrastrutture digitali e per i servizi *cloud* per la p.a. elaborato dall'Agenzia per la cybersicurezza ai sensi dell'art. 33-*septies*, comma 4, d.l. n. 179/2012, volto a sostituire il precedente regolamento del 2021 all'epoca adottato dall'AgID (su cui il Garante si era pronunciato con provv. 16 dicembre 2021, n. 449, doc. web n. 9740711).

Lo schema tiene conto delle indicazioni fornite dal Garante nel corso delle interlocuzioni informali intercorse nonché delle considerazioni formulate dall'Autorità nel dicembre 2021 sullo schema di regolamento all'epoca di competenza dell'AgID, con specifico riferimento ai ruoli assunti dai soggetti coinvolti nei trattamenti e alla necessità di adottare misure adeguate per assicurare la circolazione delle informazioni in caso di violazione dei dati personali, il controllo da parte delle amministrazioni sulle attività svolte da tutti i responsabili e il rispetto delle garanzie in caso di trasferimento di dati personali al di fuori dello SEE. In particolare, è stata introdotta una disposizione (art. 22 dello schema) dedicata specificamente alla disciplina del trattamento dei dati personali e alla corretta applicazione della normativa in materia di protezione dei dati personali, la quale mira ad assicurare il controllo, da parte delle p.a., su tutti i soggetti che intervengono nel trattamento dei dati. Le p.a. vengono individuate titolari del trattamento, mentre gli operatori di infrastrutture digitali e i fornitori di servizi *cloud* vengono indicati quali responsabili del trattamento.

Il documento stabilisce, inoltre, l'obbligo per i responsabili del trattamento di adottare misure che garantiscano una tempestiva e adeguata informazione delle amministrazioni in caso di *data breach*, considerata la mole e la delicatezza dei dati trattati (dati sulla salute, dati fiscali). I responsabili del trattamento sono tenuti poi a fornire alle p.a. idonei strumenti di controllo sulle attività di trattamento effettuate da eventuali sub-responsabili. In tema di trasferimenti dei dati al di fuori dello SEE, i responsabili del trattamento sono tenuti ad attenersi alle istruzioni delle amministrazioni e a mettere a disposizione delle stesse ogni informazione necessaria per valutare

l'effettività delle misure adottate. Su tali basi, il Garante ha espresso parere favorevole (provv. 9 maggio 2024, n. 289, doc. web n. 10021468).

Il Ministero della giustizia, con l'Agenzia delle entrate, l'INPS e UNIONCAMERE, aveva trasmesso all'Autorità, ai fini dell'acquisizione del relativo parere, gli schemi di convenzione necessari – in ossequio a quanto previsto dal codice della crisi d'impresa e dell'insolvenza (art. 367 del d.lgs. n. 14/2019) – per la definizione delle modalità di accesso, da parte degli uffici giudiziari, alle banche dati contenenti le informazioni utili per la gestione della crisi d'impresa e dell'insolvenza. In particolare, l'art. 367 del codice, dal primo al quarto comma, prevede che durante il procedimento per l'apertura della liquidazione giudiziale o del concordato preventivo, l'ufficio del registro delle imprese, l'Agenzia delle entrate e l'INPS trasmettano alla cancelleria del tribunale concorsuale i bilanci, le dichiarazioni dei redditi, gli elenchi di atti stipulati, i debiti fiscali e previdenziali, nonché ogni altro elemento utile a ricostruire integralmente la situazione patrimoniale dell'impresa in stato di crisi o di insolvenza. Il comma 5 del medesimo articolo dispone che, in assenza di sistemi informatici per la cooperazione applicativa di cui al CAD, i dati, i documenti e le informazioni sopra descritti siano acquisiti dalla cancelleria, previa stipulazione, senza nuovi o maggiori oneri per la finanza pubblica, di una convenzione a titolo gratuito tra il Ministero della giustizia e i suddetti Enti, finalizzata alla fruibilità informatica dei dati. Gli schemi di convenzione individuano misure volte ad assicurare il rispetto della disciplina in materia di protezione dei dati personali, con particolare riferimento alla trasparenza e alla garanzia dei diritti, alla sicurezza del trattamento e agli obblighi comunicativi reciproci in caso di rilevazione di violazione dei dati personali. Su tali basi, l'Autorità ha espresso parere favorevole sugli schemi di convenzione, alle seguenti condizioni: in merito ai flussi di dati personali effettuati via PEC, i messaggi siano conservati, unitamente ai relativi metadati e alle ricevute di accettazione e di consegna, con modalità adeguate a garantire integrità e riservatezza, nonché per un periodo massimo proporzionato rispetto alle finalità per le quali tali dati personali debbano essere trattati; con specifico riferimento allo schema di convenzione tra Ministero della giustizia e Agenzia delle entrate, l'accesso alle informazioni sia effettuato da responsabili del trattamento e da persone autorizzate specificamente designate e destinatarie di apposite istruzioni; in merito allo schema di convenzione tra Ministero della giustizia e INPS, gli allegati al messaggio PEC inviato dall'INPS siano sottoposti a cifratura (provv. 22 febbraio 2024, n. 19, doc. web n. 9995114).

Accesso ai dati a fini di gestione delle crisi d'impresa

L'Autorità ha esaminato lo schema di regolamento dell'IVASS istitutivo del registro delle imprese e dei gruppi assicurativi (RIGA), attraverso cui disciplinare gli adempimenti che le compagnie assicurative devono seguire per la segnalazione di informazioni anagrafiche e sulle partecipazioni, gli azionisti, i componenti degli organi sociali e i soggetti che ricoprono funzioni di controllo. Lo schema riconosce in capo all'IVASS la titolarità del trattamento e stabilisce le finalità perseguite dal RIGA, tra cui quelle di costituire una base dati integrata, per consentire l'espletamento delle funzioni di vigilanza, di tutela del consumatore e di contrasto alle frodi assicurative e assicurare un più stretto collegamento tra la vigilanza assicurativa e quella bancaria. L'alimentazione del RIGA avviene per il tramite delle informazioni che l'IVASS recupera dall'Anagrafe dei soggetti (AS), il registro della Banca d'Italia che raccoglie, tramite il cd. codice censito, le anagrafiche delle segnalazioni effettuate dalle imprese vigilate, assicurando così la qualità dei dati oggetto di trattamento. Lo schema di regolamento tiene conto delle osservazioni fornite dall'Autorità nel corso delle interlocuzioni informali intercorse, che hanno riguardato, in particolare, l'esatta attribuzione dei ruoli in capo a IVASS e Banca d'Italia, l'individuazione dei dati personali oggetto di trattamento, le misure

RIGA

tecniche e organizzative necessarie per assicurare il rispetto del principio di integrità e riservatezza e gli obblighi di sicurezza. Per questa ragione, il Garante, preso atto che i tempi di conservazione risultano proporzionati al tempo strettamente necessario per il perseguimento degli scopi istituzionali di vigilanza e statistici sulla base di quanto disciplinato dalla normativa italiana ed europea vigente, ma saranno più dettagliatamente individuati all'esito dell'adozione delle linee guida per le autorità del settore finanziario per lo scambio di informazioni, allo stato in discussione in sede europea, ha ritenuto di poter esprimere parere favorevole sullo schema di regolamento (provv. 21 marzo 2024, n. 161, doc. web n. 10009328).

ANNCSU

L'Agenzia delle entrate e l'Istat hanno sottoposto al vaglio dell'Autorità l'aggiornamento del provvedimento istitutivo dell'Archivio nazionale dei numeri civici delle strade urbane adottato, ai sensi dell'art. 11 del d.P.C.M. 12 maggio 2016 recante censimento della popolazione e archivio nazionale dei numeri civici e delle strade urbane (ANNCSU), in attuazione dell'art. 3, commi 1 e 2, del d.l. n. 179/2012, e sul quale il Garante ha espresso il proprio parere con provv. 15 ottobre 2015, n. 536, doc. web n. 4481301. L'aggiornamento è finalizzato ad allineare l'Archivio con le previsioni contenute in materia di indirizzi nel reg. di esecuzione (UE) 2023/138 della Commissione del 21 dicembre 2022 che stabilisce un elenco di specifiche serie di dati di elevato valore e le relative modalità di pubblicazione e riutilizzo. Le informazioni contenute nell'ANNCSU non sono direttamente riferite a persone fisiche; tuttavia, le stesse possono essere collegabili alle persone fisiche che risultino – attraverso la mera consultazione di pubblici registri o la interconnessione prevista dal d.P.C.M. con altre banche dati di rilevanza nazionale e regionale – *exempli gratia*, intestatarie, proprietarie, residenti o comunque collegate ai luoghi individuati, così comportando un trattamento di dati personali. Pertanto, i servizi individuati nello schema, che consentono la consultazione da parte di altri soggetti, anche privati, delle informazioni contenute nell'Archivio, devono tenere conto delle conseguenze di siffatti trattamenti sui diritti e le libertà degli interessati (artt. 25, par. 1, e 35 del RGPD) e individuare le necessarie garanzie da assicurare al riguardo. Esaminato il testo, l'Autorità ha espresso parere favorevole (provv. 4 luglio 2024, n.402, doc. web n. 10039511).

Censimento dell'appartenenza a gruppi linguistici

L'Autorità ha rilasciato parere favorevole sullo schema di decreto del Presidente della Provincia di Bolzano, recante il reg. di esecuzione relativo alla dichiarazione individuale nominativa di appartenenza o aggregazione ad uno dei gruppi linguistici in forma telematica, ai sensi del riformulato art. 20-*ter*, comma 3, d.P.R. 26 luglio 1976, n. 752 (norme di attuazione dello statuto speciale della Regione Trentino Alto Adige in materia di proporzionale negli uffici statali siti nella Provincia di Bolzano e di conoscenza delle due lingue nel pubblico impiego).

Lo schema individua le modalità di presentazione, anche in via telematica, delle dichiarazioni individuali di appartenenza o aggregazione al gruppo linguistico, nonché quelle per la relativa certificazione, da effettuarsi con le medesime modalità, specificando i motivi di interesse pubblico rilevante e la necessaria adozione di misure volte ad assicurare, in relazione al trattamento posto in essere dal Ministero della giustizia-Tribunale di Bolzano, garanzie analoghe a quelle previste per quello che già avveniva in modalità cartacea.

La versione dello schema, modificata dalla Provincia al fine di rispettare i limiti e l'ambito di applicazione delle misure di digitalizzazione di cui al citato art. 20-*ter*, tiene conto anche delle indicazioni fornite nel corso di interlocuzioni informali intercorse con l'Autorità, volte ad assicurare la conformità al RGPD e al Codice, e relative, in particolare alla definizione dei tempi di conservazione delle dichiarazioni rese in via telematica in seguito al riversamento, al fine di evitarne l'annotazione o la registrazione

informatica, nel rispetto del principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e), RGPD, nonché alla necessaria individuazione di misure volte a garantire la limitazione della consultabilità del contenuto della certificazione resa in modalità telematica unicamente al momento della verifica dei requisiti per i benefici previsti da parte delle autorità competenti, in ossequio ai principi di liceità, limitazione della finalità, minimizzazione e *privacy by design* e *by default* di cui agli artt. 5, par. 1, lett. a), b), c) e 25 del RGPD. È stata, inoltre, prevista l'autorizzazione preliminare del Garante ai sensi dell'art. 36, par. 5, RGPD, sulla base della valutazione di impatto da sottoporre all'attenzione dell'Autorità (provv. 18 luglio 2024, n. 463, doc. web n. 10039488).

Il Ministero del lavoro e delle politiche sociali ha trasmesso all'Autorità, ai fini dell'acquisizione del relativo parere, lo schema di decreto direttoriale recante la disciplina relativa agli aspetti tecnico-organizzativi, ai differenti livelli di accesso ai dati contenuti nel Sistema informativo nazionale dei minori stranieri non accompagnati (SIM), alle tipologie di dati trattabili e alle operazioni eseguibili da parte dei soggetti legittimati all'accesso, nonché alle misure di sicurezza inerenti al SIM e alla comunicazione dei dati. Lo schema, attuativo dell'art. 12 del d.P.R. n. 231/2023 (su cui il Garante si è pronunciato con provv. 19 settembre 2019, n. 172, doc. web n. 9162562 e provv. 7 luglio 2022, n. 240, doc. web n. 9799592), tiene conto delle osservazioni fornite nel corso delle interlocuzioni informali intercorse con l'Autorità che hanno riguardato, in particolare: la definizione dei compiti spettanti al Ministero nonché delle relative basi giuridiche, per i quali vengono svolte le attività di censimento e monitoraggio della presenza dei minori stranieri non accompagnati sul territorio nazionale; l'individuazione dei soggetti legittimati ad accedere al SIM, in conformità a quanto stabilito dall'ordinamento (a partire dal d.P.R. n. 23/2023); le tipologie di dati personali messi a disposizione di ciascun soggetto legittimato ad accedere al SIM e le attività di trattamento consentite; l'individuazione dei ruoli degli utenti, operanti per conto dei soggetti legittimati ad accedere al SIM, nonché le procedure di accreditamento e autenticazione, al fine di mitigare i rischi connessi agli accessi abusivi. Il Garante ha ritenuto, su tali basi, di esprimere parere favorevole, evidenziando che gli ulteriori flussi di dati personali, a partire dal SIM, che potrebbero essere instaurati, per il miglior perseguimento dell'interesse del minore, nei confronti di altre amministrazioni pubbliche e organismi internazionali competenti in materia di minori stranieri non accompagnati, devono comunque essere preordinati al perseguimento di compiti di interesse pubblico disciplinati da apposite basi giuridiche, comprendere i soli dati personali a ciò necessari ed essere effettuati in conformità alle modalità e alle misure già individuate nello schema stesso (provv. 13 novembre 2024, n. 663, doc. web n. 10080723).

Accesso da parte di terzi al SII

A seguito dello svolgimento di apposita consultazione pubblica, l'ARERA ha sottoposto al Garante lo schema di deliberazione con cui, nel dare attuazione ad apposita regolazione di matrice europea, sono state introdotte forme di accessibilità, da parte di soggetti terzi, ai dati riferiti ai clienti finali contenuti nel Sistema informativo integrato (SII), attraverso il quale vengono gestiti i flussi informativi relativi ai mercati dell'energia elettrica e del gas. A questo proposito, la l. 30 dicembre 2023, n. 214, ha, da ultimo, stabilito che l'ARERA individuasse le modalità attraverso le quali, nel caso dell'energia elettrica e del gas naturale, su richiesta del cliente finale, l'Acquirente Unico S.p.A., in qualità di gestore del SII, per il tramite del Portale dei consumi, deve mettere a disposizione i dati del contatore di fornitura relativi all'immissione e al prelievo di energia elettrica e al prelievo del gas naturale "a disposizione del medesimo cliente finale o, su sua richiesta formale, a un soggetto terzo univocamente designato,

nel rispetto della normativa in materia di protezione dei dati personali, in un formato facilmente comprensibile che possa essere utilizzato per confrontare offerte comparabili ovvero per l'erogazione di servizi da parte dei predetti soggetti terzi" (art. 9, comma 3, lett. d), d.lgs. n. 102/2014).

In attuazione della predetta previsione normativa, lo schema disciplina l'accesso di terze parti autorizzate ai dati di misura di energia elettrica e gas naturale nonché il nuovo regolamento di funzionamento del Portale consumi, sostitutivo del precedente del 2019 (su cui il Garante si era pronunciato con provv. 20 giugno 2019, n. 131, doc. web n. 9123551). In particolare, viene previsto che il cliente finale possa mettere a disposizione delle terze parti i propri dati di misura esclusivamente per le sole finalità di confronto di offerte comparabili e di erogazione di servizi connessi all'energia, indicando quale delle due con riferimento a ciascuna richiesta di autorizzazione. Con riferimento alle modalità di autorizzazione, nello schema viene previsto che sia la terza parte (previa iscrizione nell'apposito elenco detenuto dal Gestore) a trasmettere una richiesta di conferma dell'autorizzazione al cliente finale (identificato tramite il codice fiscale), specificando le forniture (e il periodo temporale) per le quali tale conferma è richiesta; spetta poi al cliente confermare esplicitamente, nell'ambito della propria area privata del Portale, la volontà di concedere l'autorizzazione affinché il gestore possa fornire alla predetta terza parte i dati di misura, selezionando la profondità temporale dei dati storici. Alla luce dei rischi elevati connessi all'accessibilità da parte di una vasta platea di terze parti alle informazioni relative ai consumi energetici dei clienti finali, nello schema sono state recepite le indicazioni fornite dall'Autorità per individuare misure idonee affinché, in particolare, l'autorizzazione per la messa a disposizione dei dati personali venga conferita dal cliente finale esclusivamente per le sole finalità determinate, esplicite e legittime previste dalla normativa e il gestore possa verificare presso la terza parte la corrispondenza tra autorizzazione rilasciata e accordo preliminare che ne dovrebbe stare alla base, con la cancellazione dei dati acquisiti dal SII, una volta scaduta o revocata l'autorizzazione. Occorrerà, poi, che siano individuate e rese evidenti agli interessati le categorie di soggetti ai quali i dati potranno essere messi a disposizione in base alle finalità specificamente perseguite e alle tipologie di servizi offerti, limitando l'ambito di applicazione del procedimento alle sole finalità di confronto di offerte comparabili e di erogazione di servizi energetici ed evitando, allo stato, di consentire l'accesso a categorie di soggetti esterni al settore energetico. Inoltre, le tipologie di dati personali che potranno essere messi a disposizione delle terze parti devono essere effettivamente limitate a quelle necessarie al perseguimento delle finalità esplicitate, anche con riferimento alla profondità temporale delle informazioni relative ai consumi storici. Gli interessati devono avere poteri di controllo sugli accessi alle proprie informazioni e sulle autorizzazioni nei confronti delle terze parti, anche al fine di consentire loro di avere cognizione, gestire e revocare le medesime autorizzazioni, e lo stesso gestore deve essere dotato di strumenti di controllo, anche effettuando apposite verifiche periodiche e procedure di audit e monitoraggio al fine di prevenire possibili trattamenti non autorizzati. In conclusione, nel ricordare che il Gestore, nel definire le specifiche tecniche in qualità di titolare del trattamento, dovrà creare, per le terze parti finora non censite (cioè diverse da imprese di vendita di energia elettrica e/o di gas naturale), appositi profili coerenti con le specifiche finalità, modalità e limiti dei trattamenti consentiti a tali soggetti, assicurando adeguati meccanismi di attribuzione e gestione delle utenze che ne garantiscano costantemente l'attualità e ne monitorino l'operatività e gli accessi al fine di mitigare i rischi di accessi non autorizzati, il Garante ha espresso parere favorevole (provv. 14 novembre 2024, n. 695, doc. web n. 10085707).

4.9.2. Vigilanza sulle banche dati e violazioni di dati personali in ambito pubblico

Vigilanza sulle banche dati pubbliche

Come negli anni passati, il Garante ha proseguito la propria attività di vigilanza sulle banche dati pubbliche anche al fine di arginare il fenomeno degli accessi abusivi, oggetto nel tempo di numerosi provvedimenti volti ad innalzare le misure di sicurezza sia da un punto di vista tecnico che organizzativo, anche attraverso lo svolgimento di accertamenti ispettivi con specifico riguardo agli accessi all'Anagrafe tributaria e alle banche dati dell'INPS.

In particolare, a seguito di un reclamo, sono stati avviati accertamenti che hanno portato a segnalare all'Autorità giudiziaria ipotesi di numerosi accessi abusivi alle banche dati dell'Agenzia delle entrate e dell'INPS, mediante condotte penalmente rilevanti poste in essere da parte di più soggetti in concorso tra loro (cfr. parte IV, tab. 8).

Negli ultimi anni, sulla base delle segnalazioni ricevute, il Garante ha riscontrato un incremento del fenomeno collegato alla rivendita di informazioni riservate presenti nelle banche dati pubbliche da parte di società private che, anche avvalendosi di agenzie di investigazione privata, offrono informazioni a chiunque, anche attraverso opachi meccanismi di reperimento dei dati.

Soprattutto a seguito di noti eventi di cronaca, l'Autorità ha ritenuto necessario, quindi, creare una *task force* interdipartimentale per individuare le azioni da intraprendere al fine di offrire maggiori garanzie a protezione delle banche dati attraverso l'innalzamento delle misure di sicurezza tecniche e organizzative, in ordine agli accessi da parte del personale autorizzato e alle operazioni di gestione e manutenzione, anche deliberando lo svolgimento di accertamenti ispettivi per verificare i sistemi di sicurezza ed i profili di accessibilità delle banche dati interessate (comunicato stampa 28 ottobre 2024, doc. web n. 10067406, cfr. par. 19.1).

Violazioni di dati personali

L'Autorità, nell'anno di riferimento, ha adottato alcuni provvedimenti sanzionatori per violazioni rilevate in materia di protezione dei dati personali, in riferimento (e per effetto) di vari incidenti di sicurezza occorsi a taluni sistemi informatici di soggetti pubblici.

Data breach
Piattaforma NSIS

Il Garante, con provv. 7 marzo 2024, n. 134 (doc. web n. 10008177), ha definito il procedimento aperto nei confronti del Ministero della salute a seguito dell'attacco informatico finalizzato all'esfiltrazione di credenziali per l'accesso ai sistemi riferiti alla Piattaforma del NSIS. Il Ministero, in qualità di titolare del trattamento, è incorso in numerose e gravi violazioni della normativa *privacy,* in particolare, dei principi di integrità e riservatezza, di sicurezza del trattamento e della protezione dei dati per impostazione predefinita (artt. 5, par. 1, lett. f), 32 e 25, par. 1, 33 e 34 del RGPD). Nella gestione dei trattamenti di dati personali effettuati nell'ambito del NSIS, che costituisce lo strumento di riferimento per le misure di qualità, efficienza e appropriatezza del SSN, infatti, non sono state adottate idonee misure tecniche ed organizzative per assicurare un'adeguata sicurezza del trattamento, anche considerate le legittime aspettative degli interessati affinché i propri dati personali relativi allo stato di salute fossero conservati al riparo da incidenti di sicurezza. É stata accertata, nel corso dell'istruttoria, la violazione degli obblighi di sicurezza di cui all'art. 32 del RGPD, in particolare, in relazione all'inadeguatezza della configurazione e alla vulnerabilità dei sistemi di trattamento, nonché alla mancata adozione di misure adeguate a rilevare le violazioni dei dati personali, circostanza confermata dal fatto che il Ministero abbia avuto conoscenza della violazione solamente a seguito della segnalazione intervenuta (*i.e.* una comunicazione telematica da parte di un utente che aveva segnalato di aver individuato informazioni afferenti l'Amministrazione in un annuncio presente sul *darkweb*), senza che in alcun modo i sistemi fossero stati in grado autonomamente di rilevare l'incidente di sicurezza occorso. Inoltre, con il predetto provvedimento è stata

confermata la violazione dell'art. 33 RGPD, non avendo il Ministero provveduto a effettuare formale notifica del *data breach* (non ritenendosi idonea una comunicazione informale via *e-mail*), né avendo documentato l'episodio con le informazioni essenziali ai sensi del par. 5 della predetta disposizione.

È stato violato anche l'art. 34 RGPD, tenuto conto che il Ministero ha effettuato la comunicazione circa la violazione dei dati personali occorsa agli interessati coinvolti solo a seguito del provvedimento ingiuntivo del Garante 10 marzo 2022, n. 88, doc. web n. 9780717.

Ransomware
Regione Lazio

L'Autorità ha poi irrogato una sanzione pecuniaria alla Regione Lazio per le violazioni accertate a seguito di un attacco informatico al Sistema sanitario regionale avvenuto nella notte tra il 31 luglio e il 1° agosto del 2021.

Il *data breach* ai sistemi informativi gestiti da LAZIOcrea S.p.A, in qualità di responsabile del trattamento per conto della Regione stessa e di diversi enti del servizio sanitario regionale – causato da un *ransomware* introdotto nel sistema attraverso un portatile in uso a un dipendente della Regione – aveva determinato, nel corso dell'attacco informatico, l'impossibilità per le strutture sanitarie regionali di accedere al sistema ed erogare alcuni servizi sanitari ai loro assistiti. Dagli accertamenti e dalle ispezioni effettuate dall'Autorità è emerso che LAZIOcrea S.p.A. e Regione Lazio, pur con differenti ruoli e livelli di responsabilità, erano incorse in numerose e gravi violazioni della normativa in materia di protezione dei dati personali – in particolare, dei principi di integrità e riservatezza dei dati, di protezione dei dati fin dalla progettazione e di responsabilizzazione (artt. 5, par. 1, lett. f*)*, 25, par. 1, e 32 del RGPD) – dovute in prevalenza all'utilizzo di sistemi operativi obsoleti e alla mancata adozione di misure tecniche e organizzative adeguate a rilevare tempestivamente le violazioni di dati personali e a garantire la sicurezza delle reti informatiche (provv. 21 marzo 2024, n. 196, doc. web n. 10002287; per quanto concerne il provvedimento sanzionatorio adottato nei confronti di LAZIOcrea S.p.A., v. provv. 21 marzo 2024, n. 194, doc. web n. 10002324, cfr. par. 5.4.1).

Divulgazione dati CCIAA

Una camera di commercio, industria, artigianato e agricoltura ha notificato, ai sensi dell'art. 33 del RGPD, una violazione dei dati personali – in particolare di dati anagrafici (nome, cognome, codice fiscale), dati di contatto (indirizzo di posta elettronica, numero di telefono fisso o mobile), nonché dati di accesso e di identificazione (*username, password* crittografata in MD5) – determinata da un attacco informatico su una delle componenti utilizzate dall'ambiente applicativo CMS nell'ambito del servizio di gestione degli appuntamenti sul proprio portale istituzionale.

Il Garante, a seguito delle attività istruttorie, ha accertato che la violazione dei dati personali oggetto di notifica aveva riguardato dati personali che non si trovavano sul sito istituzionale, bensì in un *database* costituito da una copia di *backup* dell'applicativo che gestiva gli appuntamenti, la quale era stata realizzata dall'azienda speciale della CCIAA, in via straordinaria ed *una tantum,* nell'ambito di una serie di attività volte ad ottimizzare le risorse presenti nei *server* e che comprendevano anche lo spostamento del sistema degli appuntamenti su un *server* diverso. In particolare, è emerso come, al momento in cui si era verificata la violazione dei dati personali, le *password* degli utenti registrati al sistema di gestione degli appuntamenti erano memorizzate, all'interno di un *file* creato dall'azienda e contenuto sul *server* oggetto dell'attacco informatico, previo utilizzo di una funzione di *hashing* non robusta in termini crittografici, e dunque misura affatto efficace a questi fini. Peraltro, la copia di *backup* dei dati personali degli utenti registrati al servizio di gestione delle prenotazioni avrebbe dovuto essere cancellata al termine delle attività di migrazione dell'applicativo, o, comunque, entro un termine congruo alla necessità di garantire un eventuale ripristino dei dati in

caso di malfunzionamenti o incidenti di sicurezza. Le scelte effettuate nel caso di specie sono risultate imputabili all'azienda, nell'ambito delle attribuzioni riconosciute al responsabile del trattamento su aspetti di dettaglio concernenti le misure tecniche e organizzative, e, pertanto, il Garante ha ritenuto che il trattamento di dati personali svolto dall'azienda, con riferimento ai summenzionati profili, sia stato effettuato in violazione dei principi di limitazione della conservazione (art. 5, par. 1, lett. e), RGPD), di integrità e riservatezza (art. 5, par. 1, lett. f), RGPD), nonché in violazione degli obblighi di sicurezza (art. 32 del RGPD). Su tali basi, l'Autorità ha rilevato l'illiceità della condotta tenuta dall'azienda e ha comminato alla medesima una sanzione amministrativa pecuniaria per le violazioni anzidette (provv. 11 aprile 2024, n. 198, doc. web n. 10013321).

4.9.3. PEC e servizi fiduciari

L'Autorità ha concluso l'istruttoria a suo tempo avviata nei confronti di un gestore PEC e un suo responsabile, operante anche per conto di numerosi ordini professionali, rilevando l'illiceità dei trattamenti di dati personali posti in essere (provv.ti 9 maggio 2024, n. 292, doc. web n. 10070397 e n. 293, doc. web n. 10070917). I provvedimenti sono stati impugnati e, in pendenza del giudizio di opposizione contro il provvedimento, non è applicata la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione.

L'istruttoria era stata avviata a seguito di un attacco informatico compiuto in danno dei portali istituzionali di vari ordini degli avvocati e della successiva diffusione *online* di parte dei dati personali esfiltrati da tali portali, tra cui, in particolare, le credenziali di autenticazione per l'accesso a caselle PEC, nonché i messaggi contenuti in alcune di esse. In tale sede sono stati accuratamente verificati anche i trattamenti effettuati dal predetto gestore, più in generale, nell'erogazione del servizio PEC.

È stato rilevato, in primo luogo, come, in violazione dell'art. 28 del RGPD, i trattamenti effettuati da numerosi soggetti per conto del gestore non fossero stati disciplinati adeguatamente da un contratto o da altro atto giuridico stipulato in forma scritta e avente tutti i requisiti analiticamente individuati da tale disposizione. Sono emerse altresì la tardività e l'inadeguatezza della comunicazione della violazione dei dati personali agli interessati, in violazione dell'artt. 5, par. 1, lett. a), 12 e 34 del RGPD, nonché l'assenza della valutazione di impatto sulla protezione dei dati di cui all'art. 35 del RGPD. L'Autorità ha inoltre accertato la violazione dell'obbligo di documentare i *data breach* e l'incompletezza delle informazioni presenti nel registro delle attività di trattamento, in specie considerando come la tenuta adeguata di un registro, con le principali informazioni relative alle operazioni di trattamento svolte, costituisca un adempimento funzionale al rispetto del principio di responsabilizzazione del titolare.

Con specifico riferimento al principio di integrità e riservatezza (art. 5, par. 1, lett. f), RGPD) e agli obblighi in materia di sicurezza del trattamento (art. 32 del RGPD), l'Autorità ha rilevato poi l'inadeguatezza delle misure tecniche e organizzative adottate, anche atteso che i trattamenti effettuati avrebbero richiesto l'adozione dei più elevati *standard* di sicurezza in ogni singola fase di gestione al fine di non compromettere la sicurezza complessiva del servizio PEC. In particolare, le violazioni in tale ambito hanno riguardato il processo di attivazione di caselle PEC tramite intermediario, la *password policy* relativa alle credenziali di autenticazione utilizzate per l'accesso alle caselle PEC e la mancata obbligatorietà della modifica della *password* al primo utilizzo, la mancata adozione di idonee misure di sicurezza per il *reset* delle *password* ritenute a rischio di compromissione e per l'accesso al *log* certificato del servizio PEC, nonché l'inadeguatezza di alcuni *log* di tracciamento degli accessi e delle operazioni compiute dai soggetti autorizzati al trattamento.

Infine, il Garante ha evidenziato che il gestore, per la mancata adozione delle predette misure, non era stato in grado di garantire e dimostrare che il trattamento effettuato nell'ambito della gestione del servizio PEC fosse avvenuto in conformità ai principi di responsabilizzazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita di cui agli artt. 5, par. 2, 24 e 25 del RGPD.

Al contempo, in relazione al predetto incidente di sicurezza, il Garante ha ammonito l'altra società coinvolta nel *data breach*, per aver violato gli artt. 5, par. 1, lett. f), 32 e 33, par. 2, RGPD in conseguenza di varie condotte: in particolare, la società – sia in qualità di titolare del trattamento che di responsabile del trattamento per conto del predetto gestore del servizio PEC e di diversi ordini professionali – non aveva messo in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, in violazione del principio di integrità e riservatezza e degli obblighi in materia di sicurezza del trattamento. Sono emersi al riguardo diversi profili, quali, tra gli altri l'obsolescenza dei *software* di base installati sui sistemi di trattamento; la conservazione delle *password* degli utenti senza l'utilizzo di tecniche crittografiche; la mancata definizione di *password policy*; l'utilizzo di protocolli di rete non sicuri; il rilascio delle credenziali di autenticazione delle caselle PEC con una procedura di identificazione non idonea**.** L'Autorità ha, altresì, censurato la società per la tardiva e incompleta informazione ad alcuni ordini professionali, titolari del trattamento, della violazione occorsa, pur essendovi tenuta, in qualità di responsabile, ai sensi dell'art. 33, par. 2, RGPD, sì da consentire un rapido intervento.

SPID e altri servizi fiduciari

Il Garante ha proseguito gli accertamenti ispettivi al fine di verificare, in particolare, i trattamenti effettuati nell'ambito dello SPID e della fornitura di servizi fiduciari di cui al reg. (UE) 910/2014 (cd. reg. eIDAS) da parte delle società accreditate e degli altri soggetti di cui si avvalgono in tali contesti. In ragione dei *data breach* notificati dalle predette società e delle numerose segnalazioni pervenute da vittime di furti di identità perpetrati attraverso tali strumenti di identificazione digitale, l'Autorità ha inteso proseguire la propria attività di vigilanza sui trattamenti effettuati al fine di innalzare il livello delle misure di garanzia allo stato adottate.

4.10. *La materia anagrafica, elettorale e diritti civili*

In tale ambito l'Autorità si è espressa con parere favorevole sullo schema di decreto del Ministero degli affari esteri della cooperazione internazionale di recepimento nell'ordinamento italiano della dir. 2019/997 del Consiglio del 18 giugno 2019 che istituisce un documento di viaggio provvisorio dell'Unione europea (cd. ETD UE) e abroga la decisione 96/409/PESC. Il predetto documento viene rilasciato dall'ufficio consolare a un cittadino italiano o a un cittadino europeo, non rappresentato in un paese terzo, per un viaggio di rientro verso lo Stato membro di cittadinanza o di residenza, o eccezionalmente verso altra destinazione, nel caso in cui il passaporto o documento di viaggio sia stato smarrito, rubato o distrutto, o non possa essere altrimenti ottenuto entro un lasso di tempo ragionevole. L'Istituto Poligrafico e Zecca dello Stato è l'organismo designato dall'Italia per la realizzazione dei moduli e adesivi uniformi ETD UE. I dati personali raccolti ai fini del rilascio del documento di viaggio provvisorio, sono utilizzati al solo scopo di verificarne l'identità, stampare l'adesivo uniforme e agevolare il viaggio del richiedente, e sono conservati solo per il tempo necessario allo svolgimento di tali attività, per un massimo di due anni o di 180 giorni, a seconda che il ETD UE sia rilasciato a un cittadino italiano o a un cittadino di un altro Stato membro. L'Autorità, pur non rilevando nel testo proposto per il parere

specifici profili di criticità, ha ritenuto ciononostante necessario esplicitare il ruolo di titolare del trattamento rivestito dal Ministero degli affari esteri; inserire, con riguardo alle indicate modalità di verifica e rettifica dei dati riportati sul documento di viaggio, un richiamo più generale ai diritti degli interessati previsti dagli artt. 15-22 del RGPD e precisare che il livello di sicurezza assicurato al trattamento dei dati personali sia conforme a quanto previsto dal RGPD, dal Codice e dalle disposizioni della disciplina di settore (provv. 20 giugno 2024, n. 379, doc. web n. 10061488).

4.11. *Trattamenti di dati personali in ambito pubblico mediante dispositivi video*

Anche nel corso 2024, l'Autorità ha rivolto la propria attenzione all'impiego da parte di soggetti pubblici, specialmente comuni, di sistemi di videosorveglianza e altri dispositivi video, spesso in assenza dei necessari presupposti di liceità e con modalità non conformi ai requisiti previsti dalla normativa in materia di protezione dei dati.

Sulla base di una notizia di stampa, l'Autorità ha avviato un'istruttoria nei confronti di un comune in relazione a due progetti, finanziati con fondi europei, finalizzati allo sviluppo di soluzioni tecnologiche volte a migliorare la sicurezza in ambito urbano secondo il paradigma delle cd. città intelligenti (*smart city*). In particolare, uno di tali progetti aveva previsto l'acquisizione di filmati dalle telecamere di videosorveglianza già installate nel territorio comunale per finalità di sicurezza urbana, nonché dell'audio ottenuto da microfoni appositamente collocati sulla pubblica via. I dati, che ad avviso del comune sarebbero stati immediatamente anonimizzati dopo la raccolta, venivano analizzati per rilevare in maniera automatizzata, mediante tecniche d'intelligenza artificiale, eventi di rischio per la pubblica sicurezza. Il secondo progetto aveva riguardato, invece, oltre all'acquisizione dei filmati di videosorveglianza (senza audio), la raccolta e l'analisi di messaggi e commenti d'odio pubblicati sulle reti sociali, rilevando eventuali emozioni negative ed elaborando informazioni d'interesse per le Forze dell'ordine, allo scopo di identificare rischi e minacce per la sicurezza dei luoghi di culto. In sede istruttoria, il comune, che non aveva annoverato la ricerca scientifica tra le proprie finalità istituzionali, non aveva comprovato la sussistenza di alcuna disposizione idonea a giustificare i trattamenti dei dati personali. Tenuto conto che i dati venivano condivisi anche con soggetti terzi, tra cui i *partner* di progetto, i trattamenti effettuati sono stati quindi ritenuti illeciti. Si sono, inoltre, rivelate insufficienti le tecniche di anonimizzazione impiegate per ridurre i possibili rischi di reidentificazione degli interessati. Criticità sono emerse anche sotto il profilo della trasparenza, atteso che il comune non aveva compiutamente descritto i trattamenti nelle informative di primo e di secondo livello, come la possibilità che anche le conversazioni potessero essere registrate dai microfoni installati sulla pubblica via. Inoltre, nonostante i due progetti comportassero l'impiego di nuove tecnologie e la sorveglianza sistematica di zone accessibili al pubblico, il comune non aveva comprovato di aver effettuato una valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento. Pur riconoscendo la sussistenza di alcuni fattori attenuanti, il Garante ha stigmatizzato tali modalità di trattamento, che avevano comportato significativi rischi per i diritti e le libertà degli interessati, anche di rango costituzionale, evidenziando che simili forme di sorveglianza negli spazi pubblici possono modificare il comportamento delle persone e condizionare anche l'esercizio delle libertà democratiche (provv. 11 gennaio 2024, n. 5, doc. web n. 9977020; cfr. comunicato stampa 25 gennaio 2024, doc. web n. 9977299).

A seguito di un reclamo, l'Autorità si è poi occupata del caso di un comune che, con il supporto di un'azienda fornitrice in veste di responsabile del trattamento, aveva impiegato

4

dispositivi video installati in prossimità di tre stazioni ecologiche, al fine di prevenire e individuare atti di vandalismo o eventi rilevanti per la sicurezza degli impianti o per l'incolumità degli utenti. Il comune è stato destinatario di un provvedimento sanzionatorio per non aver assicurato la necessaria trasparenza nei confronti degli interessati, per non aver adottato tecniche di cifratura dei dati o altre tecniche comunque idonee a prevenire il rischio di accesso non autorizzato alle immagini registrate, atteso che le stesse erano state memorizzate in locale su un supporto di memoria astrattamente rimovibile da chiunque, nonché per non aver stipulato un accordo sulla protezione dei dati con l'azienda responsabile del trattamento, in violazione degli artt. 5, par. 1, lett. a) e f), 12, par. 1, 13, 28, parr. 3 e 9, e 32 del RGPD. Tenuto conto delle diverse circostanze attenuanti emerse nel corso dell'istruttoria, la predetta azienda è stata, invece, destinataria di un provvedimento di ammonimento, per la mancata definizione dei rapporti con il titolare del trattamento e per l'omessa adozione delle menzionate misure di sicurezza (provv.ti 22 febbraio 2024, n. 100, doc. web n. 9990659 e n. 101, doc. web n. 9990706).

Un diverso comune, avvalendosi di un'azienda fornitrice, aveva, invece, messo a disposizione dei cittadini un'applicazione informatica, che consentiva di inviare segnalazioni alla Polizia locale in merito a situazioni di degrado o che potevano destare allarme sociale, consentendo al personale della Polizia locale, addetto alla visione delle immagini di videosorveglianza provenienti dalle telecamere installate sul territorio comunale per finalità di tutela della sicurezza urbana, di monitorare la situazione nella specifica area interessata dalla segnalazione ed eventualmente inviare una pattuglia *in loco*. Dall'istruttoria era emerso che il comune aveva reso disponibile tale applicazione benché la stessa non fosse stata ancora testata e, successivamente – nonostante le criticità di protezione dei dati in più occasioni evidenziate dal proprio RPD e da un consulente esterno, anche in merito al complessivo sistema di videosorveglianza comunale – aveva continuato ad impiegare tale applicazione e le telecamere di videosorveglianza, agendo, pertanto, in maniera non conforme ai principi di responsabilizzazione e protezione dei dati fin dalla progettazione e per impostazione predefinita. L'ente non aveva, inoltre, assicurato la necessaria trasparenza nei confronti degli interessati, aveva omesso di stipulare un accordo sulla protezione dei dati con l'azienda fornitrice, che agiva quale responsabile del trattamento, non aveva redatto una valutazione d'impatto sulla protezione dei dati prima di dare avvio ai trattamenti in questione e non aveva adottato adeguate misure di sicurezza a protezione dei dati, essendo emerso che gli operatori della Polizia locale potevano accedere ai dati raccolti mediante la predetta applicazione utilizzando una *password* generica generata dall'azienda fornitrice e dunque senza disporre di specifiche e personali credenziali di autenticazione per accedere al sistema informatico. Mentre il comune è stato destinatario di un provvedimento sanzionatorio per aver violato gli artt. 5, par. 1, lett. a) e f), e par. 2 (in combinato disposto con l'art. 24), 12, par. 1, 13, 25, 28, par. 3, 32 e 35, par. 1, RGPD), l'azienda fornitrice, quale responsabile del trattamento, tenuto conto delle circostanze attenuanti emerse nel corso dell'istruttoria, è stata ammonita dall'Autorità per la mancata definizione dei rapporti con il titolare del trattamento e per l'omessa adozione delle predette misure di sicurezza (provv.ti 20 giugno 2024, n. 374, doc. web n. 10028498 e n. 375, doc. web n. 10029393).

In un altro caso, il Garante, all'esito di un'istruttoria avviata sulla base di notizie di stampa, ha accertato che un comune aveva installato sul proprio territorio cinque telecamere non omologate, di cui una dotata di una funzionalità avanzata in grado di ricavare informazioni in merito alla tipologia, marca, modello, colore e classificazione EURO dei veicoli, che consentivano la lettura automatizzata dei numeri di targa di tutti i veicoli in transito e la conservazione di tali dati, acquisiti su base continuativa, per un esteso arco temporale, pari a centottanta giorni, indipendentemente dall'accertamento di

eventuali violazioni del codice della strada, al dichiarato fine di poter corrispondere a specifiche richieste dell'Autorità giudiziaria o delle Forze dell'ordine, nonché per effettuare elaborazioni statistiche in merito allo Stato o alla provincia dei veicoli in transito. Tali operazioni avvenivano in assenza di un'idonea base giuridica che potesse giustificare il trattamento dei dati, senza garantire la necessaria trasparenza nei confronti degli interessati e senza aver comprovato di aver previamente redatto una valutazione d'impatto sulla protezione dei dati. L'Autorità ha, pertanto, comminato al comune una sanzione amministrativa pecuniaria, per aver agito in violazione degli artt. 5, 6, 12, par. 1, 13 e 35 del RGPD, nonché 2-*ter* del Codice (provv. 19 dicembre 2024, n. 805, doc. web n. 10107263).

Si segnala, altresì, il caso di un comune, che era stato destinatario di un provvedimento sanzionatorio in materia di videosorveglianza (cfr. provv. 20 ottobre 2022, n. 341, doc. web n. 9831369) e che è stato ulteriormente sanzionato per non aver informato l'Autorità, entro il termine impartitogli, in merito alle iniziative intraprese per adempiere a quanto gli era stato prescritto con riguardo alla necessità di fornire gratuitamente all'interessato copia delle immagini di videosorveglianza, contenenti propri dati personali, che lo stesso aveva chiesto di ottenere con specifica istanza di accesso ai sensi dell'art. 15 del RGPD (provv. 24 gennaio 2024, n. 33, doc. web n. 9986278).

L'Autorità ha adottato un provvedimento sanzionatorio nei confronti di un comune, a seguito di un'istruttoria avviata sulla base di una segnalazione presentata da diversi cittadini in merito all'assenza di idonea informativa ai sensi dell'art. 12 e seguenti del RGPD, nei pressi dei luoghi di installazione di "dispositivi di ripresa foto/video" ai fini dell'accertamento delle infrazioni al d.lgs. 30 aprile 1992, n. 285 (nuovo codice della strada). Nel corso dell'istruttoria il comune aveva rappresentato di aver provveduto, a seguito della richiesta d'informazioni inviata dall'Autorità, a fornire l'informativa di primo livello mediante affissione della relativa cartellonistica nei pressi dei dispositivi installati sul territorio comunale nonché di aver adottato un'informativa estesa, pubblicata sul sito web istituzionale. Il comune aveva dichiarato, altresì, di aver provveduto a redigere la valutazione di impatto ai sensi dell'art. 35 del RGPD, seppur in un momento successivo all'avvio dell'istruttoria da parte del Garante. Al riguardo, tenuto conto che, nel corso dell'istruttoria, il comune aveva dichiarato di utilizzare dispositivi idonei a effettuare foto e riprese video al fine di documentare le infrazioni, l'Autorità ha ritenuto che l'ente fosse soggetto all'obbligo di redigere una valutazione d'impatto sulla protezione dei dati, che è sempre richiesta in caso di "sorveglianza sistematica su larga scala di una zona accessibile al pubblico". Per tali ragioni l'Autorità ha sanzionato il comune, titolare del trattamento, per violazione degli artt. 5, par. 1, lett. a), 12, 13 e 35 del RGPD (provv. 12 dicembre 2024, n. 766, doc. web n. 10102334).

5 La sanità

5.1. *La sanità digitale*

Nel processo di digitalizzazione dei sistemi e dei servizi sanitari sono stati molti gli interventi dell'Autorità volti a garantire, con un approccio di *privacy by design*, la previsione di misure a tutela dei diritti e delle libertà degli interessati.

Uno dei temi di maggior attenzione ha riguardato il trattamento dei dati sanitari attraverso *app* volte a facilitare i rapporti tra medico e paziente, ivi compresi i medici di medicina generale (MMG) e i pediatri di libera scelta (PLS).

Compendio sulla sanità digitale

In particolare, si evidenzia che, a seguito di molteplici reclami e segnalazioni, il Garante ha adottato un compendio che si articola in dieci punti, con il quale ha inteso fornire delle preliminari indicazioni sul trattamento dei dati personali anche relativi alla salute effettuato attraverso tali piattaforme.

Attraverso le predette piattaforme digitali, che nella maggior parte dei casi fanno capo a società stabilite in paesi europei diversi dall'Italia o in paesi terzi, i dati personali (anche sanitari) dei pazienti vengono utilizzati per molteplici finalità da più soggetti che intervengono a vario titolo nelle operazioni di trattamento (ossia, in qualità di titolare, contitolare e responsabile del trattamento).

Il compendio fornisce chiarimenti con riferimento a tre macro-tipologie di trattamenti: dati personali dei pazienti, necessari per offrire loro servizi anche di tipo amministrativo correlati alla prestazione sanitaria richiesta (creazione dell'*account*, prenotazione di una visita medica, ecc.); dati personali dei professionisti sanitari trattati per diversi scopi (ad es., gestione dell'agenda del medico e recensioni degli utenti); dati sulla salute dei pazienti, trattati per finalità di diagnosi e cura (si pensi alla condivisione di documenti sanitari come prescrizioni o referti).

Per ciascuna delle tre macro-tipologie di trattamenti, si identificano le specifiche basi giuridiche, i ruoli, le responsabilità e gli obblighi in capo a siti e *app* e viene ricordata la necessità di adottare misure di sicurezza tecniche e organizzative, per garantire l'integrità e la riservatezza dei dati, così da ridurre i rischi di distruzione, perdita, modifica, divulgazione non autorizzata o accesso accidentale o illegale.

Una specifica sezione del compendio è dedicata all'obbligo per le piattaforme di svolgere una preventiva valutazione di impatto sul trattamento di dati che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Un paragrafo è inoltre riservato alle informazioni da rendere ai pazienti che, in conformità ai principi di correttezza e trasparenza, devono essere semplici e chiare oltre che concise, trasparenti, intelligibili e facilmente accessibili ed un altro è infine destinato al principio di *privacy by design* allo scopo di garantire l'esistenza di un corretto livello di protezione dei dati personali fin dalla fase di progettazione (*design*) di qualunque sistema, servizio, prodotto o processo (compendio 28 marzo 2024, doc. web n. 9997624).

5.1.1. Il Fascicolo sanitario elettronico

Nel corso del 2024 sono proseguite le interlocuzioni con il Ministero della salute, il MEF e con il Dipartimento per la trasformazione digitale per l'attuazione della

disciplina sul FSE 2.0 di cui al decreto del Ministero della salute 7 settembre 2023 su cui il Garante aveva reso il proprio parere (provv. 8 giugno 2023, doc. web n. 9900433, v. Relazione 2023, p. 60).

Opposizione all'alimentazione del FSE

L'Autorità ha reso il proprio parere sullo schema di decreto di modifica del decreto 4 agosto 2017 del MEF adottato di concerto con il Ministero della salute (decreto 11 aprile 2024), avente ad oggetto l'individuazione delle modalità di esercizio della facoltà di opposizione all'alimentazione del FSE con i dati generati precedentemente al 18 maggio 2020, ai sensi dell'art. 27 del d.m. 7 settembre 2023. Il Garante ha ritenuto conforme alla disciplina sulla protezione dei dati personali la realizzazione di un'unica funzionalità a livello nazionale per la manifestazione della predetta facoltà di opposizione, individuando il portale del Sistema tessera sanitaria (TS) quale unico punto di raccolta telematico della stessa. L'Autorità ha in particolare chiesto al Ministero della salute e alle regioni/province autonome di effettuare una efficace campagna informativa per almeno sessanta giorni e con modalità idonee a raggiungere puntualmente l'ampia platea di interessati coinvolti, attraverso l'utilizzo di una pluralità di canali di comunicazione e il coinvolgimento delle strutture sanitarie operanti sul territorio come le ASL, le farmacie e i MMG e i PLS (la campagna è iniziata il 22 aprile 2024 e si è conclusa il 30 giugno 2024) (provv. 7 marzo 2024, n. 158, doc. web 10005882).

A seguito dell'avvio della procedura per l'esercizio della facoltà di opposizione all'alimentazione del FSE con i dati e i documenti sanitari generati sino al 18 maggio 2020, l'Autorità ha ricevuto segnalazioni da parte di interessati che non sono riusciti ad esercitare tale facoltà entro il termine del 30 giugno 2024, per varie cause tra cui errori del sistema operativo e l'impossibilità di esercitare tale facoltà per i cittadini italiani iscritti all'AIRE. Alla luce di tali problematiche, è stato avviato un tavolo di lavoro con il Ministero della salute e il MEF che ha portato all'adozione del parere sullo schema di decreto adottato il 22 ottobre 2024, in cui l'Autorità ha richiesto una riapertura dei termini di opposizione per tutti gli assistiti, al fine di consentire a coloro che non avessero potuto esercitare la predetta facoltà di esercitarla per un ulteriore periodo di trenta giorni (dal 18 novembre al 18 dicembre 2024). L'estensione ha riguardato anche le persone con codice fiscale o con codice STP che non siano più assistiti dal SSN, la previsione dell'esercizio della predetta facoltà di opposizione *sine die* per i soggetti non più assistiti dal SSN, ma che lo siano stati in passato, entro 30 giorni dalla riattivazione dell'assistenza al SSN, e per tutti gli assistiti che nel tempo diventeranno maggiorenni, entro trenta giorni dal compimento della maggiore età. Nel decreto è stato inoltre previsto – su richiesta dell'Ufficio – uno specifico onere in capo alle ASL consistente nel fornire informazione su tale facoltà di opposizione al soggetto che riattiva l'assistenza sanitaria specificandone i termini e le modalità, nonché un aggiornamento del modello di informativa per il trattamento dei dati personali e delle modalità tecniche per l'esercizio della facoltà di opposizione al fine di tener conto delle predette modifiche (provv. 12 settembre 2024, n. 543, doc. web n. 10062281).

Difformità di attuazione

Con riferimento al trattamento dei dati personali effettuato attraverso il FSE, un ulteriore ambito di intervento dell'Autorità ha riguardato la difformità di attuazione della disciplina sul FSE e delle garanzie a tutela dei dati ivi previste sul territorio nazionale (cfr. *Newsletter* 26 giugno 2024, doc. web n. 10029439). Il Presidente dell'Autorità ha infatti segnalato al Presidente del Consiglio dei ministri e al Ministro della salute che gli esiti dell'attività istruttoria sul FSE, avviata alla fine di gennaio, avevano mostrato che 18 regioni e le due province autonome avevano significativamente modificato il modello di informativa predisposto dal Ministero, che era stato oggetto

del parere del Garante e che avrebbe dovuto essere adottato su tutto il territorio nazionale. Le difformità riscontrate riguardavano le modalità di esercizio di alcuni diritti (es. oscuramento, delega, consenso specifico) e specifiche misure (es. misure di sicurezza, livelli di accesso differenziati, qualità dei dati) introdotte dal decreto, proprio a tutela dei pazienti. Ciò contraddiceva lo spirito della riforma del FSE 2.0 volta a introdurre misure, garanzie e responsabilità omogenee sul tutto il territorio nazionale, rischiando così di compromettere anche la funzionalità, l'interoperabilità e l'efficienza del sistema. Con queste motivazioni, è stato notificato a tutti i predetti enti l'avvio di procedimenti correttivi e sanzionatori per le numerose violazioni riscontrate nell'attuazione della nuova disciplina sul FSE 2.0.

Al fine di superare la problematica emersa, il Ministero della salute ha quindi trasmesso all'Autorità uno schema di decreto, sul quale il Garante ha reso il proprio parere, che introduce una disciplina transitoria per l'attivazione di tutti i servizi e le funzionalità del FSE, con suddivisione in tre fasi, coerenti con le scadenze del PNRR, al fine di tutelare i diritti e le libertà di tutti gli interessati coinvolti nel trattamento dei dati sulla salute effettuato attraverso il FSE 2.0 (provv. 26 settembre 2024, n. 580, doc. web n. 10061545).

In una prima fase, da concludersi entro il 31 marzo 2025, dovrà essere data attuazione alle disposizioni relative alla cd. catena dell'oscuramento (prescrizioni e relativi documenti collegati) nonché alla registrazione delle operazioni su FSE e al connesso diritto dell'interessato di prendere visione degli accessi effettuati sul FSE. In una seconda fase, da concludersi entro il 30 settembre 2025, dovrà essere data attuazione alle disposizioni relative: all'identificazione dell'assistito tramite ANA; alla completa realizzazione del profilo sanitario sintetico (PSS) da parte dei MMG/PLS di tutte le regioni e province autonome; all'alimentazione da parte di tutte le regioni e province autonome dei dati soggetti a maggiore tutela dell'anonimato direttamente oscurati; all'accesso in consultazione ai dati e ai documenti del FSE per finalità di cura, secondo i livelli diversificati di accesso previsti nell'all. A del decreto 7 settembre 2023; alla completa realizzazione del Taccuino personale (TP); all'accesso al FSE da parte dei minori e di soggetti incapaci di intendere e volere e all'attuazione del sistema delle deleghe. Infine, in una terza fase, da concludersi entro il 31 marzo 2026, dovrà essere data attuazione alle disposizioni relative: alla completezza dei contenuti del FSE; alla sua tempestiva alimentazione, con i dati e documenti, entro cinque giorni dall'erogazione della prestazione sanitaria, nonché all'alimentazione con i dati e i documenti sanitari riferiti alle prestazioni erogate anche al di fuori del SSN; alla realizzazione dei servizi telematici accessibili attraverso un'interfaccia utente unica a livello regionale; all'accesso *online* al FSE da parte delle strutture sanitarie private autorizzate dal SSN e all'alimentazione del FSE da parte delle stesse entro cinque giorni dalla prestazione.

Al fine di garantire il pieno rispetto dei diritti e delle libertà degli interessati, il Garante ha chiesto che, nelle more della realizzazione di quanto previsto nelle predette fasi, i dati soggetti a maggiore tutela dell'anonimato non alimentino il FSE, l'accesso in emergenza al FSE non sia consentito in assenza di consenso dell'assistito alla consultazione dei dati del proprio FSE, l'accesso al FSE da parte di infermieri/ostetrici, farmacisti e personale amministrativo sia abilitato gradualmente al fine di assicurare che lo stesso sia consentito solo a seguito dell'adozione delle misure necessarie a garantire il rispetto dei profili di accesso di cui al decreto sul FSE 2.0.

Dati relativi a particolari prestazioni

Un altro significativo parere è stato reso con riferimento ad uno schema di decreto che individua, dopo ripetute sollecitazioni dell'Autorità, le modalità con cui il Sistema TS, tramite l'Infrastruttura nazionale per l'interoperabilità (INI), mette a disposizione

dei FSE i dati relativi alle prescrizioni e prestazioni erogate di farmaceutica e specialistica, nonché quelle con cui il Centro nazionale trapianti (CNT), tramite il Sistema informativo trapianti (SIT) rende disponibili ai FSE, attraverso INI, i dati relativi all'ultimo consenso o diniego alla donazione degli organi e tessuti, se espresso dall'assistito (parere 12 settembre 2024, n. 542, doc. web n. 10061561). Nel decreto sono state tenute in considerazione numerose osservazioni formulate dall'Autorità, tra le quali si richiamano quelle relative all'effettività del diritto di oscuramento nella cd. catena dell'oscuramento (ovvero, in caso di oscuramento delle prescrizioni specialistiche e farmaceutiche, all'oscuramento automatico anche dei documenti relativi all'erogazione delle prescrizioni, nonché dei referti riferiti alle medesime prestazioni). Come più volte rappresentato dal Garante, sin dal parere del 22 agosto 2022, il mancato rispetto di tale tutela rischia di vanificare l'eventuale richiesta di oscuramento dell'interessato in quanto nel FSE rimangono disponibili documenti sanitari connessi alla prestazione oscurata. È stato altresì introdotto l'oscuramento per impostazione predefinita nel FSE (attraverso un'analisi automatica dei codici posti sul documento sanitario relativi al quesito diagnostico e alla diagnosi) delle prescrizioni relative a prestazioni a maggior tutela di anonimato (es. interruzione volontaria di gravidanza, parto in anonimato).

Oltre ai pareri espressi sui decreti di attuazione della disciplina del FSE 2.0, nel corso del 2024 il Garante è intervenuto in materia anche con provvedimenti correttivi e sanzionatori.

Provvedimenti correttivi e sanzionatori

L'Autorità ha ammonito una casa di cura privata per non aver rispettato le disposizioni in ordine al diritto di oscuramento previste dalla disciplina sul FSE. Nel corso dell'istruttoria è stato constatato infatti che, sino al mese di febbraio del 2024, qualora un interessato avesse fatto richiesta di oscuramento di un documento clinico, il sistema in uso presso la casa di cura "sostituiva" il documento producendone uno nuovo che recava la data di tale "sostituzione", che poteva dunque non coincidere con la data in cui era stata redatta l'istanza di oscuramento, in violazione delle procedure previste per l'oscuramento e l'esattezza dei dati e dei principi generali del trattamento (provv. 13 novembre 2024, n. 673, doc. web n. 10087191).

Ulteriore intervento ha riguardato un *data breach*, causato da una vulnerabilità del sistema informatico, che aveva consentito a un cittadino autenticatosi con il ruolo di "assistito" di effettuare una ricerca di informazioni relative a sette individui presenti nell'Anagrafe regionale. Nel corso dell'attività istruttoria, il Garante ha accertato che la violazione era stata provocata da un *bug* di sicurezza nel sistema di autenticazione con cui si accedeva al FSE della regione. In particolare, non erano state introdotte misure volte a limitare l'accesso da parte degli utenti alle sole informazioni che li riguardavano, cosicché un soggetto terzo, superata la procedura di autenticazione, aveva potuto utilizzare funzionalità a cui non era autorizzato, mediante la modifica della URL (provv.ti 27 novembre 2024, n. 761, doc. web n. 10095761; n. 762, doc. web n. 10095810 e n. 763, doc. web n., e 10095791, nonché *Newsletter* 31 gennaio 2025, doc. web n. 10095854).

5.1.2. L'Ecosistema dati sanitari

L'Ecosistema dati sanitari (EDS), previsto dalla disciplina sul FSE, era già stato oggetto di un parere non favorevole il 22 agosto del 2022, n. 295 (doc. web n. 9802752).

Con il parere reso sulla nuova soluzione architetturale proposta dal Ministero (provv. 26 settembre 2024, n. 605, doc. web n. 10062302) è stato rilevato che sono state superate le criticità sollevate nel 2022, in particolare per una visione profondamente diversa da quella precedentemente proposta che tiene conto non solo della disciplina

sulla protezione dei dati, secondo i principi di *privacy by design*, ma anche della riforma del FSE 2.0.

L'EDS sarà alimentato in modo continuo con i dati del FSE che saranno elaborati nell'Ecosistema solo su richiesta degli istanti (interessati, professionisti sanitari, regioni/province autonome, Ministero della salute, AGENAS), al fine di fornire specifici servizi necessari alle finalità di cura e di governo sanitario, prevenzione e profilassi internazionale (per tali ultime finalità saranno accessibili solo dati privati degli elementi identificativi diretti e pseudonimizzati, secondo i livelli diversificati di accesso). Con riferimento ai predetti servizi sono state richieste specifiche misure a garanzia degli interessati relative ai profili di abilitazione e autorizzazione all'accesso (limitati esclusivamente a personale sanitario), al rispetto dei principi di minimizzazione, esattezza e aggiornamento dei dati, alla tassatività dei servizi di elaborazione dei dati e alle limitazioni all'attività di estrazione dei dati.

Molte sono state le osservazioni formulate dal Garante che hanno determinato specifiche puntuali modifiche e integrazioni nello schema di decreto. Tra di esse si segnalano l'individuazione chiara dei ruoli del trattamento tra i soggetti che a diverso titolo accedono all'EDS nonché l'esigenza che il consenso al trattamento dei dati effettuato attraverso l'EDS sia specifico ed espresso, non potendo essere ritenuto valido il consenso reso (anche in passato) per il solo FSE.

È stato inoltre previsto che l'interessato potrà richiedere di prendere visione delle registrazioni delle operazioni sui *file* di *log* relative ai servizi resi dall'EDS attraverso l'elaborazione dei dati del FSE.

Peculiari garanzie sono state previste anche per l'elaborazione dei dati dell'EDS ai fini della formazione del *dossier* farmaceutico (DF), ovvero di quella partizione del FSE che serve a favorire la qualità, il monitoraggio, l'appropriatezza nella dispensazione dei medicinali e l'aderenza alla terapia ai fini della sicurezza del paziente. Il DF non sarà costituito da una banca dati, ma sarà un servizio di estrazione ed elaborazione di determinate categorie di dati presenti nel FSE 2.0 effettuato solo su richiesta.

Per quanto concerne l'accesso all'EDS in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere e di rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato, che non abbia espresso il consenso al FSE e all'EDS, è stato previsto un accesso graduato da parte degli esercenti le professioni sanitarie: prioritariamente al PSS, solo eventualmente al resto del FSE e, ove ritenuto necessario, ai servizi resi disponibili dall'EDS per finalità di cura. Sono state inoltre richieste dal Garante specifiche garanzie con riferimento al consenso dei minori e, in via generale, alla revoca del consenso e alla anagrafe nazionale dei consensi.

Al fine di garantire all'interessato informazioni omogenee e uniformi sul territorio nazionale, è stato previsto che il Ministero della salute, in collaborazione con le regioni e province autonome, integri il modello di informativa relativa al FSE 2.0, su cui l'Autorità ha reso il proprio parere il 21 dicembre 2023, n. 600 (doc. web n. 9976886), con i trattamenti dei dati effettuati attraverso l'EDS, acquisendo un nuovo parere del Garante. Il Garante ha richiesto infine che nello schema di decreto fosse previsto che l'alimentazione e l'elaborazione dei dati del FSE effettuate al fine di offrire tutti i servizi dell'EDS sarebbero state realizzate solo previa completa attuazione della disciplina sul FSE 2.0 secondo quanto indicato nelle tre fasi di cui allo schema di decreto sulla disciplina transitoria del Fascicolo adottato in pari data (v. *supra*).

Con nota 2 dicembre 2024 il Garante ha espresso il proprio nulla osta in ordine ad alcune modifiche riguardanti lo schema di decreto EDS relative all'estrazione di dati provenienti dal Sistema TS, avendo ricevuto idonee assicurazioni circa il rispetto da parte del Sistema TS delle medesime garanzie offerte dalle soluzioni tecnologiche previste nel d.m. 7 settembre 2023 sul FSE 2.0.

5.1.3. Il dossier *sanitario*

Anche nel corso del 2024 l'Autorità si è occupata dei trattamenti effettuati attraverso il *dossier* sanitario di cui alle linee guida del 2015 (doc. web n. 4084632).

Un significativo intervento ha riguardato un'azienda sanitaria sanzionata per non aver configurato correttamente le modalità di accesso al *dossier*. L'Autorità si è attivata a seguito di alcuni reclami e segnalazioni concernenti lamentati e ripetuti accessi al *dossier* da parte di personale sanitario non coinvolto nel processo di cura dei pazienti.

Dalle verifiche effettuate dall'Autorità è emerso che il sistema di gestione del *dossier* consentiva agli operatori sanitari di inserire manualmente, mediante autocertificazione, la motivazione per cui si rendeva necessario l'accesso al *dossier* sanitario. L'accesso al documento era inoltre consentito, per impostazione predefinita, ad una ampia lista di figure professionali che niente avevano a che fare con il percorso di cura dei pazienti, compreso il personale amministrativo.

Oltre ad applicare la sanzione amministrativa, l'Autorità ha dunque ordinato all'ASL di mettere in atto tutte le misure tecniche e organizzative necessarie per garantire la sicurezza dei dati personali trattati e scongiurare nuovi accessi abusivi (provv. 22 febbraio 2024, n. 97, doc. web n. 10001279).

In un altro caso, a seguito di reclami e *data breach*, l'Autorità ha adottato un provvedimento sanzionatorio e correttivo con riferimento ai trattamenti di dati personali effettuati attraverso il *dossier* sanitario di una azienda ospedaliera. Nella specie la configurazione del *dossier* sanitario, al momento in cui si erano verificati i fatti segnalati, aveva consentito l'accesso a tale strumento informativo anche agli organi amministrativi aziendali per finalità distinte da quelle di cura della salute dell'interessato. Sul punto il Garante ha osservato che il *dossier* è per sua natura incompleto, a causa dell'esercizio del diritto di oscuramento da parte dell'interessato (peraltro esercitato nei casi in esame), e ciò inficia la completezza e correttezza dei dati in esso contenuti riverberandosi necessariamente anche sulle pratiche amministrative (provv. 9 maggio 2024, n. 295, doc. web n. 10027595).

L'Autorità ha dunque contestato che i trattamenti erano avvenuti in violazione dei principi di liceità, trasparenza, correttezza e di minimizzazione dei dati in quanto il *dossier* aziendale era stato impostato in modo da poter essere utilizzato per finalità non note agli interessati e, nello specifico, da parte di personale non sanitario per finalità amministrative e di personale sanitario non avente in cura l'interessato per finalità di cura di terzi (art. 5, par. 1, lett. a) e c), RGPD). È stata rilevata, inoltre, l'assenza di un sistema per il rilevamento di eventuali anomalie indicatrici di possibili trattamenti illeciti, contrariamente a quanto previsto nelle linee guida dell'Autorità, utili per orientare successivi interventi di *audit*.

Per i suddetti motivi all'azienda è stata comminata una sanzione ed è stato ingiunto di rimuovere alcune causali che avevano consentito le predette condotte illecite.

5.2. *L'uso dell'intelligenza artificiale in sanità*

Successivamente all'adozione del Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di IA avvenuta ad ottobre del 2023 (doc. web n. 9938038), l'Autorità ha continuato a vigilare in merito allo sviluppo di iniziative in tale ambito (cfr. Relazione 2023, p. 65). In particolare, sono state avviate alcune interlocuzioni con il Ministero della salute e AGENAS con riferimento al progetto di attuazione della Missione 6 del PNRR perseguito dalla predetta Agenzia, in merito alla realizzazione di una piattaforma informatica di IA a supporto dell'assistenza primaria

nell'ambito dei servizi sanitari regionali. Al riguardo, sulla base di quanto indicato nel predetto Decalogo, si è evidenziato che, in base ai principi in materia di protezione dei dati personali e, in particolare, al principio di responsabilizzazione, spetta a ciascun titolare, prima ancora di effettuare la valutazione di impatto, individuare i presupposti e le condizioni di liceità del trattamento dei dati, anche di tipo normativo, nonché essere in grado di dimostrare che il trattamento venga effettuato conformemente al RGPD (artt. 5 e 24 del RGPD).

Con specifico riferimento agli interventi normativi relativi al settore sanitario, oltre alle osservazioni formali formulate dal Presidente dell'Autorità sulla delega al Governo in materia di IA del 24 luglio 2024 (doc. web n. 10037983), il Garante, in due importanti pareri sulla sanità digitale relativi all'Ecosistema dati sanitari (EDS) (cfr. par. 5.1.2) e alla Piattaforma nazionale sulla telemedicina (PNT), ha richiamato l'attenzione sulla necessità che l'introduzione di sistemi di IA negli strumenti di sanità digitale realizzati per fini di governo sanitario avvenga nel rispetto del RGPD e del reg. sull'IA e di quanto indicato nel citato Decalogo.

In particolare, con riguardo al Sistema EDS, a seguito delle interlocuzioni intercorse con il Ministero della salute, è venuto meno il riferimento a sistemi di IA per l'elaborazione dei dati del FSE 2.0 da parte di EDS al fine di offrire i servizi indicati nel decreto.

Nel parere sulla PNT su richiesta dell'Autorità è stata eliminata la possibilità per l'AGENAS di procedere all'elaborazione dei dati estratti dall'EDS mediante sistemi di IA (algoritmi di *machine learning*) in quanto non conforme né ai principi del reg. IA o al RGPD, né alla specifica disciplina di settore (provv. 16 gennaio 2025, n. 2, doc. web n. 10105743, punto 6).

5.3. *Trattamenti di dati personali nell'ambito dei sistemi informativi sanitari centrali: pareri dell'Autorità*

EMUR

L'Autorità ha reso parere favorevole sullo schema di decreto del Ministro della salute di modifica del decreto del Ministro del lavoro, della salute e delle politiche sociali 17 dicembre 2008 e relativo al disciplinare tecnico, concernente il Sistema informativo per il monitoraggio delle prestazioni erogate nell'ambito dell'assistenza sanitaria in emergenza-urgenza (EMUR), in attuazione dell'art. 4, l. 5 maggio 2022, n. 53. In particolare era stata prevista la raccolta di ulteriori dati relativi agli accessi in pronto soccorso delle vittime della violenza di genere.

Lo schema di decreto e il relativo disciplinare hanno tenuto conto delle osservazioni formulate dall'Autorità nel corso delle numerose interlocuzioni con il Ministero della salute, che hanno riguardato in particolare la necessità di garantire l'anonimato delle donne vittima di violenza e di quelle che chiedono di partorire in anonimato nonché il pieno allineamento del Sistema con i requisiti dell'attuale quadro normativo.

Il Sistema infatti era stato istituito nel 2008, ben dieci anni prima della piena applicazione del RGPD. In particolare, il Garante ha chiesto l'aggiornamento del sistema di codifica e di aggregazione dei dati nonché l'individuazione del tempo di conservazione delle informazioni e dei ruoli *privacy* dei diversi soggetti che intervengono nelle operazioni di trattamento (provv. 21 marzo 2024, n. 176, doc. web n. 10007868).

CEDAP

Il Garante si è inoltre espresso, favorevolmente, sullo schema di decreto del Ministro della salute recante certificato di assistenza al parto (CEDAP), per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla natimortalità ed ai nati affetti da patologie congenite che abroga e sostituisce il decreto

del Ministro della salute 16 luglio 2001, n. 349 e sul relativo disciplinare tecnico, che ne forma parte integrante.

Lo schema di decreto aveva previsto l'istituzione del relativo sistema informativo per la rilevazione da parte delle strutture sanitarie e la comunicazione alle regioni/province autonome e da esse al Ministero della salute delle informazioni di carattere sanitario, epidemiologico e socio-demografico nell'area materno-infantile contenute nel CEDAP. In particolare, al fine di consentire la richiamata procedura di interconnessione, lo schema di decreto aveva individuato le informazioni necessarie ad attribuire il codice univoco nazionale dell'assistito oltre che nuove variabili relative alla madre da inserire nel certificato, quali la coabitazione, il peso pregravidico, il peso al parto, necessarie per rilevare l'incidenza di una solida rete sociale sulle scelte procreative della donna e per esigenze di salute pubblica. Il Garante ha riconosciuto che le misure di garanzia previste con riguardo ai trattamenti in questione erano appropriate per tutelare i diritti fondamentali e gli interessi delle persone fisiche (provv. 20 giugno 2024, n. 369, doc. web n. 10036885).

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

5.4.1. Provvedimenti derivanti da data breach

Negli ultimi anni l'Autorità ha avviato numerose istruttorie a seguito di notifiche di violazioni di dati personali comunicate dai titolari del trattamento, ai sensi dell'art. 33 del RGPD, che sono sfociate nell'adozione di provvedimenti principalmente sanzionatori.

Inadeguatezza delle misure di sicurezza

In relazione alla inadeguatezza delle misure di sicurezza adottate, l'Autorità ha riscontrato che essa aveva comportato presso un'azienda sanitaria la tardiva rilevazione sia di comportamenti anomali (quali, ad es., l'orario e la frequenza degli accessi, tendenzialmente notturni, la loro provenienza da indirizzi IP di paesi stranieri), sia della violazione di dati personali, nonché delle operazioni effettuate con gli *account* di dominio con o senza privilegi amministrativi, per esempio, la disattivazione del *software antivirus* su alcuni sistemi (provv. 17 luglio 2024, n. 444, doc. web n. 10057610).

In un altro caso, gli accertamenti svolti successivamente alla notifica del *data breach* hanno evidenziato che l'azienda sanitaria non si era dotata di uno strumento di XDR e di un servizio di controllo e monitoraggio dei *firewall*, nonché la mancata attivazione di procedure di autenticazione rafforzate e l'utilizzo di *software* di base obsoleti (provv. 4 luglio 2024, n. 409, doc. web n. 10074293).

In occasione di un'ispezione presso un'azienda sanitaria che aveva notificato una violazione di dati personali a seguito di un attacco *hacker*, è stato accertato che la stessa non aveva adottato adeguate misure per segmentare e segregare le reti su cui erano attestate le postazioni di lavoro dei propri dipendenti, né i *server* utilizzati per i trattamenti e, anche in questa vicenda, non solo l'accesso remoto, tramite VPN, alla rete dell'azienda, era avvenuto mediante una procedura di autenticazione informatica basata solo sull'utilizzo di *username* e *password*, ma erano stati utilizzati, *software* di base obsoleti (provv. 17 ottobre 2024, n. 621, doc. web n. 10086523).

Una sanzione è stata irrogata nei confronti di un'azienda socio sanitaria, i cui sistemi erano stati, anch'essi, oggetto di un attacco informatico, determinato da un *malware* di tipo *ransomware*. È stato rilevato che l'attivazione di strumenti EDR/XDR era prevista solo su un limitato numero di *server* e che l'azienda non era dotata di un *Security Information and Event Management* (SIEM) quale strumento di correlazione

dei vari *log* raccolti da *server*; a ciò si aggiungevano carenze in ordine alla segmentazione/segregazione delle reti e la mancata adozione di un sistema di autenticazione a doppio fattore (provv. 14 novembre 2024, n.760, doc. web n. 10104860).

Significativo l'intervento nei confronti di una regione, della relativa società informatica e di una ASL a seguito dell'attacco informatico al Sistema sanitario regionale avvenuto in una notte dell'agosto del 2021. Il *data breach* – causato da un *ransomware* introdotto nel sistema attraverso un portatile in uso a un dipendente della regione – aveva bloccato l'accesso a molti servizi sanitari impedendo, tra l'altro, la gestione delle prenotazioni, i pagamenti, il ritiro dei referti, la registrazione delle vaccinazioni per un arco temporale compreso tra le quarantotto ore e alcuni mesi. Nei provvedimenti è stata anche considerata la circostanza che non erano state poste in essere le azioni necessarie per una gestione corretta del *data breach* e delle sue conseguenze, in particolare nei confronti dei soggetti per i quali la regione operava quale responsabile del trattamento (a partire dalle numerose strutture sanitarie coinvolte) (provv.ti 21 marzo 2024, n. 194, doc. web n. 10002324; n. 195, doc. web n. 10002533 e n. 196, doc. web n. 10002287).

A seguito della notifica di violazione ai sensi dell'art. 33 del RGPD da parte di una struttura ospedaliera di eccellenza, il Garante ha adottato un provvedimento sanzionatorio sia nei confronti di tale struttura che della società informatica nominata da quest'ultima quale responsabile del trattamento, per il verificarsi di un *bug* nel sistema informatico fornito all'ospedale. Il *bug* aveva determinato l'invio, al sistema di gestione dati dell'ospedale, di referti di laboratorio contenenti un segmento di informazione riportante un identificativo di un paziente diverso rispetto a quello contenuto del referto, in violazione dei principi di cui agli artt. 5, lett. f) e 9 del RGPD, nonché degli obblighi in materia di sicurezza, di cui all'art. 32, par. 1, lett. b) e d), RGPD (provv.ti 24 gennaio 2024, n. 38, doc. web n. 9988652 e n. 39 doc. web n. 9990640).

Erroneo invio di *e-mail*

Segnaliamo i casi seguenti in cui l'erroneo invio tramite *e-mail* di documentazione sanitaria ha indotto l'Autorità ad adottare misure correttive di diversa natura, in rapporto alla diversa gravità della fattispecie:

- un provvedimento di ammonimento nei confronti di una struttura sanitaria privata, titolare del trattamento, per la violazione dei principi di cui agli artt. 5 e 9 del RGPD e degli obblighi in materia di sicurezza di cui all'art. 32 del RGPD, nonché nei confronti dell'associazione, responsabile del trattamento, che aveva inviato erroneamente dati relativi alla salute di una coppia di pazienti, per aver violato gli obblighi previsti dall'art. 32 del RGPD (provv.ti 17 luglio 2024, n. 442, doc. web n. 10057329 e n. 443 doc. web n. 10057346);

- una sanzione pecuniaria nei confronti di un'azienda sanitaria e, in particolare, dell'ambulatorio di neurologia che aveva inviato a più destinatari due comunicazioni *e-mail* aventi ad oggetto le modalità rinnovo del piano terapeutico attraverso l'inserimento degli indirizzi nel campo c.c. e non in c.c.n. (provv. 23 maggio 2024, n. 306, doc. web n. 10037439);

- una sanzione pecuniaria significativa unitamente a prescrizioni specifiche nei confronti di una società che produce dispositivi medici per il monitoraggio, la prevenzione e il trattamento di diverse patologie, la quale aveva trasmesso a circa 730 persone diabetiche, che utilizzavano un dispositivo medico per la misurazione dei livelli di glucosio collegato con un'applicazione, informazioni tramite alcune *e-mail* inserendo gli indirizzi nel campo c.c. anziché nel campo c.c.n. Nel corso della citata istruttoria è anche emerso che nell'informativa non era stata indicata la base giuridica della comunicazione di dati personali dei pazienti interessati a collegare il proprio *account* personale con quello del

professionista sanitario, in qualità di titolare del trattamento, in violazione del principio di correttezza e trasparenza di cui agli artt. 5, par. 1 lett. a), nonché degli artt. 12 e 13 del RGPD (provv. 8 febbraio 2024, n. 62, doc. web n. 9991183);
- la sanzione pecuniaria irrogata nei confronti di un'azienda sanitaria a seguito dell'invio, da parte del professionista sanitario operante presso la stessa, a più soggetti, tra i quali l'Ordine dei medici, di una *e-mail* contenente in allegato una lista dei pazienti visitati in un determinato giorno, al fine di fornire chiarimenti in merito all'orario di lavoro svolto (provv. 12 dicembre 2024, n. 770, doc. web n. 10102444).

5.4.2. Provvedimenti derivanti da reclami e segnalazioni

A seguito di una segnalazione del Nucleo antisofisticazioni e sanità (NAS) dei carabinieri che aveva raccolto anche le testimonianze di alcuni assistiti di un medico, l'Autorità ha avviato una istruttoria nei confronti del professionista, che aveva l'abitudine di depositare le ricette per i suoi pazienti in una cassetta delle poste e in un contenitore di metallo, liberamente accessibili, posti a lato della porta di ingresso dello studio. L'Autorità ha adottato un provvedimento sanzionatorio, evidenziando che già dal periodo emergenziale erano state previste talune misure volte ad agevolare l'uso delle modalità semplificate di acquisizione del promemoria dematerializzato ovvero del numero di ricetta elettronica, proprio al fine di evitare che l'assistito dovesse recarsi presso lo studio del medico a ritirare la prescrizione (cfr. poi, d.l. 29 dicembre 2022, n. 198, così come modificato dalla l. di conversione 24 febbraio 2023, n. 14) (provv. 11 gennaio 2024, n. 11, doc. web n. 9983244).

In un altro caso ed a seguito di reclamo, un'azienda sanitaria è stata destinataria di un provvedimento sanzionatorio per avere trasmesso una *e-mail* alla reclamante ad un indirizzo diverso da quello della stessa. Tale *e-mail* conteneva, in allegato, un provvedimento (recante in chiaro molte informazioni personali, anche relative al percorso medico intrapreso e da intraprendere) con il quale l'ufficio ricoveri *extra* regionale dell'azienda aveva negato la concessione di benefici economici per usufruire di prestazioni sanitarie presso una struttura privata *extra* regione (provv. 8 febbraio 2024, n. 63, doc. web n. 9994882).

Un altro reclamo ha riguardato la condotta di un'azienda sanitaria che aveva accidentalmente applicato un'etichetta nominativa di reparto, recante il nome di una paziente su un tracciato cardiotocografico, effettuato da un'altra paziente. In tale circostanza, è stato sufficiente ammonire il titolare del trattamento in considerazione, tra l'altro, del fatto che l'episodio risultava essere un caso isolato e, sotto il profilo dell'elemento soggettivo, privo di dolo e che il grado di colpa era stato valutato come lieve (provv. 22 febbraio 2024, n. 98, doc. web n. 9997395).

In un'altra occasione, il Garante ha riscontrato una non corretta gestione dei dati personali da parte di una struttura sanitaria pubblica che aveva rilasciato, per giustificare un'assenza dal lavoro, certificazioni attestanti la presenza della lavoratrice in ospedale riportando l'indicazione del reparto che aveva erogato la prestazione sanitaria e il timbro con la specializzazione del medico, da cui potevano desumersi informazioni sullo stato di salute. In tale caso, il Garante ha ritenuto sussistere una violazione degli obblighi in materia di sicurezza, del principio di minimizzazione dei dati personali e del principio di *privacy by design* nella condotta dell'azienda (provv. 26 settembre 2024, n. 581, doc. web n. 10079346).

Nell'ambito di una istruttoria è stato accertato che una società, al momento del reclamo, non aveva messo in atto alcuna modalità volta a impedire l'illecita o fortuita acquisizione delle informazioni trasmesse, come, ad esempio, una *password* per l'apertura del *file* o una chiave crittografica nell'invio via *e-mail* di un referto.

L'acquisizione di un eventuale consenso degli interessati alla trasmissione via *e-mail* dei referti "in formato PDF senza l'utilizzo di *password*" non avrebbe, comunque, sollevato il titolare dall'obbligo di valutare, continuamente nel corso del tempo, un adeguato livello di sicurezza che tenesse anche conto dello sviluppo tecnologico e dei nuovi rischi connessi al trattamento per i diritti e le libertà degli interessati. La predetta società è stata destinataria di un provvedimento sanzionatorio (provv. 17 ottobre 2024, n. 620, doc. web n. 10074551).

Il Garante ha adottato, poi, un provvedimento nei confronti di un MMG per avere quest'ultimo rilasciato documentazione sanitaria, in busta chiusa, al marito dell'interessata in assenza di delega scritta. L'Autorità, sin dal 1997, con riferimento alla "Tutela dei dati sanitari del paziente nell'attività del medico di base" si è espressa nel senso che la documentazione medica può essere ritirata "(…) anche da persone diverse dai diretti interessati, purché sulla base di una delega scritta e mediante una consegna dei documenti in busta chiusa" (doc. web n. 49311), ribadendo tali indicazioni in successivi provvedimenti (cfr., fra altri, il provvedimento "Strutture sanitarie: rispetto della dignità - 9 novembre 2005", par. 4, "Comunicazione di dati all'interessato" - doc. web n. 1191411). Accertata la violazione dei principi di cui all'art. 5, par. 1. lett. f), RGPD, nonché degli obblighi di sicurezza di cui all'art. 32 del RGPD medesimo, in considerazione delle circostanze che hanno caratterizzato la vicenda, il Garante ha ritenuto trattarsi di violazione minore ai sensi del cons. 148 del RGPD e ha ammonito il titolare del trattamento (provv. 12 settembre 2024, n. 548, doc. web n. 10064128).

Il Garante ha, infine, sanzionato un'azienda sanitaria avendo accertato la violazione, da parte di quest'ultima, degli artt. 5, par. 1, lett. f) e 32 del RGPD, nonché dell'art. 33 del RGPD, rispettivamente per non aver adottato misure organizzative e tecniche adeguate a scongiurare l'evento verificatosi (smarrimento di un verbale redatto dalla commissione per malati gravissimi) e per non aver effettuato la notifica di violazione al Garante a seguito del sinistro occorso (provv. 19 dicembre 2024, n. 897, doc. web n. 10107405).

Diffusione di dati sanitari

Il Garante ha adottato un provvedimento sanzionatorio nei confronti di un centro estetico per avere pubblicato un video sul proprio profilo pubblico di Instagram, in cui lo stesso reclamante era stato ritratto durante un trattamento di medicina estetica, in violazione dei principi di liceità, correttezza e trasparenza.

L'Autorità ha in particolare ribadito quanto già previsto nel codice di condotta per l'utilizzo dei dati sulla salute a fini didattici e di pubblicazione scientifica, approvato con provv. 14 gennaio 2021, n. 7, doc. web n. 9535354, ossia che le richiamate ed asserite finalità divulgative-scientifiche perseguite dalla società mediante la pubblicazione del predetto video avrebbero dovuto, se del caso, essere perseguite attraverso il trattamento di dati anonimizzati alla luce dell'*Opinion* 05/2014 del WP29; qualora non fosse stato possibile procedere all'anonimizzazione dei dati (es. per le peculiarità del caso clinico rappresentato), si sarebbe dovuto acquisire uno specifico e informato consenso dell'interessato, raccolto il quale i dati avrebbero dovuto comunque essere sottoposti a pseudonimizzazione. È infatti vietata la diffusione di immagini e informazioni riferite a casi clinici per scopi divulgativi o scientifici in assenza di una idonea base giuridica (art. 2-*septies*, comma 8, del Codice). L'Autorità ha inoltre ingiunto alla struttura sanitaria l'adozione di misure correttive per conformare l'informativa alla normativa *privacy* (provv. 11 gennaio 2024, n. 10, doc. web n. 9983210).

5.4.3. Provvedimenti relativi al trattamento dei dati personali effettuato nell'ambito dell'emergenza sanitaria

In merito ai trattamenti effettuati durante la pandemia da COVID-19 il Garante ha

ritenuto necessario fornire alcune precisazioni in merito alle dichiarazioni rese dal Presidente della Regione Lombardia, che erroneamente aveva attribuito agli interventi dell'Autorità l'impossibilità di utilizzare certi dati sanitari per contrastare l'emergenza sanitaria (comunicato stampa 26 giugno 2024, doc. web n. 10030521). Sul punto è stato ricordato che sin dalla dichiarazione dello stato di emergenza deliberato dal Consiglio dei ministri il 31 gennaio 2020, l'Autorità aveva adottato diverse disposizioni che hanno consentito degli interventi emergenziali che implicavano il trattamento dei dati e che sono state frutto di un delicato bilanciamento tra le esigenze di sanità pubblica e quelle relative alla protezione dei dati personali. Alcuni interventi, impugnati dai titolari del trattamento, sono stati confermati sia in Cassazione (provv. 13 maggio 2021, n. 268, doc. web 9685332) che dalla Corte costituzionale (provv. 7 dicembre 2023, n. 587, doc. web 9978342).

Per quanto riguarda le iniziative promosse in Regione Lombardia, il Garante ha ricordato il provvedimento sanzionatorio nei confronti di una azienda sanitaria milanese del 3 maggio 2021, n. 268 (doc. web n. 9685332) confermato anche dalla Corte di cassazione che ha riconosciuto le violazioni rilevate dal Garante e la relativa competenza.

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

Di estrema delicatezza è stato l'intervento dell'Autorità a seguito di un reclamo da parte di una interessata, che aveva lamentato la trasmissione dei suoi dati personali relativi all'infezione da HIV da parte di un'azienda sanitaria all'amministrazione presso la quale prestava servizio il genero, il quale aveva richiesto alla sua amministrazione i benefici previsti dalla l. n. 104/1992 per assisterla. In particolare, l'azienda aveva trasmesso alla citata amministrazione l'intero verbale comprensivo di anamnesi completa, dalla quale risultava anche l'infezione HIV e la nefropatia HIV correlata. L'azienda è stata, pertanto, destinataria di un provvedimento sanzionatorio, per aver violato non solo i principi di minimizzazione, di integrità e riservatezza e gli obblighi in materia di sicurezza, ma anche l'art. 75 del Codice, in relazione alle specifiche disposizioni di settore riguardanti le tutele previste in materia di HIV (artt. 5, comma 4 e 1, comma 2, l. 5 giugno 1990, n. 135) (provv. 6 giugno 2024, n. 337, doc. web n. 10039453).

In un altro caso, un reclamo pervenuto all'Autorità da parte di una paziente ha riguardato la diffusione di dati sanitari da parte di un medico. In particolare, all'esito di una specifica istruttoria, è stato verificato che un chirurgo aveva pubblicato sul proprio profilo Instagram le foto di una paziente, che la ritraevano in modo riconoscibile, prima e dopo un intervento di *lifting* del volto, senza avere, peraltro, acquisito il consenso alla diffusione delle immagini. Nel provvedimento sanzionatorio adottato nei confronti del medico, il Garante ha ritenuto illecito il trattamento dei dati sanitari in parola in quanto effettuato al di fuori delle finalità di cura per le quali il medesimo medico era legittimato al trattamento e in violazione dei principi di cui agli artt. 5 e 9 del RGPD nonché del divieto di diffondere dati sulla salute (art. 2-*septies*, comma 8, del Codice) (provv. 12 dicembre 2024, n. 769, doc. web n. 10095836).

Di estrema importanza è stato il provvedimento di avvertimento nei confronti della Regione Puglia, a seguito di una disposizione legislativa regionale che aveva introdotto l'obbligo per gli studenti di scuole medie, superiori ed università, di presentare una

certificazione attestante l'avvenuta vaccinazione anti-HPV, oppure l'avvio del programma di somministrazione, oppure il rifiuto alla somministrazione del vaccino, oppure l'avvenuto espletamento del colloquio informativo sui benefici della vaccinazione, per potersi iscrivere ai relativi corsi di istruzione. È stato evidenziato che l'acquisizione di documentazione, anche sanitaria, da parte delle autorità scolastiche e l'onere di produrre la predetta documentazione da parte degli studenti e delle famiglie non appaiono essere possibili, se non nei limiti in cui ciò sia previsto da una norma uniforme a livello nazionale, nel rispetto del principio di proporzionalità (art. 6, par. 3, lett. b), RGPD) e del principio di ragionevolezza (art. 3 della Costituzione) (provv. 2 agosto 2024, n. 476, doc. web n. 10042438).

5.6. *Esercizio dei diritti*

Con riguardo, in particolare, al diritto di accesso ai dati personali previsto dall'art. 15 del RGPD, occorre segnalare che nel 2024 il Garante ha ricevuto alcuni reclami concernenti il mancato rilascio gratuito di copia documentale della propria cartella clinica da parte di talune strutture ospedaliere del territorio nazionale. In considerazione del fatto che le istanze rimaste insoddisfatte erano volte a ottenere gratuitamente l'intera copia documentale della cartella clinica, il Garante ha archiviato tali reclami in quanto non competente in materia di accesso alla documentazione. Le strutture ospedaliere in questione avevano infatti rilasciato ai richiedenti copia documentale della cartella clinica sulla base delle disposizioni nazionali in tema di accesso ai documenti (l. n. 241/1990, nonché l. n. 24/2017), le quali prevedono un rimborso dei costi sostenuti per la produzione delle copie dei documenti. Nella rappresentazione delle suddette doglianze era stata invocata, a fondamento del diritto a veder soddisfatta la propria richiesta gratuitamente, la pronuncia del 26 ottobre 2023, della CGUE nella causa C-307/22, secondo la quale il diritto di ottenere una copia dei dati personali oggetto di trattamento sulla base dell'art.15, par. 3, RGPD implica la consegna all'interessato di una riproduzione fedele e intelligibile dell'insieme di tali dati. Tale diritto, per la Corte, presuppone quello di ottenere la copia integrale dei documenti contenuti nella sua cartella medica, qualora la fornitura di una siffatta copia sia necessaria per consentire all'interessato di verificarne l'esattezza e la completezza, nonché per garantirne l'intelligibilità. Per quanto riguarda i dati relativi alla salute, il citato diritto, nell'interpretazione della Corte, include in ogni caso quello di ottenere una copia dei dati della sua cartella medica contenente informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati al medesimo.

In relazione a tale pronuncia, il Garante ha ritenuto di intervenire attraverso alcuni chiarimenti, distinguendo, ancora una volta, tra gli istituti previsti dal nostro ordinamento in materia di accesso alla documentazione (l. n. 241/1990 e, in particolare in materia sanitaria, l. n. 24/2017) e quello in materia di accesso ai dati personali *ex* art. 15 del RGPD.

In tale ottica ha pertanto pubblicato alcune FAQ sul proprio sito web istituzionale (https://www.gpdp.it/web/guest/temi/sanita-e-ricerca-scientifica/cartelle-cliniche) chiarendo che la struttura sanitaria, titolare del trattamento, a seguito di una istanza presentata ai sensi dell'art. 15 del RGPD, è tenuta a fornire al richiedente copia dei dati personali oggetto del trattamento. La prima copia di tali dati è rilasciata gratuitamente. La struttura sanitaria valuta se fornire copia integrale di tutta o parte della documentazione contenuta nella cartella clinica qualora ciò sia necessario per

consentire all'interessato – come stabilito dalla sentenza CGUE C-307/22 – di verificare l'esattezza, la completezza e l'intelligibilità delle informazioni richieste: è in tal caso che la copia integrale di tutta o parte dei documenti sanitari contenuti nella cartella clinica è fornita gratuitamente. In ultimo, il Garante ha tenuto a evidenziare che in caso di ricezione di istanze generiche di accesso, le linee guida del Comitato (EDPB) raccomandano ai titolari del trattamento di chiedere agli interessati di specificare l'oggetto della richiesta (dati personali o documentazione).

Fra i provvedimenti sanzionatori adottati in materia nel corso del 2024, segnaliamo quello nei confronti di un professionista sanitario. La questione ha tratto origine dal mancato riscontro da parte del predetto medico alla richiesta di accesso dell'interessata, poi reclamante, alle fotografie pre-operatorie relative a un intervento effettuato dal medesimo professionista. A seguito dell'attività istruttoria, l'Autorità ha accertato la violazione dell'art. 12, in relazione all'art. 15 del RGPD, per non aver il medico fornito riscontro, entro i termini previsti dall'art. 12 del RGPD, all'istanza di esercizio del diritto di accesso ai dati avanzata dall'interessata, riscontro che è stato fornito soltanto a seguito dell'invito ad aderire alle richieste della reclamante formulato dall'Autorità. Inoltre è emersa la violazione dell'art. 13, par. 2, lett. a), RGPD, mancando l'indicazione precisa, nell'informativa sottoposta ai pazienti, dei tempi di conservazione dei dati personali trattati o dei criteri per determinarli. Per tali ragioni, l'Autorità ha sanzionato il medico, in qualità di titolare del trattamento, ingiungendo allo stesso, ai sensi dell'art. 58, par. 2, lett. d), RGPD, di provvedere a integrare l'informativa, individuando più dettagliatamente tale periodo di conservazione dei dati personali o i criteri utilizzati per determinarlo (provv. 24 giugno 2024, n. 372, doc. web n. 10037411).

Il Garante ha, poi, sanzionato un'azienda sanitaria per avere trattato alcuni dati personali dell'interessato (indirizzi di residenza anagrafica e di domicilio sanitario), nell'inosservanza del principio di esattezza e per non aver risposto all'istanza di esercizio dei diritti dell'interessato di cui all'art. 16 del RGPD entro i termini di cui all'art. 12 del RGPD, in violazione dell'art. 5, par. 1, lett. d), RGPD. (provv. 23 maggio 2024, n. 305, doc. web n. 10036837).

Al termine dell'istruttoria riguardante altra vicenda oggetto di reclamo, il Garante, accertato il mancato riscontro da parte di uno psicoterapeuta a una istanza di esercizio del diritto di accesso ai dati di cui all'art. 15 del RGPD nei termini di cui all'art. 12 del RGPD, unitamente all'accertamento di altre violazioni (violazione dell'art. 5, lett. a), RGPD e degli obblighi informativi di cui all'art. 13 del RGPD, nonché violazione dell'art. 157 del Codice per il mancato riscontro alla richiesta di informazioni dell'Autorità), ha adottato un provvedimento sanzionatorio nei confronti del titolare del trattamento (provv. 17 ottobre 2024, n. 619, doc. web 10072669).

5.7. *Oblio oncologico*

La l. 7 dicembre 2023, n. 193 ha attribuito al Garante il compito di vigilare sull'applicazione delle disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone che sono state affette da malattie oncologiche (cd. oblio oncologico). In tale ambito l'Autorità ha reso il 20 giugno 2024 due pareri su due schemi di decreto del Ministero della salute attuativi delle predette disposizioni (n. 367, doc. web n. 10036869 e n. 368, doc. web n. 10043511).

È stata segnalata la necessità di apportare correttivi al fine di rendere la disciplina in parola pienamente conforme ai principi in materia di protezione dati. In tal senso

5

sono state introdotte disposizioni puntuali al fine di determinare con certezza la data di conclusione del trattamento attivo necessario per determinare chiaramente da quando decorre il diritto all'oblio nonché di individuare il periodo di conservazione dei dati raccolti nell'esercizio di tale diritto. L'Autorità ha inoltre chiesto di prevedere un unico modello (a livello nazionale) di informativa in cui risultino chiari i ruoli ricoperti dai vari soggetti che intervengono nel trattamento.

Il Garante nel 2024 ha pubblicato sul proprio sito una scheda informativa e alcune FAQ al fine di fornire chiarimenti ai cittadini su tale diritto e di dare indicazioni utili a tutti i datori di lavoro pubblici e privati affinché possano applicare correttamente la nuova normativa (https://www.gpdp.it/web/guest/temi/sanita-e-ricerca-scientifica/oblio-oncologico).

Nelle FAQ viene chiarito che la normativa vieta a banche, assicurazioni e a tutti i datori di lavoro (sia nella fase di selezione del personale sia durante il rapporto lavorativo), di richiedere all'utente e al dipendente informazioni su una patologia oncologica da cui sia stato precedentemente affetto e il cui trattamento si sia concluso – senza episodi di recidiva – da più di dieci anni (ridotti a cinque se il soggetto aveva meno di 21 anni al momento in cui è insorta la malattia).

La legge stabilisce, inoltre, particolari tutele per le coppie che presentano domanda di adozione al tribunale per i minorenni; quest'ultimo, nella selezione delle coppie, non può raccogliere informazioni sulle patologie oncologiche pregresse quando siano trascorsi più di dieci anni dalla conclusione del trattamento della patologia – in assenza di recidive o ricadute – o più di cinque anni se la patologia si è manifestata prima del compimento del 21esimo anno di età.

6 La ricerca scientifica

6.1. *La modifica dell'art. 110 del Codice*

Nell'anno di riferimento, è stata approvata una modifica normativa di estremo rilievo per il trattamento dei dati personali per finalità di ricerca scientifica in campo medico, biomedico ed epidemiologico. L'art. 44, comma 1-*bis*, d.l. 2 marzo 2024, n. 19, convertito con l. 29 aprile 2024, n. 56, ha infatti modificato la seconda parte dell'art. 110, comma 1, del Codice.

In base alla nuova formulazione dell'art. 110 del Codice, laddove non sia possibile acquisire il consenso degli interessati e non vi siano altri presupposti normativi, il titolare del trattamento di dati sulla salute per scopi di ricerca medica, biomedica e epidemiologica non è più tenuto a presentare un'istanza di consultazione preventiva al Garante, ma deve osservare le garanzie individuate da quest'ultimo, ai sensi dell'art. 106, comma 2, lett. d), del Codice, nella deliberazione di promovimento delle nuove regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, con la quale è stata data appunto attuazione anche al novellato art. 110 del Codice (artt. 2-*quater* e 106 del Codice, provv. 9 maggio 2024, n. 298, doc. web n. 10016146) (cfr. par. 6.4).

In tale ambito, l'Autorità ha, in primo luogo, precisato quali sono le circostanze nelle quali informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, correlandole a motivi di ordine etico (ossia quelli riconducibili alla circostanza per cui l'interessato ignora la propria condizione) o organizzativo (ovvero ad esempio, quelli riconducibili alla circostanza per cui il mancato completamento del campione considerato potrebbe produrre conseguenze significative per lo studio in termini di qualità dei risultati della ricerca stessa).

Rispetto alle specifiche garanzie da adottare, in omaggio al principio di *accountability*, prima dell'inizio dei trattamenti, l'Autorità ha ribadito che il titolare del trattamento deve adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche alla luce di quanto sopra indicato, e acquisire il parere favorevole del competente comitato etico a livello territoriale sul progetto di ricerca come previsto dall'art. 110 del Codice.

E' stato disposto, in particolare, che i titolari debbano accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative in virtù delle quali informare gli interessati e quindi acquisirne il consenso risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, eventualmente documentando altresì i ragionevoli sforzi profusi per tentare di contattarli.

In tutti questi casi, i titolari del trattamento di dati per finalità di ricerca medica, biomedica e epidemiologica riferiti a soggetti deceduti o non contattabili devono altresì svolgere e pubblicare, anche solo per estratto, la valutazione di impatto, ai sensi dell'art. 35 del RGPD, dandone comunicazione al Garante.

Le istruttorie pendenti aventi ad oggetto le istanze di consultazione preventiva presentate antecedentemente alla novella dell'art. 110 del Codice sono state definite

con note di esito nelle quali è stato rappresentato quanto poc'anzi illustrato, evidenziando in special modo i rinnovati adempimenti posti a carico dei titolari del trattamento.

6.2. *Provvedimenti adottati ai sensi dell'art. 110 del Codice prima della riforma di aprile 2024*

Nella prima parte del 2024, il Garante ha adottato numerosi provvedimenti a seguito della consultazione preventiva prevista, prima della novella ricordata al par. 6.1, ai sensi degli artt. 110 del Codice e 36 del RGPD. In ciascuno di essi, il Garante ha avuto l'occasione di fornire importanti indicazioni in ordine alle modalità di trattamento dei dati personali nel settore di riferimento, anche ai sensi del punto 5.3. delle prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (all. n. 5 al provv. 5 giugno 2019, n. 146, doc. web n. 9124510).

Nello specifico, l'Autorità si è soffermata sul corretto inquadramento delle condizioni di liceità. Si è così evidenziato che, da un lato, la base giuridica del trattamento dei dati riferiti a soggetti deceduti ovvero non contattabili deve essere rinvenuta nella procedura di consultazione preventiva ai sensi degli artt. 110 del Codice e 36 del RGPD e, dall'altro lato, che, qualora lo studio comporti il trattamento di dati personali di soggetti che versano in condizioni di "stato vegetativo", essa vada rinvenuta nel consenso prestato dai soggetti di cui all'art. 82, comma 2, lett. a), del Codice.

Con particolare riguardo agli obblighi di trasparenza, il Garante ha ribadito la necessità di rendere pubbliche, per tutta la durata dello studio, le informazioni da fornire agli interessati, deceduti e non contattabili, attraverso una specifica inserzione sui siti internet del promotore e dei centri di sperimentazione coinvolti nello studio, secondo quanto previsto dagli artt. 14, par. 5, lett. b), RGPD e 6, comma 3, delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica (all. A.5 del Codice), al fine di assicurare l'autodeterminazione informativa dei pazienti non contattabili e, se del caso, anche dei loro aventi causa (provv.ti 24 gennaio 2024, n. 36, doc. web n. 9988614; 7 marzo 2024, n. 132, doc. web n. 10007008; 7 marzo 2024, n. 157, doc. web n. 10009033).

In taluni provvedimenti, il Garante ha riaffermato, secondo un orientamento ormai consolidato, che l'anonimizzazione deve essere considerata un trattamento dinamico da valutare in ragione dei differenti criteri indicati nel cons. 26 del RGPD e, segnatamente, delle concrete finalità che il titolare intende perseguire con i dati all'esito della loro anonimizzazione. Più nel dettaglio, si è detto che il rischio di re-identificazione degli interessati può variare a seconda che l'anonimizzazione sia effettuata al solo scopo di archiviazione delle informazioni trattate, ovvero di ulteriore utilizzazione delle stesse, eventualmente in combinazione con altre informazioni o anche per un'eventuale condivisione dei dati con la comunità scientifica. In ogni caso, sia in ipotesi di archiviazione che di condivisione dei dati anonimizzati, il titolare del trattamento è tenuto ad impegnarsi a rimuovere ogni singolarità, qualora, con qualsiasi mezzo, ne venga a conoscenza in una fase successiva all'anonimizzazione e a tenere traccia di tali eventi in modo da ripetere la valutazione del rischio di re-identificazione al raggiungimento di una soglia predefinita, adeguata rispetto al contesto, individuata sul totale di *record* inclusi nella banca dati.

Al riguardo, il Garante ha altresì chiarito che, in caso di diffusione dei dati in forma anonima, il titolare del trattamento deve indicare nella valutazione di impatto le considerazioni svolte in ordine al rischio di re-identificazione degli interessati, evidenziando sul punto che un numero elevato di statistiche aggregate aumenta il potere identificativo

di ciascuna di esse, fino alla possibile completa ricostruzione di un *dataset* (cd. *reconstruction attack*). Pertanto, al fine di evitare tale rischio, è necessario che il numero delle statistiche oggetto di diffusione sia significativamente inferiore rispetto al numero delle variabili che si intendono divulgare (provv.ti 24 gennaio 2024, n. 36, doc. web n. 9988614; provv. 7 marzo 2024, n. 132, doc. web n. 10007008; provv. 7 marzo 2024, n. 157, doc. web n. 10009033; provv. del 24 aprile 2024, n. 242, doc. web n. 10018511).

Inoltre, si segnala che in tre dei richiamati pareri, favorevoli ma condizionati (provv.ti 7 marzo 2024, n. 132, doc. web n. 10007008; 24 aprile 2024, n. 242, doc. web n. 10018511; 24 aprile 2024, n. 300, doc. web n. 10036817) il Garante ha prescritto ai titolari del trattamento di implementare ulteriori e più robuste misure tecniche, per assicurare *by design* piena effettività al principio di esattezza dei dati, che ne garantisce anche la qualità. Ad esempio, in caso di raccolta dei dati dei pazienti arruolati sul foglio *excel*, esso dovrà almeno essere firmato digitalmente attraverso un *hash* e la firma digitale così generata dovrà essere detenuta da un soggetto diverso da quello addetto alla raccolta dei dati. Tale misura, infatti, nell'intento di rafforzare l'esattezza e la qualità dei dati raccolti nei fogli *excel*, è idonea soprattutto ad assicurare che eventuali successive alterazioni degli stessi siano rapidamente rilevate e corrette.

In due dei richiamati pareri, il Garante si è soffermato più precisamente sul trattamento dei dati genetici. In un caso, ha prescritto ai titolari di integrare la valutazione di impatto con una specifica sezione dedicata al trattamento dei dati genetici con l'indicazione delle misure implementate, alla luce dei rischi considerati conformemente allo specifico quadro normativo vigente (v. le prescrizioni relative al trattamento dei dati genetici, all. n. 4 al provv. 5 giugno 2019, n. 146, doc. web n. 9124510) e di integrare altresì le informative predisposte ai sensi degli artt. 13 e 14 del RGPD, facendo espresso riferimento al trattamento dei dati genetici e agli elementi previsti ai punti 4.3 e 4.11.1 delle citate prescrizioni relative al trattamento dei dati genetici (provv. 24 aprile 2024, n. 300, doc. web n. 10036817); nell'altro invece, ha stabilito che nell'informativa sul trattamento dei dati siano anche indicate le modalità di riscontro alle istanze di accesso da parte degli interessati alle informazioni contenute nel progetto di ricerca secondo quanto previsto al punto 4.11.1 delle citate prescrizioni relative al trattamento dei dati genetici (provv. 24 aprile 2024, n. 242, doc. web n. 10018511).

Il Garante si è espresso altresì su uno studio retrospettivo osservazionale denominato "Intelligenza artificiale per la definizione di nuove signature e modelli per la personalizzazione delle strategie di preservazione d'organo del cancro laringeo e ipofaringeo - PRESERVE". In relazione alla fase di "sviluppo di un algoritmo predittivo", l'Autorità ha valutato positivamente, da una parte, la motivata indispensabilità anche di informazioni riferite a soggetti deceduti e non contattabili in assenza delle quali il campione selezionato sarebbe stato incompleto creando di conseguenza, come rappresentato nella richiesta di parere, possibili *bias* nello sviluppo dell'algoritmo stesso e, quindi, nella qualità delle capacità predittive.

Ancora, in merito agli obblighi di trasparenza, il Garante ha ritenuto necessario che il titolare del trattamento rappresentasse nelle informative rese ai sensi degli artt. 13 e 14 del RGPD, con un linguaggio semplice e chiaro, la finalità del progetto di ricerca consistente nell'implementazione di un algoritmo; in aggiunta, per altro aspetto, in considerazione dell'impiego di sistemi di IA, ha altresì prescritto al titolare di pubblicare sul proprio sito internet istituzionale la valutazione di impatto, anche solo per estratto, integrata dalla puntuale elencazione dei modelli matematici statistici adoperati per elaborare i dati e dall'indicazione delle logiche algoritmiche utilizzate. Il Garante ha

inoltre prescritto al medesimo titolare di applicare, al termine del periodo di conservazione dei dati per lo svolgimento dello studio e comunque in ipotesi di condivisione dei dati con soggetti terzi, le sopra richiamate misure volte a prevenire la re-identificazione degli interessati (provv. 24 gennaio 2024, n. 36, doc. web n. 9988614).

6.3. *L'art. 110*-bis*, comma 4, del Codice*

Il Garante ha adottato apposite FAQ sui presupposti giuridici e principali adempimenti per il trattamento da parte degli istituti di ricovero e cura a carattere scientifico (IRCCS) dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca, fornendo sintetici chiarimenti in ordine all'art. 110-*bis*, comma 4, del Codice.

Gli IRCCS sono enti del SSN a rilevanza nazionale dotati di autonomia e personalità giuridica che, secondo standard di eccellenza, perseguono finalità di ricerca nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari ed effettuano prestazioni di ricovero e cura di alta specialità (v. art. 1, d.lgs. n. 288/2003).

Più precisamente, è stato rappresentato che, in forza dell'art. 110-*bis*, comma 4, del Codice, gli IRCCS godono di una base normativa per trattare i dati sulla salute raccolti originariamente per scopi di cura a fini ulteriori di ricerca scientifica, senza dovere acquisire uno specifico consenso da parte degli interessati e senza dover effettuare alcuna comunicazione preventiva al Garante, tenuto anche conto della specifica disciplina di settore che ne vincola l'attività a uno stretto controllo da parte del Ministero della salute e al rispetto di elevati standard etici e metodologici (art. 8, d.lgs. n. 288/2003).

Invero, il Garante ha chiarito che l'art. 110-*bis*, comma 4, del Codice costituisce una di quelle disposizioni di legge che si inseriscono nello spazio di normazione lasciato agli Stati membri, ai sensi dell'art. 9, par. 2, lett. j), RGPD. Di conseguenza, qualora gli IRCCS fondino l'ulteriore trattamento dei dati inizialmente raccolti per finalità di cura per successivi scopi di ricerca sull'art. 110-*bis*, comma 4, del Codice, questi sono chiamati obbligatoriamente a svolgere e pubblicare, se necessario anche solo per estratto, la valutazione d'impatto sui propri siti web. Il mancato adempimento di tali obblighi comporta l'applicazione di una sanzione amministrativa, ai sensi dell'art. 166, comma 1, del Codice e dell'art. 83, par. 4, RGPD.

6.4. *Le regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*

Nell'anno di riferimento, il Garante ha adottato la deliberazione di promovimento delle nuove regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-*quater* e 106 del Codice. Le regole deontologiche costituiscono un atto normativo idoneo a incidere sulla liceità e correttezza dei trattamenti promosso dagli operatori del settore, rispetto al quale l'Autorità si limita ad operare una verifica di conformità con il quadro normativo vigente in materia di protezione dei dati personali, oltre che a provvedere alla loro formale promulgazione. Esse sono pertanto promosse nel rispetto del principio di rappresentatività, la cui effettiva applicazione è in concreto verificata dal Garante secondo quanto indicato nel reg. del Garante n. 1/2019 (doc. web n. 9107633), specialmente rispetto a quanto è in esso disposto dagli artt. 23 e ss. (provv. 9 maggio 2024, n. 298, doc. web n. 10016146).

A seguito della predetta deliberazione, l'Autorità ha verificato l'appartenenza alla categoria dei soggetti interessati ovvero a quella dei portatori di un interesse qualificato

dei numerosi soggetti che hanno manifestato il proprio interesse a partecipare alla redazione delle regole, e ha dato avvio alle riunioni di lavoro preordinate all'analisi del relativo schema preliminare (artt. 23, comma 2, 24 e 25 del reg. del Garante n. 1/2019, cit.). Al tavolo di lavoro per la redazione delle regole partecipano enti e istituti di ricerca, pubbliche amministrazioni, università, istituti di ricovero e cura a carattere scientifico, enti del terzo settore, comitati etici, ma anche enti rappresentativi degli interessati i cui dati potrebbero essere coinvolti nei trattamenti che verranno disciplinati come associazioni di malati.

6.5. *Altri provvedimenti in materia di trattamenti per scopi di ricerca scientifica*

Tra gli altri provvedimenti adottati dal Garante in materia di trattamento per scopi di ricerca scientifica, merita di essere evidenziato quello sanzionatorio e correttivo adottato nei confronti di un IRCCS, a seguito di specifici accertamenti ispettivi (provv. 17 luglio 2024, n. 473, doc. web n. 10057629).

Il Garante ha rilevato l'illiceità del trattamento di dati personali effettuato dall'IRCCS in questione, in quanto svolto in violazione dei principi di protezione dei dati, in particolare quelli di liceità, di limitazione della conservazione, di *accountability*, di *privacy by design* e *by default*, e in violazione degli obblighi di trasparenza e dell'obbligo di svolgere la valutazione d'impatto (art. 5, par. 1, lett. e), par. 2, art. 9, par. 2, lett. j), art. 14, par. 5, lett. b), art. 25 e art. 35 del RGPD, nonché artt. 110, comma 1, prima parte, e 110-*bis*, comma 4, del Codice, e art. 6, comma 3, delle regole deontologiche).

Con riferimento al principio di liceità del trattamento di cui all'art. 5, par. 1, lett. a), RGPD, la violazione accertata riguarda i trattamenti di dati personali relativi ai soggetti deceduti o non contattabili arruolati negli studi retrospettivi svolti dall'istituto nell'ambito delle proprie linee di ricerca, nella misura in cui quest'ultimo, quale titolare, ha sistematicamente omesso di svolgere e pubblicare la valutazione di impatto, adempimenti in tal caso obbligatori, ai sensi degli artt. 9, par. 2 lett. j), RGPD nonché 110, comma 1, prima parte e 110-*bis*, comma 4, del Codice. Per altro verso, con riferimento ai pazienti contattabili, il Garante ha accertato l'inidoneità del consenso – in particolare in punto di specificità – a consentire i trattamenti per le finalità di ricerca scientifica, in quanto il modulo di richiesta del consenso si limitava a individuare macro-finalità della ricerca stessa e non uno specifico progetto.

Inoltre, tale consenso non essendo preceduto da un'informativa completa di tutti i suoi elementi, si è accertata la violazione dei principi di trasparenza e di correttezza di cui all'art. 5, par. 1, lett. a), RGPD in quanto l'informativa è stata considerata atta a ingenerare negli interessati confusione in ordine alla sorte dei propri dati, in violazione del principio di autodeterminazione informativa e dunque di correttezza e trasparenza (artt. 13 del RGPD; cfr. punti 23 e ss. delle linee guida sulla trasparenza ai sensi del RGPD, adottate dal WP29 il 29 novembre 2017, versione emendata adottata l'11 aprile 2018).

Con specifico riferimento al periodo di conservazione dei dati, il Garante ha accertato la violazione dell'art. 5, par. 1, lett. e), RGPD, in quanto, nelle informative rese agli interessati in fase di accettazione presso la struttura ospedaliera, era previsto che il tempo di conservazione dei dati trattati per scopi di ricerca sarebbe stato indicato nei relativi protocolli; tuttavia, non solo questo tempo non era definito (quanto meno nei protocolli relativi agli studi esaminati nel corso del procedimento e neppure nei documenti informativi indirizzati agli interessati) ma non venivano neanche indicati i criteri per la relativa determinazione.

La sistematica, e già rilevata, omissione dello svolgimento di una valutazione d'impatto

e l'inidoneità delle informative rese sia direttamente agli interessati, ove intervenissero elementi ulteriori rispetto a quelli già rappresentati, sia attraverso la loro pubblicazione, qualora gli interessati risultassero deceduti o non contattabili, ha condotto il Garante ad accertare la violazione dell'art. 35 del RGPD, in quanto l'istituto non ha tenuto in debita considerazione la centralità dell'approccio basato sul rischio imposto dal RGPD, nonché dell'art. 14, par. 5, lett. b), RGPD e dell'art. 6, comma 3, delle regole deontologiche, ribadendo che il titolare del trattamento ha l'obbligo di rendere preventivamente una specifica informativa rispetto ad ogni singolo progetto di ricerca.

Più in generale, è stata accertata la violazione dei principi di responsabilizzazione e di *privacy by design* di cui agli artt. 5, par. 2 e 25 del RGPD, avendo l'IRCCS dato prova di una condotta inidonea a garantire l'effettiva applicazione dei principi di protezione dei dati personali attraverso l'implementazione e il constante riesame e aggiornamento di misure specifiche, adeguate e misurabili anche in relazione al particolare contesto del trattamento e ai correlati rischi per i diritti e le libertà degli interessati.

Alla luce delle violazioni accertate, il Garante, in aggiunta alla sanzione amministrativa pecuniaria, ha ingiunto al titolare di conformare i trattamenti alle disposizioni del RGPD adottando specifiche misure correttive.

Dati sintetici

Nell'ambito delle cd. *privacy enhancing technology* (PET), quella dei dati sintetici sta suscitando particolare interesse da parte degli operatori del settore. I cd. dati sintetici sono dati generati in modo artificiale e capaci di riprodurre fedelmente le caratteristiche e i comportamenti dei dati reali, senza tuttavia contenerli. Per tale ragione sono sempre più numerosi gli enti pubblici e privati, titolari del trattamento, intenzionati ad investire in tale tecnologia anche al fine di poter svolgere analisi di dati assistiti da robuste misure di protezione.

L'Autorità si è pertanto dedicata a una specifica attività ispettiva e conoscitiva nei confronti di una società che offre ai propri clienti uno strumento di sintetizzazione operante sui *dataset* di cui questi ultimi sono titolari del trattamento, mettendo a disposizione degli stessi una piattaforma che genera i dati sintetici. Gli accertamenti erano finalizzati ad approfondire la conoscenza di tale processo applicato ai trattamenti svolti per scopi di ricerca scientifica verificandone la conformità ai principi di protezione dei dati personali, con particolare riguardo a quelli di minimizzazione e di esattezza dei dati.

7 La statistica

7.1. *La statistica ufficiale*

Programma statistico nazionale

Il Garante si è espresso favorevolmente sul lavoro statistico EMR-00028 "Rilevazione delle tipologie e caratteristiche dei clienti negli esercizi ricettivi", inserito nel PSN 2020-2022 e in quello 2023-2025 (provv. 22 febbraio 2024, n. 93, doc. web n. 9994638), precedentemente sospeso con il parere sullo schema di Programma statistico nazionale 2020-2022, aggiornamento 2022 (provv. 30 giugno 2022, n. 237, doc. web n. 9794929).

Atteso che le richiamate informazioni erano apparse non necessarie alle strutture ricettive per l'esecuzione dei relativi contratti, il Garante aveva rilevato specifiche criticità in ordine alle basi giuridiche del trattamento e al corretto inquadramento dei ruoli soggettivi attribuiti alle strutture ricettive e all'ufficio di statistica della Regione Emilia Romagna (artt. 6, 12, 13, 24, 28 del RGPD).

A tale riguardo, è stato chiarito che l'ufficio di statistica della Regione non raccoglie dati direttamente presso gli interessati ma presso le strutture ricettive che, agendo in qualità di autonomi titolari del trattamento, acquisiscono dati per l'esecuzione del contratto di ospitalità o sulla base del consenso degli interessati per altre finalità. Il Garante, quindi, viste le modifiche apportate alla scheda informativa del lavoro statistico e i chiarimenti resi, verificati anche altri aspetti di protezione dei dati quali, in particolare, la conformità dei tempi di conservazione, ha ritenuto che nulla osti alla realizzazione del richiamato lavoro.

INPS

Merita di essere evidenziato altresì il provvedimento, sanzionatorio e correttivo, reso nei confronti dell'INPS, a seguito degli accertamenti ispettivi svolti al fine di verificare l'osservanza da parte del relativo ufficio di statistica delle disposizioni in materia di protezione dei dati personali, con particolare riferimento alla corretta applicazione dei principi applicabili al trattamento e alle misure di cui all'art. 89 del RGPD (provv. 13 novembre 2024, n. 674, doc. web n. 10090499).

In tale provvedimento, il Garante ha accertato l'illiceità del trattamento di dati personali effettuato dall'INPS in violazione dell'art. 5, par. 1, lett. c), e par. 2, e degli artt. 25 e 35 del RGPD, nonché, con specifico riferimento al lavoro statistico IPS-00081, dell'obbligo di rendere un'informativa esatta e completa ai sensi dell'art. 14 del RGPD. In relazione alla raccolta dal *data warehouse* dell'Ente di dati direttamente identificativi degli interessati, segnatamente attraverso l'indicazione del codice fiscale, il Garante, nell'accertare la violazione dei principi di minimizzazione e di *privacy by design*, ha ribadito la centralità della pseudonimizzazione dei dati alla luce dell'art. 89, par. 1, RGPD, in quanto misura che, nel far salva la possibilità per il titolare di risalire all'identità dell'interessato laddove necessario, favorisce un equo contemperamento con i principi di protezione dei dati, ivi inclusi quelli di limitazione della finalità e della conservazione (cfr. anche provv. 23 gennaio 2020, n. 10, doc. web n. 9261093 e provv. 16 settembre 2021, n. 315, doc. web n. 9717477, punto 3). Alla luce delle violazioni accertate, il Garante, in aggiunta alla sanzione amministrativa pecuniaria, ha altresì ingiunto al titolare di conformare i trattamenti alle disposizioni del RGPD adottando specifiche misure correttive.

8 I trattamenti in ambito giudiziario e di sicurezza

8.1. *Trattamenti in ambito giudiziario*

Pubblicazione di sentenze recanti dati sensibili e giudiziari

Di assoluto rilievo nell'anno è stato il procedimento avviato d'ufficio dall'Autorità nei confronti della Corte di cassazione. Il caso trae origine da un ricorso presentato, dinanzi al Tribunale di Roma ai sensi dell'art. 152 del Codice, da un interessato nei confronti del Ministero della giustizia e trasmesso da quest'ultimo all'Autorità al fine di acquisire elementi utili alla difesa in giudizio. In particolare il ricorso era volto ad ottenere la deindicizzazione del nominativo del ricorrente dal portale SentenzeWeb della Suprema Corte che consente la libera consultazione degli archivi delle sentenze civili e penali della Cassazione. Il ricorrente aveva altresì rappresentato che nel portale era possibile effettuare una ricerca nominale per malattia o patologia dell'interessato. A seguito degli accertamenti istruttori effettuati dall'Autorità è emerso che la Suprema Corte, in taluni casi, nel pubblicare i provvedimenti giurisdizionali sul predetto portale, aveva divulgato dati identificativi di persone offese da atti di violenza sessuale e di soggetti affetti da HIV o da altre patologie, in violazione degli artt. 52, comma 5, e 2-*septies* del Codice e del divieto di diffusione di dati cui all'art. 9 del RGPD, nonché in maniera non conforme ai principi di liceità e di minimizzazione dei dati di cui all'art. 5, par. 1, lett. a) e c), RGPD. Il Garante, valutate le risultanze istruttorie e la collaborazione prestata dalla stessa Corte nel corso del procedimento, ha adottato un provvedimento correttivo di ammonimento, unitamente ad alcune richieste di informazioni su specifici profili relativi all'implementazione delle misure organizzative e di sicurezza, riscontrate dalla Corte (provv. 9 maggio 2024, n. 435, doc. web n. 10054644).

Con provvedimento 9 maggio 2024, n. 296 (doc. web n. 10027814), il Garante ha accertato che un avvocato, in qualità di titolare del trattamento, aveva violato la disposizione di cui all'art. 12, par. 3, RGPD, non avendo rispettato il termine di trenta giorni per fornire all'interessato le informazioni relative all'azione intrapresa ai sensi degli artt. da 15 a 22 del RGPD né comunicato all'interessato la necessità della proroga del termine per il riscontro alla richiesta di informazioni e dei motivi del ritardo, entro un mese dal ricevimento della richiesta, come previsto dal predetto art. 12. In considerazione dell'assenza di precedenti violazioni pertinenti commesse dallo stesso titolare, della lievissima entità del danno subito dall'interessato nonché dell'insussistenza di eventuali fattori aggravanti (quali benefici finanziari conseguiti o perdite evitate, direttamente o indirettamente, quale conseguenza della violazione), l'Autorità non ha ritenuto di infliggere una sanzione amministrativa pecuniaria ma, in ragione dell'accertata illiceità del trattamento, ha ammonito l'avvocato ai sensi dell'art. 58, par. 2, lett. b), RGPD.

Trattamenti in ambito forense

Con provvedimento 19 dicembre 2024, n. 804 (doc. web 10113493) il Garante ha altresì accertato l'illiceità del trattamento dei dati personali dell'interessato effettuato da un avvocato, in violazione delle disposizioni di cui agli artt. 5, comma 1, lett. a), 6 e 10 del RGPD, nonché 2-*octies* del Codice, comminandogli l'ammonimento. Nella specie il legale aveva notificato un'intimazione di pagamento contenente l'atto di precetto e il titolo esecutivo costituito dalla sentenza penale di condanna, tramite PEC inviata

all'indirizzo del protocollo dell'azienda ospedaliera presso cui l'interessato prestava servizio, così comunicando ad una pluralità di destinatari i dati personali, anche giudiziari, dell'interessato in assenza di una idonea base giuridica e dunque in violazione delle condizioni di liceità del trattamento.

Nel 2024 sono stati presentati all'attenzione del Garante numerosi reclami o segnalazioni concernenti la produzione di informazioni in giudizio, rispetto ai quali si è provveduto a dichiarare, con provvedimento dirigenziale di archiviazione, l'incompetenza del Garante, secondo un orientamento ormai consolidato. Infatti, l'art. 160-*bis* del Codice stabilisce che la validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali. In proposito, l'Autorità ha costantemente ricordato che, al fine di salvaguardare l'indipendenza della magistratura nell'adempimento dei suoi compiti giurisdizionali (cfr. cons. 20 del RGPD), il Garante non è competente per il controllo dei trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni giurisdizionali (cfr. artt. 55, par. 3, RGPD, 37, comma 6, d.lgs. n. 51/2018 e 154, comma 7, del Codice).

8.2. *Trattamenti da parte di forze di polizia*

Merita di essere menzionato il provvedimento 20 giugno 2024, n. 371 a mezzo del quale il Garante, a seguito di numerose segnalazioni, ha adottato la misura correttiva dell'ammonimento nei confronti del Ministero dell'interno - Dipartimento della pubblica sicurezza in relazione ad un caso concernente la diffusione di immagini dell'interessato in stato di detenzione da parte di una questura. Più nel dettaglio le predette segnalazioni avevano riguardato la divulgazione su diversi siti internet, giornali *online*, *blog* e pagine *social*, di uno scatto fotografico, che riproduceva una persona arrestata in attesa di essere fotografata a fini segnaletici negli uffici della polizia scientifica, affiancata in alcuni casi da un agente di polizia (doc. web n. 10090430).

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

Per quanto riguarda l'attività consultiva del Garante su schemi di decreto ministeriali non aventi natura regolamentare o di altri atti amministrativi generali, ai sensi degli artt. 36, par. 4, RGPD, 154, comma 5-*bis*, del Codice, e 37, comma 4, d.lgs. n. 51/2018, nonché su schemi di convenzione ai sensi dell'art. 47, comma 1, d.lgs. n. 51/2018, il Garante, nel corso del 2024, ha espresso i seguenti pareri:

a) parere 9 maggio 2024, n. 291, doc. web n. 10026254, su uno schema di convenzione tra "il Dipartimento della pubblica sicurezza e il Dipartimento per gli affari interni e territoriali del Ministero dell'interno per disciplinare l'accesso ai dati ed alle informazioni contenuti nella banca dati ANPR - Anagrafe della popolazione residente". A seguito dell'istruttoria, particolarmente complessa, è stato adottato uno schema conclusivo su cui il Garante ha espresso parere favorevole;

b) parere 6 giugno 2024, n. 434, doc. web n. 10050361, su uno schema di decreto del Direttore generale della Direzione generale dei sistemi informativi automatizzati (DGSIA) del Ministero della giustizia, recante le specifiche tecniche del processo telematico civile e penale, in attuazione di quanto previsto dall'art. 34 del decreto del Ministro della giustizia 21 febbraio 2011, n. 44, come da ultimo novellato dal decreto 29 dicembre 2023, n. 217. Il provvedimento disciplina le infrastrutture informatiche del sistema

digitale giustizia, le modalità di trasmissione e consultazione di atti e documenti informatici nel processo civile e penale e i pagamenti telematici. Il Ministero ha rappresentato che l'adozione di nuove specifiche tecniche si è resa necessaria a seguito della riforma dei codici di rito, effettuata con i decreti legislativi delegati 10 ottobre 2022 n. 149 e n. 150. Il Garante – preso atto delle integrazioni apportate al testo nel corso della complessa istruttoria – ha espresso parere condizionato alla riformulazione in senso conforme ai principi in materia di protezione dei dati personali di una disposizione relativa alle informazioni da rendere nell'area pubblica del portale dei servizi telematici del Ministero della giustizia. Nel provvedimento in esame, l'Autorità ha altresì individuato ulteriori profili di criticità sul piano applicativo del sistema del processo telematico, che necessitano della pianificazione ed attuazione di misure tecniche e organizzative necessarie a incrementare il livello di sicurezza dei servizi e dei sistemi informatici;

c) parere 20 giugno 2024, n. 368, doc. web n. 10043511, su uno schema di decreto del Ministro della salute, di concerto con il Ministro della giustizia, in materia di oblio oncologico e procedimento di adozione di minori, ai sensi dell'art. 3, comma 2, l. 7 dicembre 2023, n. 193, concernente le modalità di attuazione delle disposizioni della l. n. 184/1983, in materia di adozioni, espressamente modificate dalla l. n. 193/2023. Nel corso dell'istruttoria propedeutica all'adozione del parere, il Garante ha chiesto di apportare alcune modifiche al testo originario. In particolare, un primo schema del decreto prevedeva che i soggetti titolari del diritto di oblio oncologico che presentavano la domanda di adozione avrebbero dovuto produrre, unitamente al certificato di sana e robusta costituzione rilasciato dalla azienda sanitaria competente, il certificato di oblio oncologico; tuttavia, ciò avrebbe comportato l'ostensione dell'informazione relativa alla pregressa malattia oncologica, ancorché già soggetta ad oblio, il che, in assenza di un apparente giustificato motivo, appariva non in linea con il principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c), RGPD e con lo spirito stesso della riforma normativa sull'oblio oncologico.

L'ostensione del certificato di oblio oncologico al Tribunale dei minorenni sarebbe giustificata, invece, qualora l'oblio oncologico maturasse dopo la conclusione delle indagini sanitarie da parte della azienda sanitaria. Nella bozza definitiva il Ministero ha recepito le osservazioni del Garante, prevedendo che i soggetti che presentano domanda di adozione, a qualsiasi titolo, se sono stati pazienti oncologici e sono maturati i termini previsti dall'art. 22, comma 4, secondo periodo, l. 4 maggio 1983, n. 184, producono alla azienda sanitaria competente nel procedimento di adozione il certificato di oblio oncologico previsto dal decreto del Ministro della salute adottato ai sensi dell'art. 5, comma 1, l. 7 dicembre 2023, n. 193. Qualora l'oblio oncologico maturi dopo la conclusione delle indagini sanitarie da parte della azienda sanitaria, il certificato di oblio oncologico è depositato presso il Tribunale dei minori competente per l'adozione. Il certificato di oblio oncologico preclude di attribuire, nel procedimento di adozione, qualsiasi conseguenza alla patologia oncologica;

d) parere 18 luglio 2024, n. 464, doc. web n. 10063581, su tre schemi di provvedimenti del direttore della Direzione generale dei sistemi informativi automatizzati (DGSIA) del Ministero della giustizia contenenti specifiche tecniche in materia di aste giudiziarie con modalità telematiche. Il Garante ha espresso parere favorevole, richiedendo tuttavia alcune integrazioni per rendere i provvedimenti aderenti alla disciplina della protezione dei dati personali, in particolare sull'adozione di meccanismi per attenuare il rischio connesso all'attivazione fraudolenta di identità digitali SPID o certificati di autenticazione CNS intestati a utenti esterni, sull'implementazione di misure di sicurezza per l'accesso degli utenti interni alla banca dati, sulla definizione dei profili di autorizzazione delle

diverse tipologie di utenti, sulla precisazione delle responsabilità del soggetto legittimato alla pubblicazione degli avvisi di vendita e sull'adozione di *disclaimer* per ricordare ai soggetti legittimati alla pubblicazione degli avvisi di vendita di adottare adeguate misure per rimuovere dalla documentazione allegata le generalità e gli altri dati identificativi delle persone fisiche a cui appartenevano i beni mobili o immobili oggetto dell'asta o di soggetti terzi;

e) parere 18 luglio 2024, n. 466, doc. web n. 10064748, su uno schema di decreto direttoriale interministeriale interno (Commissione asilo) - giustizia (Direzione generale dei sistemi informativi e automatizzati), avente ad oggetto l'individuazione delle specifiche tecniche per la messa a disposizione, nella fase giurisdizionale di merito, della videoregistrazione dei colloqui dei richiedenti asilo (cd. progetto S.IN.D.A.C.A. - Sistema informativo di documentazione delle audizioni delle Commissioni asilo). Il Garante si è espresso in senso favorevole sul testo sottoposto al suo esame, ritenendo adeguate le misure tecniche e organizzative individuate, ma ponendo una condizione in merito alla necessità di individuare termini certi di conservazione dei dati personali trattati;

f) parere 26 settembre 2024, n. 579, doc. web n. 10072013, su uno schema di decreto del Ministero della giustizia contenente disposizioni in tema di distruzione di atti e documenti originali analogici depositati nei procedimenti giudiziari civili definiti con provvedimento decisorio non più soggetto a impugnazione da almeno un anno, in ottemperanza alle disposizioni previste dall'art. 22, comma 4-*bis*, del CAD. Tale disposizione assume particolare rilevanza nel tracciare il percorso del Ministero della giustizia verso la transizione digitale, disponendo che le copie su formato digitale di tali atti sono idonee ad assolvere agli obblighi di conservazione previsti dalla legge se il cancelliere vi appone la firma digitale, ne attesta la conformità all'originale e le inserisce nel fascicolo informatico nel rispetto della normativa anche regolamentare concernente il processo civile telematico. All'esito di una articolata istruttoria, il Garante ha espresso parere favorevole sullo schema di decreto, richiedendo tuttavia all'amministrazione di modificare l'art. 3 dello schema, recante indicazioni sul trattamento di dati personali, ampliando il vincolo di conformità a tutte le disposizioni del RGPD e del Codice ed esplicitando il riferimento alle pertinenti regole deontologiche applicabili ai trattamenti in questione.

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

A seguito di reclami e segnalazioni, anche nel 2024 l'Autorità, limitatamente alle sue competenze in tale ambito, ha assicurato il riscontro da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e di uffici periferici di polizia alle richieste degli interessati, sia di accesso e comunicazione dei dati conservati presso il CED, sia di eventuale rettifica degli stessi, nel rispetto delle disposizioni previste dall'art. 10 della l. n. 121/1981, cui fanno rinvio gli artt. 47 e 48 del d.lgs. n. 51/2018.

8.5. *Il controllo sul Sistema di informazione Schengen*

Come è noto, successivamente all'eliminazione dei controlli alle frontiere interne dell'UE, il Sistema di informazione Schengen (SIS) permette alle autorità nazionali di polizia, di controllo delle frontiere e doganali di scambiarsi agevolmente informazioni sulle persone che potrebbero essere coinvolte in reati gravi, oltre a conservare segnalazioni su persone scomparse e informazioni su varie tipologie di beni potenzialmente rubati, sottratti o smarriti. Il SIS è disciplinato attualmente dal reg.

(UE) 2018/1861, che è entrato in vigore il 7 marzo 2023, con riguardo alle attività di controllo alle frontiere, e dal reg. (UE) 2018/1862, anch'esso entrato in vigore il 7 marzo 2023, relativamente alla cooperazione giudiziaria e di polizia.

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

Nella Relazione 2023 si è dato conto degli esiti dalla valutazione Schengen dell'Italia condotta nel 2021 con il *report* finale della Commissione europea giunto nell'ottobre del 2023, a seguito del quale l'Autorità ha svolto una attività ispettiva nell'ambito dei controlli quadriennali previsti dall'art. 55 del reg. 2018/1861. Le attività di verifica e di *audit* hanno evidenziato, nel complesso, una situazione di sostanziale conformità al quadro normativo di riferimento. Sono stati, tuttavia, rilevati alcuni profili di criticità.

8.5.2. L'attività di controllo e monitoraggio sul SIS

Nel 2024 è proseguita l'attività di controllo e monitoraggio dei trattamenti su dati registrati nella sezione nazionale del Sistema di informazione Schengen in relazione agli obblighi in capo al Dipartimento della pubblica sicurezza del Ministero dell'interno, titolare del trattamento, e all'esercizio dei diritti riconosciuti agli interessati. Sotto quest'ultimo profilo, il Ministero invia trimestralmente all'Autorità *report* statistici, privi di dati di natura personale, contenenti informazioni di dettaglio (nazionalità dei richiedenti, uffici di polizia coinvolti, tipologia delle richieste, ecc.) idonee a monitorare il flusso delle istanze degli interessati e la conseguente attività di riscontro compiuta dal Dipartimento della pubblica sicurezza. Nel periodo di riferimento l'Autorità ha avviato le attività relative a un nuovo obbligo previsto dal mutato quadro normativo concernente il SIS, in particolare ai sensi dell'art. 54, par. 3, reg. 2018/1861 e dell'art. 68, par. 3, reg. 2018/1862. Questi ultimi prevedono che gli Stati membri debbano inviare ogni anno al CEPD un rapporto recante il numero di richieste di accesso, rettifica o cancellazione dei dati trattati nel SIS, il numero di richieste evase e, se presenti, il numero di ricorsi intrapresi dagli interessati per l'esercizio dei propri diritti o al fine di ottenere informazioni o ristori in relazione ad una segnalazione ad essi inerente, così come il numero di casi in cui l'Autorità giudiziaria abbia emanato una decisione favorevole al ricorrente. Il modello per la relazione annuale al CEPD, una volta ricevuto dal Ministero dell'interno nei termini previsti, è stato utilmente inoltrato dall'Autorità all'CEPD.

9 L'attività giornalistica

L'Autorità ha continuato a trattare questioni connesse alla libertà di manifestazione del pensiero attraverso la formulazione di giudizi di bilanciamento tra la libertà di informazione, da un lato, e il rispetto dell'identità personale e la protezione dei dati personali, dall'altro, esaminando un considerevole numero di reclami e segnalazioni concernenti la diffusione di notizie in rete e sui *social media* nonché da parte degli organi di informazione.

In termini generali, non vi sono state variazioni significative nel numero e nella tipologia delle istanze ricevute che hanno annoverato reclami e segnalazioni nonché comunicazioni di altra natura (in particolare, comunicazioni di notizie di reato da parte dell'Autorità giudiziaria con possibili risvolti in termini di normativa applicabile alla protezione dei dati). Come sempre, per alcune segnalazioni ricevute si è dato poi impulso a un'attività istruttoria secondo la procedura prevista per i reclami, avendo ravvisato gli estremi di possibili violazioni. Anche i destinatari delle istanze provenienti dagli interessati sono stati, come in passato, principalmente gestori di motori di ricerca e organi di informazione, con un numero minore di casi relativi a *social media*.

Con specifico riguardo all'esercizio dei diritti di cui agli artt. 15-22 del RGPD, è stata registrata, in diversi casi, l'adesione da parte dei titolari del trattamento alle richieste avanzate dai reclamanti, in tal modo consentendo, nella maggior parte delle fattispecie, la definizione dei reclami senza imporre alcuna misura correttiva al titolare.

In relazione alle fattispecie più critiche, che hanno necessitato l'intervento del Collegio, il Garante ha applicato anche misure sanzionatorie di tipo pecuniario, valutando con cura le peculiarità legate all'esercizio di tale potere correttivo in un ambito di particolare delicatezza quale quello della libertà di manifestazione del pensiero.

9.1. *Trattamento dei dati personali nell'esercizio dell'attività giornalistica*

9.1.1. Dati giudiziari

Rispetto al tema del trattamento dei dati giudiziari da parte di testate giornalistiche e siti di informazione, l'Autorità è intervenuta attraverso l'individuazione dei principi volti a garantire un proporzionato e corretto bilanciamento tra il trattamento dei dati in questione e la salvaguardia delle esigenze informative connesse a fatti di cronaca di pubblico interesse.

Non sono mancati casi in cui, pur reputando infondate le richieste di rimozione di dati personali riportati in articoli confluiti negli archivi di giornali per una legittima finalità di archiviazione di interesse storico-documentaristico, l'Autorità ha comunque ritenuto di dover accogliere le richieste di deindicizzazione in ragione del tempo trascorso e del mancato aggiornamento dei predetti dati; ad es. per via dell'evoluzione della vicenda giudiziaria descritta nell'articolo, conclusasi con esito favorevole nei confronti dell'interessato (*ex pluris*, provv. 7 marzo 2024, n. 142, doc. web n. 10007098).

Le medesime valutazioni sono state effettuate dal Garante in relazione ad un reclamo con cui è stata lamentata la pubblicazione, da parte di più editori, di una notizia relativa ad una vicenda giudiziaria risalente al 2017 e definitasi, rispetto al reclamante, nel 2018

con una sentenza di patteggiamento e con il beneficio della sospensione condizionale della pena. Pur non ritenendo di accogliere la richiesta di cancellazione del reclamante, è stata in ogni caso ritenuta fondata la misura della deindicizzazione, non risultando sussistere specifiche ragioni di interesse pubblico che, allo stato attuale, giustificassero una perdurante reperibilità dell'articolo contestato al di fuori dell'archivio dell'editore (provv. 22 febbraio 2024, n. 115, doc. web n. 10022424). Parimenti si è pronunciata l'Autorità, nell'ambito del medesimo reclamo, in relazione al trattamento di dati personali posto in essere all'interno della piattaforma Wikipedia, affermando così l'applicabilità nei confronti di quest'ultima della disciplina di cui agli artt. 136 e ss. del Codice (provv. 9 maggio 2024, n. 274, doc. web n. 10022403 - impugnato dinanzi al Tribunale di Matera).

9.1.2. Illecita diffusione di dati sanitari

L'Autorità è intervenuta in relazione alla diffusione di immagini raffiguranti persone affette da gravi patologie, ritenendo illecite tali pubblicazioni qualora, benché finalizzate a denunciare le difficili condizioni di vita dei malati, risultassero eccedenti e suscettibili di ledere la dignità dei medesimi.

Il Garante si è pronunciato, in particolare, su un reclamo presentato dall'amministratore di sostegno dell'interessata per lamentare la diffusione, avvenuta ad opera della madre all'interno di *social network* e in altri organi di comunicazione mediatica, di immagini e notizie riguardanti la salute e la vita privata della reclamante, compresi dettagli sui fatti di cronaca nera di cui quest'ultima era stata vittima, nonché di informazioni relative alle sue vicende processuali dinanzi al giudice tutelare. Alla luce di quanto emerso nel corso dell'istruttoria, il reclamo è stato dichiarato fondato limitatamente alla diffusione dei *post* pubblicati su *social network* ritraenti l'interessata senza alcuna forma di oscuramento e pertanto lesivi della sua dignità. Il reclamo è stato invece dichiarato infondato con riferimento ai contenuti degli altri *post* e alle restanti immagini la cui diffusione è stata ritenuta lecita in quanto espressione del diritto alla libera manifestazione del pensiero, qui finalizzata a denunciare, con modalità non lesive della dignità della reclamante, la qualità di vita della stessa (provv. 11 aprile 2024, n. 206, doc. web n. 10016102).

9.1.3. Dati relativi a minori

La tutela della dignità, della personalità e del diritto alla riservatezza dei minori, da sempre una priorità per il Garante, è stata orientata come di consueto al rispetto delle garanzie previste dalle regole deontologiche (art. 7) e dalla Carta di Treviso.

In tale contesto si colloca una segnalazione con la quale il Garante regionale dei diritti della persona presso la Regione Veneto aveva contestato la reperibilità sul sito di una rivista *online* di una sentenza concernente una controversia tra due comuni in ordine alle spese sostenute per il mantenimento di alcuni minori presso strutture socio-assistenziali. In particolare, tale sentenza era stata pubblicata in forma integrale, senza l'adozione di alcuna misura volta ad anonimizzare i dati identificativi dei minori ivi menzionati e riportando inoltre ulteriori informazioni quali i luoghi di residenza degli stessi, le strutture presso cui erano stati ospitati e i relativi periodi di permanenza. Pur avendo preso atto delle misure adottate dal titolare nel corso del procedimento per rimuovere gli effetti negativi derivanti dal lamentato trattamento, l'Autorità ha tuttavia ritenuto di disporre il divieto di ulteriore trattamento dei dati personali dei minori e di comminare al titolare una sanzione pecuniaria in ragione dell'accertata violazione dei principi di liceità e correttezza del trattamento e di minimizzazione dei dati, nonché del principio di essenzialità dell'informazione (provv. 4 luglio 2024, n. 441, doc. web n. 10052798).

Le disposizioni a tutela dei minori sono state altresì richiamate dall'Autorità con riguardo a casi in cui gli organi di informazione, nel riportare notizie su fatti che avevano coinvolto minorenni in qualità di vittime, non avevano provveduto ad assicurare nei confronti di questi ultimi un adeguato livello di tutela.

In questo senso il Garante si è pronunciato su un reclamo concernente la diffusione, durante una trasmissione radiofonica in cui venivano narrati episodi di bullismo, di dati identificativi di una minore vittima di tali episodi da parte di alcune coetanee, con conseguente esposizione della medesima al rischio di ritorsioni. In relazione a tale fattispecie è stata rilevata la violazione del principio dell'essenzialità dell'informazione, essendo stata ritenuta eccedente la diffusione di dati e dettagli tali da identificare la minore coinvolta nel fatto di cronaca. L'Autorità ha pertanto disposto nei confronti dell'emittente radiofonica il divieto di ogni ulteriore trattamento dei dati identificativi della minore, procedendo altresì ad irrogare una sanzione pecuniaria (provv. 23 maggio 2024, n. 365, doc. web n. 10109586).

Analoga esigenza di tutela è stata riscontrata dal Garante in relazione a una segnalazione con la quale era stato rappresentato che, mostrando stralci degli atti di un'inchiesta giudiziaria durante un telegiornale, erano stati resi noti i nomi di due minori vittime di uno stupro di gruppo, unitamente ai nominativi dei presunti autori. Pur avendo l'editore dichiarato di avere tempestivamente bloccato la diffusione del servizio sulle piattaforme *online* (causata da un errore nella fase di montaggio del servizio) e di avere incrementato i controlli interni, l'Autorità ha ritenuto di dover comunque ammonire il titolare del trattamento in ordine all'esigenza di adeguarsi integralmente alle disposizioni previste in materia di trattamento dei dati in ambito giornalistico, con particolare riguardo alle misure da adottare per salvaguardare la riservatezza di minori, tutelandone l'anonimato ove coinvolti, in qualsiasi veste, in fatti di cronaca (provv. 26 settembre 2024, n. 594, doc. web n. 10072054).

Sono altresì pervenuti all'Autorità reclami e segnalazioni, presentati da genitori di minorenni, aventi ad oggetto la pubblicazione non autorizzata da parte dell'altro genitore di immagini di minori all'interno di *social network*.

Al riguardo è stato valutato un reclamo con il quale una donna aveva lamentato la pubblicazione, realizzata dal precedente *partner* attraverso il proprio profilo Facebook e senza il consenso della reclamante, di una foto ritraente il figlio minore infraquattordicenne concepito dalla pregressa relazione tra i due. L'Autorità ha dichiarato il reclamo fondato, accertando l'illiceità del trattamento posto in essere dal precedente *partner* e rilevando che, nel caso di specie, la pubblicazione della foto del minore fosse avvenuta in mancanza del consenso rilasciato da entrambi i genitori e, pertanto, in assenza di un'idonea base giuridica del trattamento (provv. 13 novembre 2024, n. 681, doc. web n. 10076481).

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

Anche nel periodo di riferimento l'Autorità ha ribadito i principi fondamentali della disciplina relativa alla protezione dei dati personali in ambito giornalistico ed in particolare quello in base al quale la diffusione di dati personali per finalità giornalistiche e, più in generale, per finalità riconducibili alla libera manifestazione del pensiero (art. 136 del Codice) può prescindere dal consenso dell'interessato purché siano rispettati i limiti del diritto di cronaca a tutela dei diritti fondamentali della persona e segnatamente il limite della "essenzialità dell'informazione" riguardo a fatti di interesse pubblico (art. 137). Tale principio – espressione del principio generale di "minimizzazione" dei dati sancito dal RGPD (art. 5, par. 1, lett. c)) – viene richiamato anche nelle regole deontologiche in materia (artt. 6, 8, 10 e 11) e costituisce il parametro di orientamento del giornalista per un'informazione corretta e rispettosa dei diritti della persona.

In conformità ad esso l'Autorità ha ritenuto infondato un reclamo – presentato da un avvocato, in proprio e in qualità di amministratore di sostegno di un anziano – concernente alcuni servizi televisivi nei quali era stata narrata la vicenda del predetto anziano (noto benefattore nella comunità di sua residenza) e del suo ricovero in una struttura residenziale assistenziale, nonostante il suo dissenso. Il Garante, circoscritta la propria pronuncia ai dati della reclamante, essendo sopraggiunto il decesso dell'anziano-amministrato, ha ritenuto che la diffusione dei dati relativi alla amministratrice di sostegno (ovvero i dati identificativi, le videoriprese e le audio riprese ad essa riferite, nonché quelli inerenti al suo studio professionale), nell'ambito dell'attività giornalistica d'inchiesta rispetto ad una vicenda dal grande risalto mediatico (oggetto peraltro di una condanna dell'Italia da parte della Corte europea dei diritti dell'uomo n. 46412/21 del 6 luglio 2023), fosse conforme al principio di essenzialità dell'informazione. In tale contesto, si è tenuto conto del ruolo assunto dalla medesima reclamante nelle decisioni in merito agli interessi del suo assistito e della circostanza che la stessa avesse manifestato pubblicamente le proprie opinioni, rappresentando la propria posizione rispetto a ricostruzioni ritenute diffamatorie in quanto allusive a scelte non assunte nell'interesse e a tutela dell'amministrato, ma al solo fine di privarlo della sua libertà e di appropriarsi del suo ingente patrimonio (provv. 11 aprile 2024, n. 207, doc. web n. 10018487).

Analogamente, sulla base di una valutazione di conformità al parametro di essenzialità dell'informazione riguardo a fatti di interesse pubblico, l'Autorità ha ritenuto infondato un reclamo avente ad oggetto la diffusione, su un settimanale e sul relativo sito internet, di un articolo contenente una classifica, sulla base del reddito totale, di soggetti ricoprenti cariche pubbliche o comunque di nomina pubblica, tra i quali figurava – tra le prime posizioni – anche il reclamante. Il Garante ha al riguardo ricordato, come correttamente riportato nell'articolo in parola, che la trasparenza e la conoscibilità dei dati reddituali di tali figure è prevista dalla legge (artt. 2 e 12, l. n. 441/1982 e 5, d.lgs. n. 33/2013) anche quando la carica è esercitata a titolo gratuito, come nel caso di specie (provv. 17 luglio 2024, n. 447, doc. web n. 10063747).

9.2. *Trattamento di dati personali da parte dei motori di ricerca e deindicizzazione*

Anche nel 2024 sono stati numerosi i reclami proposti nei confronti dei gestori di motori di ricerca al fine di ottenere la deindicizzazione di contenuti con riferimento all'ambito della libertà di informazione.

La maggior parte delle richieste di *delisting* ha riguardato trattamenti posti in essere tramite il motore di ricerca gestito da Google LLC, ai quali non trova applicazione il meccanismo di cooperazione di cui agli artt. 56 ss. del RGPD, cui ha fatto seguito l'attivazione di altrettanti procedimenti. Diversamente, con riguardo alle società che gestiscono altri motori di ricerca – in particolare Microsoft Corporation con riferimento a Bing e Verizon Media con riguardo a Yahoo! – si è fatto ricorso, nei casi nei quali non vi sia stata adesione alle richieste nella fase istruttoria preliminare, all'avvio di un'interlocuzione diretta con l'autorità capofila nell'ambito del meccanismo di cooperazione.

L'ambito al quale risulta ascrivibile la maggior parte delle richieste di *delisting* è quello relativo ad articoli di stampa in cui sono riportate informazioni attinenti a vicende giudiziarie, più o meno recenti, riguardo alle quali gli interessati invocavano l'esercizio del diritto all'oblio ritenendo i contenuti superati dall'evoluzione del procedimento nel quale sono stati coinvolti, laddove favorevole, o comunque in ragione del tempo decorso rispetto ai fatti.

Dati giudiziari relativi a indagati o imputati

Si è posto il caso di un'istanza diretta ad ottenere la rimozione dell'associazione tra il nominativo dell'interessata ed alcuni risultati di ricerca che riconducevano ad articoli

recanti la notizia di reati gravi addebitati all'interessata e per i quali quest'ultima era stata condannata con sentenza confermata dal giudice di legittimità; tale circostanza, taciuta dall'interessata, era emersa, tuttavia, solo nel corso del procedimento attraverso le osservazioni rese dal titolare. L'Autorità, sulla base di un bilanciamento che ha tenuto conto, tra l'altro, della gravità delle imputazioni a carico della reclamante e della recente definizione del procedimento, ha dichiarato infondato il reclamo ritenendo che la reperibilità delle informazioni fosse ancora rispondente all'interesse pubblico (provv. 24 gennaio 2024, n. 42, doc. web n. 9995994).

Analoga valutazione è stata effettuata con riferimento ad altro caso nel quale era stata chiesta la deindicizzazione di alcuni risultati di ricerca riconducibili a notizie di cronaca giudiziaria riferita a reati di particolare gravità che erano stati definiti all'estero in tempi recenti con la condanna dell'interessato. L'Autorità, in considerazione della gravità dei fatti e del breve lasso di tempo decorso dagli stessi, ha dichiarato infondato il reclamo, ritenendo ancora sussistente l'interesse pubblico alla conoscenza delle informazioni, tenuto anche conto del fatto che la maggior parte degli articoli conteneva notizie aggiornate; quest'ultima circostanza consentiva di attualizzare anche i fatti riportati nei pochi articoli non contenenti l'informazione dell'intervenuta condanna a carico dell'interessato (provv. 7 marzo 2024, n. 143, doc. web n. 10007439).

Meritano di essere segnalate le istanze degli interessati funzionali ad ottenere la deindicizzazione di alcuni contenuti reperibili tramite criteri di ricerca non coincidenti con il nome e cognome dei medesimi. Si evidenzia in particolare un caso in cui era stato chiesto il *delisting* di alcuni articoli riguardanti il coinvolgimento in vicende di bancarotta fraudolenta di un gruppo societario, la cui denominazione includeva anche il cognome degli interessati. Tale richiesta era stata motivata in ragione della reperibilità delle predette informazioni tramite ricerche effettuate attraverso i dati personali dei medesimi. I reclamanti avevano affermato di essere stati coinvolti solo marginalmente nei fatti addebitati alla società e di avere comunque patteggiato la relativa pena già da alcuni anni, ragione per la quale non vi sarebbe stato alcun interesse attuale ad avere disponibilità di tali informazioni. Nel corso del procedimento, peraltro, era emerso che gli URL oggetto di richiesta di rimozione non erano in realtà reperibili tramite il nome e cognome degli interessati, ma solo in associazione a quest'ultimo, ovvero con criteri diversi da quelli in relazione ai quali tale deindicizzazione può essere generalmente chiesta. L'Autorità ha pertanto dichiarato infondato il reclamo, in quanto il criterio di ricerca indicato dagli interessati (il solo cognome) non era da ritenersi un dato personale idoneo ad identificarli in modo univoco, potendo lo stesso dato riferirsi, se isolatamente considerato, anche ad altri soggetti (persone fisiche e giuridiche) (provv. 24 gennaio 2024, n. 56, doc. web n. 9994293).

La valutazione che l'Autorità è chiamata a svolgere al fine di valutare la fondatezza delle richieste di deindicizzazione comprende diversi elementi, tra i quali di indubbia rilevanza è quello riferito all'interesse pubblico alla conoscibilità delle informazioni; la sussistenza di un tale interesse, tuttavia, non necessariamente implica la rilevanza penale della condotta oggetto di diffusione.

Si segnala al riguardo il caso di un interessato che aveva lamentato la perdurante reperibilità, in associazione al proprio nominativo, di alcuni URL collegati ad articoli di stampa contenenti la notizia del suo coinvolgimento, avvenuto diversi anni prima, in un procedimento disciplinare avviato all'estero dall'ordine professionale di appartenenza e conclusosi con la sua cancellazione dall'albo professionale. L'interessato aveva eccepito l'inesattezza delle informazioni pubblicate affermando di non essere mai stato sottoposto a procedimento penale per i fatti contestati. L'Autorità ha dichiarato infondata la richiesta, ritenendo la notizia di interesse per la collettività in quanto relativa a condotte

di particolare disvalore sociale a prescindere dalla rilevanza penale dei fatti, come confermato dall'esito dell'accertamento disciplinare (provv. 7 marzo 2024, n. 141, doc. web n. 10015262).

In altri casi l'Autorità ha invece valutato positivamente la richiesta di deindicizzazione riguardante dati giudiziari ritenendo che l'interesse pubblico alle relative informazioni potesse ritenersi affievolito in virtù del decorso di un certo lasso di tempo o che comunque il relativo trattamento non fosse più conforme ai principi previsti dalla normativa di riferimento.

Ciò è quanto si è verificato nel caso riguardante la richiesta di deindicizzazione di alcuni URL riconducibili a contenuti attinenti a vicende giudiziarie che, pur riferite a reati gravi, risalivano a circa dieci anni prima e per le quali l'interessato aveva espiato la pena comminata. Alla luce del tempo decorso e del mutamento della situazione personale e professionale dell'interessato nel frattempo intervenuta, l'Autorità ha accolto il reclamo ritenendo che la reperibilità delle notizie in associazione al nominativo del medesimo non fosse più rispondente all'interesse pubblico (provv. 7 marzo 2024, n. 145, doc. web n. 10009274).

In un altro caso ancora, l'Autorità è pervenuta alla medesima valutazione valorizzando, unitamente al profilo temporale, anche la funzione rieducativa della pena, tenendo conto del fatto che la vicenda giudiziaria in parola si era conclusa con una misura di "affidamento in prova ai servizi sociali" a seguito della quale era stata poi pronunciata l'estinzione della pena (provv. 7 marzo 2024, n. 144, doc. web n. 10008263).

Unitamente all'elemento temporale, la valutazione dell'Autorità tiene conto anche di altri elementi, quali la rispondenza del trattamento al principio di esattezza del dato. Con riferimento al trattamento di dati giudiziari, si possono citare alcune decisioni, tra le quali quella in cui l'interessato aveva chiesto la deindicizzazione di alcuni articoli riferiti ad una vicenda giudiziaria che, pur avendo avuto una grande rilevanza a livello nazionale, era risalente nel tempo e si era peraltro conclusa sotto un profilo giudiziario. L'Autorità ha accolto il reclamo rilevando che le informazioni riportate negli articoli non erano state aggiornate, ma risultavano ferme alle fasi iniziali del procedimento producendo, in capo all'interessato, un pregiudizio che non poteva ritenersi bilanciato dalla sussistenza di un perdurante interesse pubblico alla reperibilità di tali informazioni in associazione al nominativo del medesimo (provv. 22 febbraio 2024, n. 114, doc. web n. 10006460; analogamente provv. 4 luglio 2024, n. 413, doc. web n. 10050339).

Nello stesso senso l'Autorità ha ritenuto fondato il reclamo proposto da un interessato che aveva beneficiato in tempi recenti dell'istituto della riabilitazione; in tale occasione il Garante ha ritenuto che la perdurante reperibilità di tali notizie non aggiornate in associazione al nominativo dell'interessato fosse idonea a determinare in capo al medesimo un pregiudizio derivante dall'incompletezza dell'informazione (provv. 24 aprile 2024, n. 248, doc. web n. 10027483).

Dati giudiziari relativi a parti offese

Un certo numero di richieste di deindicizzazione sono invece pervenute da soggetti che in ambito giudiziario avevano assunto il ruolo di parte offesa oppure da soggetti ai quali erano state attribuite condotte illecite non sostenute da alcun accertamento oggettivo. Questo è quanto si è verificato nel caso di una richiesta di rimozione di URL collegati ad articoli di stampa in cui era stata riportata la notizia della sospensione del reclamante dal suo ministero sacerdotale a seguito del coinvolgimento in una vicenda di estorsione, tentata a suo danno dietro minaccia di diffondere un video *hard* che lo ritraeva nell'atto di compiere un rapporto sessuale con uno degli estorsori. L'Autorità ha ritenuto il reclamo fondato in considerazione del tempo decorso dai fatti, della circostanza che l'interessato fosse vittima di un reato commesso da altri e del fatto che già da diverso tempo fosse stato reintegrato nella sua funzione (provv. 8 febbraio 2024, n. 68, doc. web n. 9999866).

Alla seconda categoria è invece riconducibile il caso relativo alla richiesta di deindicizzazione di un URL rinviante ad una lettera non firmata dal contenuto ritenuto diffamatorio in quanto diretto a ricostruire in maniera non veritiera la carriera del reclamante, avuto riguardo al conferimento degli incarichi ricevuti e delle cariche ricoperte nella pubblica amministrazione. L'Autorità ha ritenuto fondato il reclamo ritenendo che la ricostruzione effettuata dall'autore della lettera, priva di riscontri puntualmente verificabili e in assenza di procedimenti giudiziari pendenti o pregressi a carico dell'interessato, sembrava riflettere una visione personale rispetto alla quale non assumeva rilevanza la circostanza che il reclamante non avesse rappresentato le proprie doglianze o dato prova di essersi attivato in altre sedi in merito a tale aspetto (provv. 21 marzo 2024, n. 180, doc. web n. 10015401; profili analoghi in provv. 9 maggio 2024, n. 297, doc. web 10027850). Si può citare ancora il caso riguardante la richiesta di deindicizzazione di un articolo attinente a presunte irregolarità nell'espletamento di un concorso in ambito universitario, contenente informazioni e commenti relativi a fatti risalenti che non avevano determinato a carico del reclamante provvedimenti o procedimenti di natura giudiziaria e/o disciplinare, né peraltro erano emersi seguiti tali da rinnovare l'interesse per la notizia. Sulla base di tali elementi l'Autorità ha ritenuto fondata la richiesta dell'interessato reputando che la pagina oggetto di richiesta non offrisse un quadro aggiornato rispetto al complesso delle azioni intentate e dei procedimenti avviati in relazione alla procedura concorsuale e che fosse tale da rendere il trattamento dei dati personali dell'interessato non conforme al principio di esattezza (provv. 24 aprile 2024, n. 269, doc. web n. 10043417).

L'operazione di bilanciamento sottesa alla valutazione delle richieste di rimozione deve inoltre tenere conto, da un lato, delle esigenze di tutela espressa dagli interessati e, dall'altro, della necessità di garantire agli utenti della rete l'accessibilità ad informazioni utili riguardo ai medesimi. Al fine di poter apprezzare la sussistenza di un interesse pubblico attuale alla conoscibilità di determinate informazioni, occorre tenere in considerazione l'effettiva rilevanza della notizia e la sua idoneità a contribuire in modo efficace alla costruzione di un profilo dell'interessato rispondente alla sua attuale identità.

È questo il caso di un interessato che aveva avanzato una richiesta di rimozione di URL riconducibili ad alcuni video pubblicati dal medesimo e che quest'ultimo aveva provveduto a rimuovere dalle piattaforme *social* anche in seguito alla ricezione di contenuti offensivi. L'interessato aveva evidenziato che la continua associazione a tali contenuti gli aveva impedito di dissociarsi da un'immagine che non rappresentava più la sua identità, nuocendo al suo attuale percorso professionale. Il medesimo aveva altresì chiesto la rimozione dalla funzione di completamento automatico (cd. *autocomplete*) di termini idonei ad agevolare la ricerca di detti contenuti, amplificando il pregiudizio subìto. L'Autorità ha ritenuto il reclamo fondato trattandosi di articoli scritti principalmente in lingua straniera e risalenti a qualche anno prima, destinati alla pubblicazione su una specifica piattaforma e non più attuali in quanto rimossi dallo stesso interessato. Tali contenuti non risultavano attinenti all'attuale dimensione lavorativa del medesimo e rispetto ad essi non risultava sussistente un interesse pubblico alla relativa conoscibilità, valutazione che, per le medesime ragioni, è stata estesa anche alla richiesta di rimozione degli ulteriori termini resi disponibili nella funzione di completamento automatico (provv. 9 maggio 2024, n. 275, doc. web n. 10027521).

10 Cyberbullismo e *revenge porn*

Nel periodo di riferimento le segnalazioni in materia di cyberbullismo pervenute all'Autorità hanno riguardato, in via principale, la pubblicazione di *post* denigratori e diffamatori, nonché la creazione di falsi profili all'interno di *social network*. In taluni casi i segnalanti avevano lamentato anche situazioni riconducibili alle fattispecie di cui all'art. 144-*bis* del Codice e riguardanti la diffusione di immagini intime senza il consenso dell'interessato, ragione per cui, in simili circostanze, erano state fornite anche indicazioni riguardo alla specifica procedura all'uopo prevista.

Le istanze in materia di cyberbullismo sono state trattate mediante l'invio di apposite richieste di intervento al gestore della piattaforma di volta in volta coinvolto e, in taluni casi, anche prendendo contatti con il segnalante allo scopo di acquisire elementi aggiuntivi utili alla gestione dell'istanza o di fornire al medesimo informazioni rispetto alla vicenda segnalata. Si sono registrati altresì casi in cui non sono stati ravvisati i presupposti per poter procedere, sia a causa della mancata indicazione da parte del segnalante degli elementi necessari all'invio della relativa richiesta al gestore della piattaforma coinvolta, sia in ragione della carenza dei requisiti minimi previsti per qualificare una condotta come atto di cyberbullismo ai sensi dalla l. n. 71/2017.

Si è inoltre intensificata in modo significativo l'attività del Garante volta a prevenire e contrastare il fenomeno della diffusione non consensuale di materiale a contenuto sessualmente esplicito (cd. *revenge porn*) ai sensi dell'art. 144-*bis* del Codice.

Rispetto al periodo precedente si è verificato un notevole incremento delle segnalazioni in materia pervenute al Garante, che hanno raggiunto nel corso del 2024 il numero complessivo di 823, presentate prevalentemente attraverso l'apposita procedura di segnalazione *online* resa disponibile sul sito istituzionale dell'Autorità.

Laddove si è reso necessario, le segnalazioni sono state gestite chiedendo agli interessati le integrazioni necessarie ai fini della relativa trattazione, ivi compresa, in talune ipotesi, la trasmissione del materiale a contenuto sessualmente esplicito la cui acquisizione è prevista dall'art. 144-*bis* del Codice. In alcuni casi il materiale inviato dai segnalanti non è risultato idoneo (come nel caso di *screenshot* di videochiamate o di *chat*) all'invio alle piattaforme interessate, stante la possibilità per la persona malintenzionata di caricare l'immagine originale in suo possesso (talora diversa o ulteriore rispetto a quella fornita dal segnalante).

La trattazione delle segnalazioni ha portato in larga misura all'adozione in via d'urgenza di una determinazione dirigenziale (nel complesso 625), oggetto di successiva ratifica da parte del Collegio e diretta ai gestori delle piattaforme coinvolte per ottenere l'intervento di blocco preventivo del materiale a contenuto sessualmente esplicito oggetto della temuta attività di diffusione.

Nel corso del periodo di riferimento si è inoltre intensificata l'interlocuzione tra l'Autorità e la Procura della Repubblica in relazione alle segnalazioni di *revenge porn*

da cui risulterebbero prospettarsi possibili notizie di reato.

Unitamente a tale casistica, le istanze pervenute hanno riguardato con maggiore frequenza fattispecie in cui i segnalanti avevano lamentato di essere stati vittime di richieste di denaro da parte di soggetti non identificabili ai quali erano stati volontariamente inviati video e/o immagini a contenuto sessualmente esplicito e ciò a fronte della minaccia che, in caso di mancato pagamento, avrebbe avuto luogo una diffusione del materiale acquisito (cd. *sextortion*).

Nel corso del 2024 sono state altresì inviate all'Autorità talune segnalazioni aventi ad oggetto la temuta diffusione di materiale manipolato ed artefatto, realizzato attraverso l'impiego di sistemi algoritmici e di IA (cd. *deep fake*).

11 *Marketing* e trattamento di dati personali

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

Nel corso del 2024 l'Autorità ha proseguito l'attività di contrasto al *telemarketing* indesiderato attraverso una capillare attività di verifica e controllo nei confronti di operatori attivi nell'ambito di vari settori merceologici e diversamente dislocati sul territorio nazionale, nonché operanti a vario titolo nell'ambito della filiera del trattamento che dal contatto consente di giungere al contratto.

L'attività in parola ha registrato una crescente intensità in ragione del numero sempre più elevato di reclami e segnalazioni riguardanti la ricezione di comunicazioni indesiderate, effettuate mediante il canale telefonico, SMS ed *e-mail*. In aggiunta, ad aggravare la portata e le dimensioni del fenomeno, ha contribuito anche lo svolgimento di attività promozionali mediante il ricorso alle nuove tecnologie: internet e *social*.

In tale contesto, l'azione di contrasto posta in essere nel corso dell'anno ha principalmente seguito un triplice ordine di direttrici. In primo luogo, l'Autorità ha avviato una fattiva azione di cooperazione e confronto con le altre autorità di regolazione competenti *ratione materiae* e con i soggetti a vario titolo coinvolti nell'azione di contrasto al *telemarketing* indesiderato. Ha inoltre accreditato l'Organismo di monitoraggio e, contestualmente, definitivamente adottato il codice di condotta per le attività di *telemarketing* e *teleselling* promosso da associazioni di committenti, *call center*, *teleseller*, *list provider* e associazioni di consumatori (v. provv. 9 marzo 2023, n. 70, doc. web n. 9868813) ed ha successivamente adottato un nuovo provvedimento di accreditamento dell'Organismo di monitoraggio in considerazione della sostituzione di due membri. Tale Organismo ha così potuto iniziare a operare concretamente comunicando al Garante di aver predisposto anche un apposito sito web per il contatto con l'utenza (provv.ti 7 marzo 2024, n. 148, doc. web n. 9993808 e 17 ottobre 2024, n. 624, doc. web n. 10079413).

Per garantire l'ottemperanza alla normativa *privacy,* le società che aderiranno al codice si impegneranno ad adottare misure specifiche per garantire la correttezza e la legittimità dei trattamenti di dati svolti lungo tutta la filiera del *telemarketing*. Dovranno raccogliere consensi specifici per le singole finalità (*marketing*, profilazione, ecc.), informare in maniera precisa e puntuale le persone contattate sulle finalità per le quali vengono usati i loro dati, assicurando il pieno esercizio dei diritti previsti dalla normativa *privacy* (*i.e.* opposizione al trattamento, rettifica o aggiornamento dei dati). Il codice ha inoltre introdotto regole per contrastare il fenomeno del "sottobosco" dei *call center* abusivi, prevedendo che all'interno dei contratti stipulati dall'operatore con l'affidatario del servizio dovrà essere prevista una penale o la mancata corresponsione della provvigione per ogni vendita di servizi realizzata a seguito di contatto promozionale senza consenso.

Nell'ambito della seconda linea direttrice perseguita, l'Autorità ha profuso un costante e giornaliero impegno per fornire, già all'esito dell'istruttoria preliminare, riscontro, chiarimenti e indicazioni operative alle migliaia di doglianze trasmesse dai soggetti interessati.

Infine, nel perseguimento del terzo ordine di obiettivi, a partire dalle segnalazioni e dai reclami portati all'attenzione dell'Autorità, sono state svolte puntuali attività istruttorie,

anche attraverso iniziative ispettive, che hanno condotto all'adozione di numerosi provvedimenti correttivi e sanzionatori, sovente di portata interpretativa tale da trascendere le specificità del singolo caso concreto.

Le istruttorie espletate in materia di *telemarketing* continuano ancora a evidenziare il dilagante utilizzo di numerazioni *VoIP* fittizie, volte a occultare la reale linea telefonica chiamante (fenomeno del cd. *spoofing*) e la realizzazione di contatti effettuati da operatori non censiti all'interno del registro degli operatori della comunicazione e postali (ROC). Più in generale, l'attività di indagine ha rivelato la mancata assimilazione degli obblighi gravanti sul titolare del trattamento in virtù del principio della cd. *accountability*, l'omesso controllo lungo tutta la filiera del trattamento, la mancata adozione di adeguate misure tecniche e organizzative, nonché l'utilizzo di liste di contattabilità acquisite in assenza dei presupposti previsti dalla vigente normativa. In alcuni casi, le istruttorie hanno riguardato il trattamento di dati personali forniti ai titolari da soggetti terzi (*list provider*) in assenza di adeguate verifiche in ordine ai presupposti di liceità del trattamento, con particolare riferimento all'informativa conferita ai soggetti interessati e alle condizioni di validità dei consensi resi dagli interessati.

Le istruttorie avviate dall'Autorità in relazione alla materia del *telemarketing* indesiderato hanno portato all'adozione dei provvedimenti illustrati più in dettaglio nei successivi paragrafi.

11.1.1. Il telemarketing *illegale nel settore delle compagnie telefoniche*

L'Autorità ha adottato un provvedimento, a conclusione di un'istruttoria sviluppatasi negli anni 2022 e 2023. Nel 2022, il Garante aveva emesso un provvedimento (provv. 10 novembre 2022, n. 379, doc. web n. 9826417) contro una società in relazione a diverse problematiche relative alle attività di *telemarketing*. Nonostante gli sforzi profusi dal titolare al fine di conformarsi alle prescrizioni del Garante, come l'istituzione di controlli sulle numerazioni telefoniche utilizzate dai *partner* commerciali, l'Autorità ha continuato a ricevere un numero elevato di segnalazioni e reclami. Il Garante ha avviato quindi un'ulteriore indagine per valutare le pratiche di *telemarketing* e ha riscontrato la sussistenza di diverse criticità, ipotizzando la violazione dei principi di liceità e responsabilizzazione nel trattamento dei dati personali, non avendo la società adottato misure tecniche e organizzative adeguate a garantire la conformità al RGPD. All'esito del procedimento, l'Autorità ha adottato il nuovo provvedimento, riconoscendo che il percorso intrapreso dalla società è risultato in gran parte in linea con le prescrizioni del Garante, evidenziando una scelta di fondo chiaramente indirizzata verso una razionalizzazione dei processi per l'acquisizione dei cd. *lead*, ovvero dei dati di contatto di clienti e potenziali clienti e dei documenti atti a comprovate la loro volontà di essere contattati, nonché verso una rilevante responsabilizzazione della rete di vendita. Tuttavia l'Autorità ha constatato la permanenza di talune criticità, in particolare per la scelta di implementare una procedura di ricontatto dei clienti o potenziali clienti su loro richiesta che non appare funzionale a disincentivare l'eventuale utilizzo di sistemi automatizzati che, massivamente, possano inserire numerazioni telefoniche da sottoporre a ricontatto. La procedura di ricontatto, inoltre, era stata introdotta solo dopo le attività di controllo del Garante che avevano evidenziato l'esistenza di chiamate nei confronti di utenze iscritte nel RPO. Anche la procedura di verifica "dal contatto al contratto", prevista peraltro nel codice di condotta per le attività di *telemarketing,* pur risultando rigorosa e puntuale in fase di accertamento, è apparsa carente sotto l'aspetto dell'informazione da rendere al cliente al fine di renderlo edotto della eventuale natura illecita del contatto promozionale e di consentire al medesimo di recedere senza costi dal contratto attivato. Con il provvedimento in commento l'Autorità ha applicato alla compagnia telefonica una sanzione

amministrativa pecuniaria dell'importo di euro 500.000,00, ingiungendo inoltre di introdurre correttivi nella procedura di ricontatto del cliente a seguito di richieste veicolate attraverso le pagine web della società o dei propri *partner*, al fine di impedire l'introduzione massiva di numerazioni da sottoporre a ricontatto (provv. 9 maggio 2024, n. 574, doc. web n. 10107938).

Sempre con riferimento ai servizi di telefonia, l'Autorità ha adottato un provvedimento correttivo e sanzionatorio in materia di *telemarketing* ed esercizio dei diritti degli interessati. All'esito dell'istruttoria, il Garante ha accertato la responsabilità della società per avere effettuato attività promozionali in assenza di un'idonea base giuridica e senza la previa verifica presso il RPO, nonché per aver effettuato trattamenti di dati personali appartenenti ai propri clienti in contrasto con i principi di liceità, correttezza e trasparenza del trattamento, con riferimento alla minimizzazione dei dati, limitazione delle finalità, responsabilizzazione, in assenza di un'idonea base giuridica, mettendo in atto misure tecniche e organizzative non adeguate per garantire, fin dalla progettazione, ed essere in grado di dimostrare, che il trattamento è effettuato, in ogni suo aspetto e in qualsiasi stadio e/o livello, conformemente al RGPD (provv. 20 giugno 2024, n. 401, doc. web n. 10040382).

Si segnala, inoltre, il provvedimento correttivo e sanzionatorio adottato nei confronti di un altro operatore telefonico in forza del quale sono state fornite per la prima volta importanti indicazioni circa il perimetro di applicazione del *soft spam*, nonché preliminari chiarimenti in merito alle modalità di realizzazione del servizio di "recupero carrello" (o *basket recovery*) nelle attività di *e-commerce*. Dall'istruttoria era emerso che la società effettuava periodiche attività di *marketing*, utilizzando sia canali tradizionali che automatizzati, previa acquisizione del consenso degli interessati, nonché comunicazioni promozionali via *e-mail* avvalendosi della deroga al consenso prevista dall'art. 130, comma 4, del Codice (*soft spam*). Per tali due diverse modalità erano previste altrettante tipologie di registrazioni nei sistemi con l'attivazione di conseguenti procedure, rispettivamente, per la gestione/revoca dei consensi o per l'opposizione. L'unica differenza tra *e-mail* di *marketing* ed *e-mail* di *soft spam* era rinvenibile nella circostanza che queste ultime fossero afferenti a prodotti analoghi a quelli acquistati dai clienti. Stante la formulazione generica dell'informativa e della formula di richiesta del consenso per finalità di *marketing* presenti nell'area personale, di fatto, tra le due tipologie di trattamento vi era meramente un rapporto di genere a specie (la generalità delle comunicazioni promozionali inviate via *e-mail* e la specialità delle stesse comunicazioni inviate via *e-mail* per prodotti analoghi). A tale riguardo il Garante ha osservato che la possibilità di gestire in autonomia i consensi nell'area personale è una misura che consente all'interessato di avere il controllo sui propri dati abilitando, contemporaneamente, il titolare a tenere traccia di tale volontà. Parallelamente, il diniego manifestato nell'area personale – per la genericità e ampiezza della formulazione – non poteva essere considerato distinto da quello formulato ai fini dell'opposizione al *soft spam*, né aggirato invocando la deroga di cui all'art. 130, comma 4, del Codice. La disposizione appena citata, che costituisce un'eccezione alla regola generale, opera solo al ricorrere di determinate condizioni tra cui la necessità che "l'interessato, adeguatamente informato, non rifiuti tale uso inizialmente o in occasione di successive comunicazioni". Inoltre l'avverbio "inizialmente" deve essere interpretato come ricadente in un momento anteriore all'invio delle *e-mail*, analogamente a quanto previsto per la fase informativa, disciplinata dall'ultimo capoverso dell'art. 130, comma 4, del Codice ove si legge che "l'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione (…) è informato della possibilità di opporsi". Tale opposizione iniziale può essere espressa dall'interessato anche accedendo alla propria area personale dopo la sottoscrizione

del contratto. Un modello così impostato, dunque, comportava che la volontà correttamente espressa dall'interessato di non ricevere comunicazioni promozionali (in generale), veniva di fatto aggirata veicolandogli comunque *e-mail* indesiderate basate sul *soft spam*. Il provvedimento in esame, inoltre, ha dato modo di tornare ad esprimersi sulla qualificazione giuridica del *soft spam* che, pur essendo stata oggetto di altre pronunce da parte del Garante, suscita ancora molti dubbi interpretativi (cfr. provv. 11 gennaio 2023, n. 9, doc. web n. 9861941). In particolare, il Garante ha ribadito che l'art. 130, comma 4, del Codice non può essere considerato analogo al legittimo interesse, ma costituisce una mera deroga all'obbligo del consenso in quanto, data la disciplina speciale cui soggiace l'invio di comunicazioni promozionali via *e-mail*, la base giuridica del trattamento va ricercata tra quelle indicate dall'art. 130 del Codice, che recepisce l'art. 13 della direttiva 2002/58/CE, e non tra i presupposti di liceità di cui all'art. 6 del RGPD. Per tale motivo, la disposizione contenuta nell'art. 130, comma 4, non può essere equiparata a una delle basi giuridiche di cui all'art. 6 del RGPD, ossia, in particolare, al legittimo interesse. Infine, rispetto alle comunicazioni comunemente note come *basket recovery* o "recupero carrello", l'Autorità ha osservato che non si può ignorare il fatto che tale pratica possa avere anche un'utilità per il potenziale cliente. Infatti, nel caso in cui questi abbia dovuto suo malgrado interrompere il processo di acquisto o abbia avuto un successivo ripensamento, per acquistare il servizio dovrebbe avviare una nuova richiesta compilando nuovamente tutti i campi necessari. In tali termini dunque può essere considerata utile la procedura di *basket recovery* se, come nel caso di specie, contiene un *link* per recuperare il carrello senza dover reinserire tutti i dati. Tuttavia, affinché la pratica sia riconducibile alla sola funzionalità di recupero carrello e non ingeneri il dubbio che essa abbia anche una finalità latamente promozionale, è sufficiente che l'utente riceva una sola comunicazione di questo tipo (provv. 17 luglio 2024, n. 576, doc. web n. 10084158).

L'Autorità ha anche adottato un provvedimento con il quale ha affrontato il tema dell'affidamento di chiamate promozionali all'esterno del circuito aziendale del titolare del trattamento. Il provvedimento ha tratto origine da un reclamo, con il quale è stato lamentato un contatto telefonico indesiderato con finalità promozionali riconducibile ad una impresa impegnata nel procacciamento di contratti per fornitura di servizi di comunicazione elettronica. Le successive interlocuzioni del reclamante e le conseguenti richieste di informazioni formulate dall'Ufficio hanno consentito di appurare che l'azienda italiana aveva commissionato l'incarico di contattare persone residenti nella propria area territoriale ad un'agenzia tunisina, la quale effettuava tali contatti senza osservare le condizioni di liceità del trattamento stabilite dal RGPD e dal Codice e senza sottoporre le numerazioni da contattare al preventivo controllo presso il RPO. Nel provvedimento l'Autorità ha ribadito che i soggetti che affidano all'esterno della propria realtà imprenditoriale attività promozionali, assumono in ogni caso la veste giuridica del titolare dei correlati trattamenti di dati personali e ha altresì affermato che affidare le attività di contatto telefonico ad un soggetto non stabilito nel territorio dell'Unione europea e quindi sottratto ai vincoli previsti nel RGPD e nel Codice, comporta che l'unico soggetto al quale devono ricondursi gli obblighi relativi al trattamento sia quello presso il quale approdano i dati personali, a seguito dei commissionati contatti promozionali (provv. 26 settembre 2024, n. 586, doc. web n. 10072622).

Sempre nel settore telefonico, l'Autorità ha adottato un provvedimento correttivo e sanzionatorio nei confronti di un operatore mobile nazionale. Il procedimento aveva preso avvio da un reclamo mediante il quale l'interessato aveva lamentato la ricezione di SMS, successivamente alla compiuta portabilità della propria utenza mobile verso altro

operatore. Peraltro, la ricezione delle lamentate comunicazioni, era avvenuta anche dopo la revoca dei consensi e la richiesta di cancellazione dei propri dati personali. A tale riguardo, l'Autorità anzitutto ha ritenuto doveroso distinguere fra messaggi promozionali e messaggi "informativi". Con riferimento alla prima categoria, la richiesta di cancellazione dei dati di contatto e la revoca dei consensi prestati in sede di attivazione *online* del contratto di telefonia aveva comportato la revoca del consenso prestato alla ricezione di comunicazioni promozionali. Parimenti, anche i messaggi "informativi" successivi all'estinzione del contratto, sono risultati privi di una valida base giuridica, in quanto non supportati più dal presupposto del contratto, essendo quest'ultimo cessato con l'avvenuta portabilità dell'utenza. Pertanto, l'Autorità ha ritenuto necessario ingiungere alla società di adottare misure tecniche e organizzative adeguate a garantire il tempestivo ed effettivo esercizio delle istanze formulate dagli interessati ai sensi degli artt. 15 e 22 del RGPD e applicare una sanzione amministrativa pecuniaria (provv. 27 novembre 2024, n. 832, doc. web n. 10107716).

Con riguardo alle attività promozionali poste in essere dai titolari del trattamento che elaborano grandi quantità di dati, si evidenzia il provvedimento adottato nei confronti di un operatore telefonico all'esito di un lungo e complesso procedimento nell'ambito del quale, anche attraverso un'apposita attività ispettiva, sono stati effettuati puntuali controlli sulle modalità operative poste in essere dal titolare. Il provvedimento rappresenta anche una ricognizione dell'evoluzione registrata nell'ambito delle modalità di realizzazione delle campagne di *marketing* per adattarsi ai requisiti sempre più stringenti di liceità resisi necessari a seguito delle numerosissime doglianze oggetto di istruttoria del Garante, nonché dei correlati danni arrecati dal *marketing* selvaggio allo stesso mercato e al settore dei *call center*. Nel provvedimento, dunque, è data evidenza alle problematiche emerse dall'uso delle cosiddette liste fredde (ossia, liste formate da soggetti terzi attraverso asserite iscrizioni a portali web), problematiche che ancora oggi non sembrano superabili date le numerose criticità rilevate nella documentazione dei consensi raccolti. In particolare, il provvedimento dà atto del lungo percorso effettuato dal titolare per modificare le proprie modalità operative superando l'utilizzo di tali liste e valorizzando invece i contatti effettuati solo sulla base di manifestazione di interesse da parte dell'utente (ossia, i cd. *lead* o liste calde) (provv. 12 dicembre 2024, n. 774, doc. web n. 10105764).

11.1.2. Il telemarketing *illegale nel settore energetico*

In continuità con quanto realizzato negli anni precedenti, nel 2024 l'Autorità ha proseguito l'attività istruttoria e sanzionatoria finalizzata al contrasto del cd. *telemarketing* selvaggio nel campo delle forniture energetiche.

Lo svolgimento di attività di *telemarketing* nell'ambito del settore in commento è stato caratterizzato dal passaggio al mercato libero e dalla proliferazione di società cd. *multiutility*; per l'effetto, il tema si è rivelato di primario interesse e allarme sociale per i soggetti interessati, che attraverso numerose segnalazioni e reclami si rivolgono ogni giorno al Garante chiedendo tutela. Inoltre, a seguito delle iniziative anche di matrice europea in materia di efficientamento energetico, si è ampliata la platea di operatori operanti nel campo e la tipologia di servizi offerti, con conseguente aumento del rischio di trattamenti illeciti di dati personali ai fini promozionali.

I disagi patiti, per come rappresentati dagli utenti, sono di varia natura e interessano sovente sia la sfera patrimoniale che quella non patrimoniale. Inoltre le metodologie e le tecnologie impiegate appaiono sempre più insidiose. Gli interessati non lamentano soltanto la ricezione di chiamate promozionali, ma manifestano altresì diffusa preoccupazione per la circostanza che gli autori delle telefonate sono già in possesso di tutti i loro dati personali, nonché delle informazioni relative alle forniture e alle coordinate bancarie.

Si segnala, in proposito, l'adozione di due provvedimenti mediante i quali è stata imposta l'adozione di talune misure prescrittive e irrogata ad entrambi i titolari del trattamento una sanzione amministrativa pecuniaria di euro 100.000,00. Nell'ambito dei richiamati provvedimenti è stata accertata la mancata predisposizione di idonee misure di sicurezza tecniche e organizzative e di controlli nei confronti della filiera commerciale e dei *partner*, nonché la responsabilità delle società per avere contattato, nell'ambito delle attività di *telemarketing*, numerazioni telefoniche in costanza dell'iscrizione al RPO (provv.ti 11 aprile 2024, n. 204, doc. web n. 10008019 e n. 205, doc. web n. 10008076).

Con provvedimento adottato nei confronti di un'importante società operante nel settore energetico, l'Autorità ha irrogato una sanzione amministrativa pecuniaria pari ad euro 6.419.631,00. Dall'istruttoria espletata, è infatti emerso che la società aveva effettuato trattamenti di dati personali in violazione dei principi di liceità, correttezza, trasparenza, esattezza e sicurezza e aveva realizzato attività di *telemarketing* in assenza di un'idonea base giuridica. Nel medesimo procedimento, inoltre, è stata accertata anche l'omessa implementazione di idonee misure di sicurezza, monitoraggio e controllo sull'intera filiera commerciale. Con il provvedimento in parola, sono state fornite preziose indicazioni anche in relazione alla gestione delle campagne di cd. *win back* ai sensi dell'art. 1, comma 5, l. n. 5/2018, precisando che la norma in commento non può trovare applicazione in mancanza dell'implementazione di modalità semplificate per l'esercizio del diritto di revoca e che in ogni caso tali campagne devono essere realizzate entro ragionevoli limiti di tempo e di tentativi di ricontatto. L'Autorità si è poi espressa anche sul tema dei cd. *lead* caldi, chiarendo che considerare le anagrafiche contattabili per un arco di tempo eccessivamente prolungato non appare conforme al dettato normativo e sembra confondere l'interesse precontrattuale all'offerta con il conferimento di un vero e proprio consenso al trattamento per finalità di *marketing* (provv. 6 giugno 2024, n. 342, doc. web n. 10029424).

L'Autorità ha altresì comminato, nei confronti di una nota compagnia energetica, una sanzione pecuniaria di euro 678.897,00, imposto talune prescrizioni nonché fornito indicazioni utili in ordine all'interpretazione della nozione di dato personale, agli obblighi gravanti sul titolare del trattamento in virtù del principio di *accountability* e ai doveri di controllo e vigilanza sull'operato dei responsabili del trattamento. L'Autorità ha in particolare chiarito che, nell'ambito della nuova concezione del ruolo stesso del titolare, il principio di *accountability* deve necessariamente essere considerato alla stregua di un *fil rouge* che informa l'interpretazione e l'applicazione di tutte le norme e i principi contenuti all'interno del RGPD e, quindi, un imprescindibile canone ermeneutico. Per l'effetto, gli obblighi gravanti sul titolare del trattamento ai sensi dell'art. 28 del RGPD, se interpretati alla luce del principio di responsabilizzazione, non possono ritenersi efficacemente assolti dalla mera previsione di clausole di stile o da interventi realizzati soltanto *ex post* al verificarsi di un'anomalia, ma impongono un *quid pluris*, vale a dire l'effettiva governabilità della filiera di trattamento e l'aggiornamento periodico delle stesse misure tecniche e organizzative implementate per realizzarla (provv. 13 novembre 2024, n. 672, doc. web n. 10086536).

L'Autorità ha irrogato una sanzione pecuniaria pari ad euro 892.738,00 e imposto l'adozione di talune misure correttive, con un provvedimento che può costituire un utile strumento di orientamento per gli operatori del settore sia con riferimento all'applicazione del principio dell'onere della prova nei procedimenti dinanzi al Garante, sia in relazione alle misure da implementare in caso di utilizzo di *form online* per la raccolta di dati personali e/o l'inoltro di richieste di ricontatto. La decisione in parola, inoltre, innalza l'attenzione sull'utilizzo di tali strumenti, anche alla luce del noto e

pervasivo utilizzo di internet e dei *social*. In assenza di adeguate misure sotto il profilo della *data protection*, infatti, il conferimento di dati personali illecitamente ottenuti o "non consensati" all'interno di *form online* finisce per conferire una parvenza di liceità rispetto al trattamento di dati personali e liste di contattabilità di provenienza illecita, realizzando di fatto un inammissibile riciclaggio di dati personali e alimentando l'indotto del sottobosco del *telemarketing* (provv. 27 novembre 2024, n. 736, doc. web n. 10097012).

11.1.3. Il telemarketing *illegale in altri settori commerciali*

Errata base giuridica

Con provvedimento emanato nei confronti di un noto istituto bancario, l'Autorità si è espressa sul tema del legittimo interesse, spesso invocato dai titolari del trattamento quale base giuridica per l'inoltro di comunicazioni promozionali indirizzate ai propri clienti. L'Autorità ha ribadito che la realizzazione delle comunicazioni promozionali mediante telefono soggiace all'obbligo del consenso in virtù della *lex specialis* di cui all'art. 130 del Codice, non potendo essere invocato il legittimo interesse. Soltanto nelle ipotesi del cd. *soft spam* può essere invocato il legittimo interesse (art. 130, comma 4, del Codice), ma esclusivamente in riferimento a comunicazioni promozionali effettuate utilizzando il canale *e-mail*. Diversamente, al *marketing* postale si applica l'art. 130, comma 3, del Codice e, di conseguenza, il titolare può avvalersi del legittimo interesse tenuto conto che la posta cartacea, non essendo veicolata tramite un canale di comunicazione elettronica, non ricade nelle fattispecie disciplinate dai commi 1 e 2 del medesimo articolo e soggette al consenso preventivo degli interessati. L'utilizzo di tale base giuridica del legittimo interesse, tuttavia, richiede un attento bilanciamento di interessi a carico del titolare del trattamento. L'Autorità ha comminato al predetto istituto bancario una sanzione amministrativa pecuniaria pari a euro 100.000,00, disponendo al contempo il divieto del trattamento di dati personali effettuato mediante il canale telefonico in assenza del preventivo consenso all'attività di *marketing* e ingiungendo di modificare il testo dell'informativa sul trattamento dei dati personali (provv. 11 gennaio 2024, n. 4, doc. web n. 10082705).

Analoga la fattispecie esaminata nel caso di un provvedimento emanato nei confronti di una società con sede nella Repubblica di San Marino, a seguito della ricezione di una doglianza con la quale l'interessato aveva lamentato l'impossibilità di interrompere la ricezione di *e-mail* e SMS indesiderati. Nel corso dell'istruttoria, il titolare aveva fornito giustificazioni contraddittorie e non documentate, sostenendo che si fosse trattato di un errore dovuto alle piccole dimensioni dell'azienda e aggiungendo, altresì, che la propria condotta potesse basarsi sull'interesse legittimo del titolare. Il Garante ha ricordato nuovamente che l'invio di comunicazioni promozionali tramite strumenti di comunicazione elettronica è disciplinato dall'art. 130 del Codice, che costituisce una *lex specialis* dove l'unica base giuridica ammessa è il consenso dell'utente salvo alcune deroghe, tassativamente descritte. Una di esse è contenuta nella disposizione di cui all'art. 130, comma 4, del Codice che consente l'invio di comunicazioni promozionali esclusivamente tramite *e-mail* senza il consenso dell'interessato, con riferimento a servizi analoghi a quelli oggetto della vendita e purché l'interessato, adeguatamente informato, non rifiuti tale uso inizialmente o in occasione di successive comunicazioni. Su tale specifico aspetto il Garante si era espresso, da ultimo, con il provvedimento dell'11 gennaio 2023, n. 9 (doc. web n. 9861941). Ne consegue che l'indicazione del legittimo interesse quale base giuridica non poteva essere ammessa nel caso di specie, né tantomeno poteva essere invocata la deroga prevista dall'art. 130, comma 4, del Codice poiché le comunicazioni erano state inviate anche tramite SMS e nonostante l'interessato si fosse più volte opposto a tale ricezione. La carenza

di misure organizzative aveva avuto anche la conseguenza di non recepire le richieste di cancellazione ripetutamente inoltrate dall'interessato. Pertanto, si è ritenuto necessario imporre al titolare il divieto di trattare per finalità promozionali i dati personali presenti nelle proprie liste ove non fosse in grado di documentare la presenza di un idoneo consenso espresso dagli interessati. Inoltre, in considerazione della gravità della condotta è stata ritenuta applicabile anche la sanzione amministrativa pecuniaria quantificata in euro 10.000,00 (provv. 12 dicembre 2024, n. 775, doc. web n. 10102462).

Con provvedimento emanato nei confronti di una ditta individuale che si occupa di pubblicizzare, mediante sito internet, le opere di artisti e i profili di quest'ultimi, l'Autorità ha ingiunto l'adozione di misure adeguate a fornire un idoneo riscontro alle richieste di esercizio dei diritti degli interessati mediante il corretto presidio dei canali di comunicazione e, in particolare, dell'indirizzo PEC preposto alla relativa trattazione, comminando la sanzione amministrativa pecuniaria pari a euro 5.000,00 (provv. 22 febbraio 2024, n. 111, doc. web n. 10006950).

Misure tecniche e organizzative inadeguate

L'Autorità è inoltre intervenuta a seguito di reclamo in un caso di ricezione di *e-mail* promozionali indesiderate ad opera di una piccola impresa che si avvaleva anche del canale *e-commerce*. Nel corso dell'istruttoria, tuttavia, è emerso che molti di questi messaggi erano partiti dai sistemi del titolare senza che questo ne avesse contezza, avendo appreso solo in tale occasione di aver subito un attacco informatico. Nonostante i tentativi fatti, anche chiedendo ausilio a tecnici informatici, la società non era stata in grado di comprendere compiutamente l'origine dell'evento e le sue reali conseguenze. L'Autorità ha pertanto considerato inadeguate le misure adottate dalla società in considerazione del fatto che essa utilizzava un sistema di gestione dei contenuti (CMS) del sito web obsoleto e affetto da gravi vulnerabilità note dall'inizio del 2022. Ne conseguiva una violazione dell'obbligo di garantire un'adeguata protezione dei dati personali da trattamenti e accessi non autorizzati, mediante misure tecniche opportune che assicurassero l'integrità e la riservatezza dei dati personali. Si è pertanto ritenuto necessario ingiungere al titolare di provvedere all'aggiornamento dei sistemi e si è ritenuta congrua l'applicazione di una sanzione amministrativa pecuniaria di euro 30.000,00 (provv. 24 aprile 2024, n. 237, doc. web n. 10025835).

In aggiunta, si segnala il provvedimento adottato nei confronti di una società italiana che opera nel settore della tv interattiva, all'esito di un'istruttoria avviata a seguito della ricezione di 275 segnalazioni in materia di *telemarketing* e poi estesa anche ai contratti attivati nella cd. settimana campione. Le principali criticità rilevate hanno riguardato, in particolare, l'assenza di adeguate verifiche sugli adempimenti in materia di informativa e consenso, nonché la mancata consultazione del RPO prima di ogni campagna promozionale. Dalla complessa istruttoria, è emerso che alcune delle utenze erano state contattate in base ad un consenso acquisito molto tempo prima e, in alcuni casi, in epoca antecedente alla piena efficacia del RGPD. La documentazione volta a comprovare i consensi acquisiti dalle società fornitrici di dati (cd. *list provider*) era apparsa, inoltre, inidonea a comprovare in modo inequivocabile la volontà degli interessati ad essere contattati per finalità promozionali, dal momento che la società aveva conservato i dettagli dei consensi in *file excel* modificabili. In alcuni casi, tali consensi erano stati considerati validi dalla società, benché riguardanti distinte finalità del trattamento. Con il provvedimento in esame, è stata comminata una sanzione pecuniaria di euro 842.062,00 ed è stato ingiunto alla società di verificare, anche mediante controlli a campione, la liceità delle utenze da contattare, nonché di adottare misure adeguate a contestualizzare la volontà dell'interessato a ricevere telefonate promozionali, registrando nei sistemi le modalità e i tempi di ac-

quisizione dei dati personali. In assenza di uno specifico consenso degli interessati, è stato inoltre vietato ogni ulteriore trattamento con finalità promozionale dei dati personali riferiti ad *account* aperti sulla piattaforma fornita dalla società (provv. 12 settembre 2024, n. 553, doc. web n. 10076504).

Rapporti con *list provider*

L'Autorità ha inoltre affrontato il tema dell'utilizzo di liste di anagrafiche provenienti da *list provider*, in assenza della previa verifica dell'avvenuto adempimento degli obblighi imposti dalla vigente normativa sulla protezione dei dati personali, con particolare riferimento all'acquisizione del consenso dell'interessato e al conferimento dell'informativa in occasione della raccolta dei dati. Nel caso in questione, inoltre, il titolare non aveva fornito all'interessata alcun riscontro nel termine di 30 giorni, previsto dall'art. 12, par. 3, RGPD. Per le ragioni appena illustrate, con il provvedimento in parola è stato preliminarmente accertato che il trattamento di dati personali realizzato mediante l'effettuazione di una telefonata promozionale indesiderata, è avvenuto in assenza di una idonea base giuridica e al contempo si è reso necessario vietare al titolare l'ulteriore trattamento per finalità promozionali dei dati personali acquisiti dal *list provider*, ingiungendo la cancellazione degli stessi. Infine, tenuto conto del carattere isolato della condotta (una sola telefonata indirizzata alla reclamante) e della natura di micro-impresa del titolare del trattamento, è stata ritenuta congrua l'applicazione di una sanzione amministrativa pecuniaria pari a euro 5.000,00 (provv. 17 ottobre 2024, n. 622, doc. web n. 10079389).

L'Autorità ha poi adottato un provvedimento nei confronti di una società attiva nel campo della fornitura di depuratori di acqua, con il quale è stata accertata l'assenza di controlli da parte del titolare del trattamento nei confronti del *list provider,* che da una verifica in rete, è parso riconducibile ad una società priva dei necessari presupposti di garanzia della liceità del trattamento. Pertanto, si è reso necessario, in primo luogo, vietare alla società l'ulteriore trattamento dei dati personali acquisiti dal *list provider* in violazione della normativa, ingiungendo, in relazione a tali dati, la relativa cancellazione; inoltre è stato ingiunto alla società di adottare misure tecniche e organizzative adeguate a fornire un idoneo riscontro alle richieste di esercizio dei diritti degli interessati mediante il corretto presidio dei canali di comunicazione e, in particolare, dell'indirizzo PEC preposto alla relativa trattazione (provv. 13 novembre 2024, n. 758, doc. web n. 10108867).

Errata qualificazione dei ruoli soggettivi

Con riferimento alla qualificazione dei ruoli soggettivi nell'ambito del trattamento dei dati personali, in assenza di documentazione idonea a definire le responsabilità dei soggetti coinvolti, l'Autorità ha riconosciuto in capo a una società assicurativa la qualifica di titolare del trattamento sulla base della condotta tenuta in concreto nel rapporto con i propri clienti, con conseguente imputazione delle violazioni rilevate. In particolare, è stata accertata la responsabilità della società per la violazione degli artt. 12, 17 e 21 del RGPD per la mancata registrazione dell'opposizione avanzata dall'interessato in ordine alla ricezione di *e-mail* promozionali, in ragione del rapporto contrattuale in essere e non ritenendo adeguato il canale della *e-mail* per l'identificazione del richiedente. Inoltre, pur prendendo atto del tempestivo intervento sul testo dell'informativa pubblicata sul sito internet dopo la contestazione da parte dell'Autorità, è stata accertata anche l'avvenuta violazione degli artt. 12 e 13 del RGPD. Alla luce degli elementi sopra rappresentati, l'Autorità ha ingiunto l'adozione di misure tecniche e organizzative adeguate in ordine all'esercizio dei diritti previsti dalla normativa in materia di protezione dei dati personali, nonché il conferimento agli interessati di un'idonea informativa recante l'indicazione delle operazioni di trattamento effettivamente svolte dalla società, comminando altresì la sanzione amministrativa pecuniaria di euro 5.000,00 avuto riguardo al fatturato della società, alla natura episodica dei fatti oggetto di doglianza, nonché dell'assenza di precedenti procedimenti avviati nei confronti del medesimo titolare del trattamento. (provv. 14 novembre 2024, n. 699, doc. web n. 10107986).

L'Autorità ha adottato un provvedimento nei confronti di una società che era già stata destinataria di precedente provvedimento inibitorio, correttivo e sanzionatorio (provv. 18 luglio 2023, n. 323, doc. web n. 9925674) a seguito dell'avvenuta ricezione di numerose segnalazioni in materia di chiamate indesiderate effettuate verso utenze iscritte al RPO e in assenza di uno specifico consenso al trattamento per finalità di *marketing*. All'esito dell'istruttoria svolta e tenuto conto che nel corso dell'audizione la società ha comprovato di essere estranea alla condotta oggetto di doglianza, imputabile unicamente alle agenzie concessionarie che avrebbero agito in qualità di autonomi titolari del trattamento, preso atto delle iniziative già intraprese in adempimento delle prescrizioni imposte dall'Autorità, non è apparso necessario imporre ulteriori prescrizioni. Per l'effetto, l'Autorità ha accertato la sola violazione dell'art. 157 del Codice ed è stata applicata la sanzione amministrativa pecuniaria di euro 10.000,00, quantificata tenendo conto della reiterata condotta omissiva (tale da denotare insufficienti misure organizzative) e del conseguente aggravamento dei tempi e dei costi del procedimento (provv. 27 novembre 2024, n. 737, doc. web n. 10108064).

In una fattispecie analoga, in base a quanto indicato in calce alle comunicazioni oggetto di doglianza, la campagna promozionale era stata commissionata da una società operante nel campo dell'informazione e curata da soggetti terzi, selezionati sul mercato dai *partner* della società medesima, quest'ultimi nominati responsabili del trattamento. L'Autorità ha ritenuto che in relazione ai richiamati trattamenti di dati personali, la società avesse assunto il ruolo di titolare del trattamento dal momento che indipendentemente dalla materiale apprensione dei dati, la medesima aveva in concreto determinato le finalità (la veicolazione dei messaggi pubblicitari dei propri prodotti e servizi) e i criteri della campagna promozionale, nonché il contenuto della comunicazione commerciale, con ciò definendo i mezzi essenziali del trattamento stesso.

Gli affiliati, invece, sono stati inquadrati alla stregua di titolari autonomi del trattamento avendo svolto operazioni di trattamento (raccolta e conservazione dei dati) in una fase precedente e del tutto indipendente dalla campagna promozionale pianificata dalla società. L'errata qualificazione di committente "senza ruolo" che la società si era attribuita nel corso del procedimento, inoltre, aveva fatto emergere l'inadeguata gestione delle istanze di esercizio dei diritti degli interessati, nonché l'assenza di verifiche dei consensi asseritamente rilasciati dal reclamante.

Pertanto, con il provvedimento in commento è stato in primo luogo imposto il divieto del trattamento dei dati personali effettuato mediante *network* di affiliazione in assenza di una comprovata acquisizione di un idoneo consenso, anche svolgendo verifiche su campioni congrui rispetto alla mole dei dati trattati. In aggiunta, è stata ingiunta l'adozione di misure tecniche e organizzative finalizzate a facilitare l'esercizio dei diritti degli interessati e a soddisfare, senza ritardo, le relative istanze. Infine, è stata irrogata la sanzione amministrativa pecuniaria pari a euro 60.000,00 tenendo anche in considerazione la circostanza attenuante correlata all'avvenuta definizione della controversia con il pagamento in misura ridotta della sanzione irrogata in ordine al precedente procedimento avviato nei confronti della società e concluso con il provvedimento sanzionatorio adottato dal Garante 15 dicembre 2022, n. 429, doc. web n. 9852290 (provv. 19 dicembre 2024, n. 823, doc. web n. 10110018).

11.1.4. Attivazione illecita di schede telefoniche

Nell'ambito delle attività di contrasto del fenomeno delle attivazioni illecite di SIM *card* e servizi di comunicazione elettronica, il Garante ha adottato un provvedimento

nei confronti di una azienda che gestisce due punti vendita di prodotti di telefonia la cui istruttoria era stata avviata a seguito di un dettagliato rapporto della Guardia di finanza. L'indagine ha rivelato che la società aveva attivato sistematicamente schede SIM, servizi telefonici e vendite di dispositivi mobili all'insaputa dei clienti e senza il loro consenso. I suoi dipendenti, seguendo le direttive dei soci amministratori, avevano utilizzato i dati personali dei clienti, estrapolandoli dai sistemi della compagnia telefonica di riferimento o conservando illegalmente i documenti d'identità, per effettuare le illecite attivazioni. La società aveva anche indotto i clienti a firmare documenti tramite tavolette elettroniche, senza fornire spiegazioni chiare, attivando così servizi non richiesti e addebitando dispositivi mai ricevuti. Tali condotte hanno consentito di ottenere profitti illeciti nell'ordine di varie decine di migliaia di euro. Con il provvedimento in parola è stata inflitta alla società una sanzione amministrativa di euro 150.000,00, pari allo 0,75% della sanzione massima. Questa decisione ha tenuto conto della gravità delle violazioni, della natura intenzionale delle condotte, del numero di persone colpite, dei guadagni illeciti e della mancanza di collaborazione della società con l'Autorità (provv. 22 febbraio 2024, n. 159, doc. web n. 10007895).

Sempre in tema di illecita attivazione di schede telefoniche, l'Autorità ha applicato una sanzione amministrativa pecuniaria ad un'azienda, *dealer* ufficiale di una compagnia telefonica, per aver attivato in tempi diversi più contratti di servizi di telefonia fissa e dati a nome di una cliente, senza che la stessa li avesse richiesti e/o si fosse recata presso il punto vendita del *dealer* e senza quindi seguire le procedure per l'identificazione della clientela. La segnalante, infatti, si era potuta avvedere delle attivazioni solo a seguito di addebiti sul proprio conto corrente e consultando il cassetto fiscale messo a disposizione dei contribuenti dall'Agenzia delle entrate. Nel provvedimento è stato, fra l'altro, evidenziato che deve considerarsi irrilevante la circostanza dedotta dal *dealer* che la violazione sarebbe stata materialmente posta in essere da un addetto che si sarebbe autonomamente discostato dalle procedure ordinariamente seguite. L'azienda infatti, oltre a non aver rivelato le specifiche circostanze di fatto che avevano determinato le indebite reiterate attivazioni, non aveva neanche descritto le misure e gli accorgimenti ordinariamente posti in essere per garantire il corretto svolgimento delle attività di identificazione dei clienti da parte dei propri addetti. La sussistenza di controlli già predisposti dalla compagnia telefonica non esonera il *dealer* dall'effettuare ulteriori attività di controllo e di verifica, potenzialmente più efficaci perché svolte nel contesto delle attivazioni (provv. 27 novembre 2024, n. 735, doc. web n. 10103653).

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

Anche nel corso del 2024, 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.

11.2. Marketing *e profilazione*

Con provvedimento adottato nei confronti di una società attiva nel *marketing* digitale e nella comunicazione *online*, l'Autorità si è occupata di un caso relativo alla raccolta dei dati per finalità di *marketing* e di profilazione in senso stretto e all'*advertisement online*, effettuato direttamente dalla predetta società, nonché mediante la cooperazione con un noto motore di ricerca. Nell'occasione, è stata esaminata la questione dei ruoli svolti nel trattamento dei dati di navigazione da parte dei predetti soggetti. Sono stati considerati

anche ulteriori aspetti, quali la gestione dei consensi per finalità di *marketing* e profilazione; il trattamento di dati di minori in occasione dell'attivazione di *account* di posta elettronica e il trattamento di dati eccedenti (quali il documento di identità) per la chiusura di caselle di posta elettronica, tenuto conto che gli stessi dati, invece, non risultavano richiesti al momento dell'attivazione. L'Autorità ha accertato l'avvenuta violazione della vigente normativa in relazione all'utilizzo di un'unica formula per l'acquisizione del consenso al trattamento per finalità di *marketing* e profilazione, e nel caso in cui l'interessato conferisse tale consenso, di ulteriori *form* già pre-flaggati relativi alle singole finalità (*marketing* e profilazione) e quindi, necessariamente, da deselezionare, ove si intendesse non prestare il consenso per l'una o l'altra di esse. Tale configurazione è risultata in contrasto con il principio della volontà dell'interessato libera e specifica, oltre che informata, comprovabile ed espressa in modo inequivocabile. Peraltro, nel caso di specie, anche l'informativa risultava carente in relazione all'indicazione della finalità di profilazione e dei tempi di conservazione dei dati raccolti mediante i due portali utilizzati dalla società. Poiché quest'ultima aveva proceduto autonomamente a correggere i profili sopra rilevati, si è ritenuto di ingiungere alla medesima società, soltanto con riferimento ai trattamenti connessi alla ricerca in internet condivisi con il motore di ricerca, di fornire un'idonea informativa con la quale descrivere i trattamenti ed i relativi ruoli, anche con riguardo alla gestione dei diritti degli interessati *ex* artt. 15-22 del RGPD. È stata comminata anche una sanzione pecuniaria pari a euro 100.000,00, tenuto conto delle circostanze attenuanti emerse nel corso del procedimento (provv. 22 febbraio 2024, n. 112, doc. web n. 10027096).

L'Autorità ha adottato un provvedimento correttivo e sanzionatorio nei confronti di una nota società che opera nel mercato della grande distribuzione alimentare, originato da una segnalazione in materia di *mailing* indesiderato ed oggetto di opposizione da parte dell'interessato. Con tale provvedimento, l'Autorità ha chiarito che il concetto di *marketing* non può essere ampliato tanto da ricomprendervi anche le peculiari attività statistiche e di analisi economica, strutturalmente diverse da quelle promozionali. Nelle motivazioni del provvedimento in parola il Garante ha ritenuto improprio il rinvio effettuato dalla società ai criteri indicati nelle linee guida del 2013 (provv. 4 luglio 2013, n. 330, doc. web n. 2542348) che prendevano in considerazione unicamente le finalità tipizzate dall'art. 130, comma 1, del Codice, ossia "quelle di invio di materiale pubblicitario, di vendita diretta, di compimento di ricerche di mercato e di comunicazione commerciale […]" ritenendo che solo "le suddette attività – e non anche finalità ulteriori, come quelle di analisi economica e statistica – "siano funzionali, nella maggior parte dei casi, a perseguire un'unica finalità (*lato sensu)* di *marketing,* con la conseguenza che il connesso trattamento appare giustificare – sempre di norma – l'acquisizione di un unico consenso". L'Autorità ha ribadito, inoltre, che un consenso non specifico non è libero in quanto determina una coazione della volontà dell'interessato, con conseguente violazione dei principi di correttezza del trattamento e della libertà di manifestazione del consenso. All'esito dell'istruttoria, pur potendo ritenere che le attività statistiche ed economiche si ponessero in termini di stretta e diretta connessione con quelle di profilazione, poiché necessarie e propedeutiche a quest'ultima, soprattutto di tipo aggregato, l'Autorità ha concluso che tali attività non potevano essere ricomprese nella richiesta di consenso per finalità di *marketing*, poiché così facendo si inficiava la piena manifestazione di volontà riguardante l'effettiva finalità del trattamento. Con riguardo al trattamento dei dati personali raccolti in occasione di "eventi e fiere" (p.e. foto e videoriprese), l'Autorità ha ritenuto di accogliere l'eccezione difensiva formulata dalla società, che ha invocato il principio dell'autonomia contrattuale dei soggetti privati ai sensi dell'art. 1321 c.c., nel senso che la loro "conservazione avviene in base a liberatorie

sottoscritte dagli interessati, le quali includono anche obbligazioni di carattere civilistico (diritto di immagine, uso ai sensi degli artt. 10 e 320 c.c., e artt. 96 e 97, l. n. 633/1941)", garantendo agli interessati l'esercizio dei loro diritti in materia di protezione dei dati. Peraltro, con riguardo al trattamento dei dati personali raccolti mediante le piattaforme *social*, l'Autorità ha chiarito che, se si può ammettere la conservazione quinquennale dei dati relativi "a richieste di informazioni ed assistenza, gestita dall'ufficio di *Customer Care*", con particolare riferimento a quelle presentate dai clienti, altrettanto non può dirsi per i dati relativi a meri utenti, per i quali non sussiste la base giuridica del contratto e non risulta ravvisabile alcuna ragione di necessità (provv. 22 febbraio 2024, n. 130, doc. web n. 10007060).

11.3. Marketing *attraverso dati estratti da pubblici registri e attività promozionale*

Il Garante è tornato nuovamente a censurare l'utilizzo di dati estratti da pubblici elenchi per l'invio di comunicazioni promozionali. Infatti, nonostante le costanti pronunce al riguardo, sono ancora frequenti i casi di titolari, spesso realtà aziendali di piccole dimensioni, che inviano messaggi promozionali via *e-mail* avvalendosi di elenchi estratti da pubblici registri (come INIPEC o albi professionali). Con riguardo all'utilizzo dei dati di contatto pubblicati *online*, il Garante ha più volte ricordato che essi non sono liberamente utilizzabili per finalità promozionali per il solo fatto di essere resi pubblici, poiché deve essere sempre rispettata la finalità di utilizzo in base alla quale i dati sono stati originariamente raccolti (provv. 4 luglio 2024, n. 410, doc. web n. 10070284).

12 Servizi di comunicazioni elettroniche e internet

12.1. *Meta* Election Day Information *(EDI)*

Il 20 giugno 2024 il Garante ha adottato un provvedimento nei confronti di Meta Platforms Ireland Ltd, a conclusione di una complessa e articolata istruttoria risalente al settembre 2022.

Il provvedimento ha riguardato la legittimità dei trattamenti svolti dalla compagnia nell'imminenza delle elezioni per il rinnovo della Camera dei deputati e del Senato della Repubblica, svoltesi domenica 25 settembre 2022. In quella occasione Meta aveva lanciato una nuova funzionalità, Meta *Election Day Information* (EDI), con la quale gli utenti di Facebook e Instagram, cliccando su dei "promemoria" elettorali, venivano reindirizzati al sito web del Ministero dell'interno della Repubblica italiana, dove trovavano "informazioni attendibili sulle elezioni".

A seguito di una istruttoria preliminare, il Garante aveva adottato un primo provvedimento urgente di avvertimento (provv. 21 dicembre 2022, n. 448, doc. web n. 9853406, cfr. Relazione 2022, p. 118) in deroga al meccanismo di cooperazione e quindi con efficacia limitata a soli 3 mesi con cui aveva diffidato formalmente Meta dal procedere alla raccolta e aggregazione di tali dati e alla loro cessione a terzi.

Successivamente, a seguito dell'avvio di una specifica procedura, l'autorità irlandese di protezione dei dati (*Data Protection Commission,* DPC) aveva riconosciuto al Garante la competenza sul caso poiché i trattamenti presi in esame incidevano in modo sostanziale unicamente sugli interessati italiani (conformemente a quanto previsto dall'art. 56, par. 2, RGPD). Nel caso di specie, la peculiarità del diritto di voto nell'ordinamento costituzionale italiano e la normativa interna in materia elettorale giustificavano un impatto prevalentemente localizzato del trattamento posto in essere da Meta e, dunque, la competenza dell'Autorità italiana.

Ottenuto il riconoscimento della competenza locale e con l'approssimarsi del termine del periodo di validità del primo provvedimento, il Garante, il 22 marzo 2023, aveva adottato un secondo provvedimento d'urgenza, volto a imporre una limitazione provvisoria del trattamento (provv. 22 marzo 2023, n. 77, doc. web n. 9879700) nelle more del completamento dell'istruttoria nazionale.

Al termine dell'istruttoria e a seguito delle memorie depositate da Meta, il 20 giugno 2024 il Garante ha adottato il richiamato provvedimento che ha previsto: a) un divieto di trattamento per tutti i dati di utenti italiani raccolti tramite la funzionalità EDI; b) un avvertimento per diffidare Meta dall'applicare EDI ad altre tornate elettorali in Italia in assenza di idonea base giuridica; c) un ammonimento per non aver sufficientemente collaborato con il Garante; d) una sanzione amministrativa pari a euro 25.000.000,00.

L'esercizio di tali incisivi poteri correttivi da parte del Garante si è reso necessario principalmente per l'assenza di una idonea base giuridica del trattamento dei dati degli utenti realizzato tramite EDI e nonostante Meta abbia sostenuto di aver offerto un servizio di valore civico.

Con il provvedimento, infatti, l'Autorità ha chiarito che le finalità civiche avrebbero

dovuto trovare riscontro in una disposizione normativa in grado di investire la società di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ai sensi dell'art. 6, par. 1, lett. e), RGPD e, conseguentemente, dell'art. 2-*ter* del Codice. Riscontro che, nel caso della funzionalità oggetto dell'istruttoria, non è risultato sussistere né nella normativa di settore, né tantomeno nelle delibere dell'autorità di vigilanza in materia elettorale (AGCOM).

Il provvedimento ha, altresì, evidenziato l'assenza nell'ordinamento costituzionale e giuridico italiano di alcun obbligo in capo a soggetti privati come Meta – per di più di diritto straniero – a sollecitare la partecipazione elettorale. Nel contempo, si è sottolineato che la legislazione italiana prevede un regime di particolare attenzione e rigore nella divulgazione di notizie e nello svolgimento di iniziative riconducibili alla materia elettorale, in particolare a ridosso e nelle giornate di apertura dei seggi, al fine di consentire agli elettori di non subire, in tali contesti, indebiti condizionamenti (cd. silenzio elettorale).

Più specificamente, al fine di dare attuazione alle garanzie costituzionali previste a tutela del corretto esercizio del diritto di voto e del pluralismo, le informazioni sulle modalità di voto possono essere veicolate dalle emittenti radiotelevisive pubbliche e private, solo previa espressa autorizzazione, mentre per ciò che riguarda le piattaforme *social*, esse sono espressamente chiamate a far rispettare le disposizioni indicate da AGCOM, come richiamate nel provvedimento, senza prevedere per essi un ruolo attivo.

È stato quindi rilevato che Meta ha svolto un trattamento di dati personali non supportato da idonea base giuridica e quindi illecito sia in relazione ai trattamenti finalizzati all'invio di messaggi informativi riguardanti le elezioni, sia per la raccolta e la conservazione di dati personali degli utenti e delle loro interazioni con le funzionalità EDI. Con riferimento agli ulteriori trattamenti, Meta ha altresì violato i principi di correttezza e di limitazione delle finalità ed ha fornito, nel corso dell'istruttoria, una cooperazione gravemente insufficiente con l'Autorità italiana, in particolare non procedendo alla sospensione provvisoria dei trattamenti, aggravando gli effetti delle condotte illecite e serbando un comportamento non collaborativo.

Il provvedimento è stato trasmesso al Ministero dell'interno e all'AGCOM, al fine di consentire le verifiche di competenza in relazione alla conformità dell'iniziativa di Meta con la disciplina interna in materia di legislazione elettorale di contorno e comunicazione istituzionale. È stata invece demandata alla DPC irlandese la valutazione circa gli aspetti, pur emersi nel corso dell'istruttoria, relativi alla conformità al principio di trasparenza e alla *privacy by design* che interessano la funzionalità EDI nel suo insieme e che, in quanto tali, rientrano nella competenza generale della DPC (provv. 20 giugno 2024, n. 609, doc. web n. 10112606).

12.2. Cookie *e altri strumenti di tracciamento dei dati personali*

Nell'ambito dell'attività di collaborazione instaurata tra il Corpo della Guardia di finanza ed il Garante per la protezione dei dati personali, nel corso del 2024 è proseguita l'intensa attività ispettiva – condotta in modalità remota – finalizzata al controllo e al monitoraggio dell'ottemperanza dei siti web alle indicazioni contenute nel Codice, nel RGPD, nonché nelle linee guida in materia di *cookie* e altri strumenti di tracciamento del 10 giugno 2021 (provv. 10 giugno 2021, n. 231, doc. web n. 9677876).

A tal fine, utilizzando i dati contenuti nell'Anagrafe tributaria e sulla base di criteri predefiniti (dimensioni, ubicazione geografica, categoria merceologica), è stato individuato

un campione di titolari del trattamento destinatari delle attività di accertamento.

All'esito di tali accertamenti, sono state riscontrate numerose violazioni riconducibili a situazioni di mancato adeguamento dei siti web alla più recente normativa oppure alla non corretta configurazione dei *banner* o dei *tool* implementati. In numerose istruttorie è emerso che, nonostante l'avvenuta predisposizione di un *banner* utile al conferimento del consenso, il sito oggetto di accertamento aveva utilizzato soltanto *cookie* di natura prettamente tecnica. In altri casi ancora è stato riscontrato che il titolare aveva mantenuto settaggi risalenti, che rendevano di fatto obbligatorio il conferimento del consenso ai fini della navigazione e/o non consentivano di esprimere un consenso differenziato rispetto alle diverse tipologie di *cookie* utilizzate (cd. principio di granularità e specificità). In un numero ridotto di procedimenti i siti web apparivano totalmente carenti degli accorgimenti richiesti dalla normativa in materia di protezione dei dati personali, stante la totale assenza di *banner* e informativa (provv.ti 12 settembre 2024, n. 556, doc. web n. 10095143; n. 554, doc. web n. 10094911; n. 555, doc. web n. 10094929; n. 557, doc. web n. 10095159; provv.ti 26 settembre 2024, n. 583, doc. web n. 10087270; n. 584, doc. web n. 10088904; n. 585, doc. web n. 10088927; provv.ti 17 ottobre 2024, n. 648, doc. web n. 10090460; n. 649, doc. web n. 10091156; n. 650, doc. web n. 10091178; n. 651, doc. web n. 10091719; provv. 26 ottobre 2024, n. 582, doc. web n. 10087254; provv.ti 13 novembre 2024, n. 667, doc. web n. 10091735; n. 668, doc. web n. 10093443; n. 669, doc. web n. 10093459; n. 670, doc. web n. 10093485; provv.ti 14 novembre 2024, n. 701, doc. web n. 10093533; n. 702, doc. web n. 10093549; provv. 18 novembre 2024, n. 703, doc. web n. 10093567; provv.ti 27 novembre 2024, n. 738, doc. web n. 10108088; n. 739, doc. web n. 10107798).

L'attività di verifica in tale specifico ambito proseguirà anche nel corso del 2025, rappresentando una delle linee di priorità fissate dal Garante nella programmazione dei propri interventi.

12.3. *Trattamento dei dati personali e* age verification

Il Garante, nell'ambito della cooperazione prevista dall'art. 13-*bis*, d.l. 15 settembre 2023, n. 123 convertito, con modificazioni, dalla l. n. 159/2023, recante disposizione per la verifica della maggiore età per l'accesso a siti pornografici, ha fornito all'AGCOM il proprio parere positivo al testo sottoposto (provv. 17 luglio 2024, n. 470, doc. web n. 10056284). In particolare, l'Autorità ha fornito la propria posizione in merito ad alcuni aspetti di dettaglio che hanno contribuito alla descrizione del sistema proposto da AGCOM che, per la fornitura della prova della maggiore età, prevede l'intervento di soggetti terzi indipendenti certificati e due passaggi logicamente separati: identificazione e successiva autenticazione della persona identificata e ciò per ciascuna sessione di utilizzo del servizio regolamentato (cioè, la fornitura di contenuti pornografici tramite sito o piattaforma web).

12.4. *Attività in materia di trattamento dati mediante sistemi di intelligenza artificiale*

L'Autorità ha proseguito l'attività di cooperazione in ambito europeo, in seno alla *task force* dell'EDPB, costituita *ad hoc* per affrontare in modo coordinato le tematiche connesse al trattamento dei dati personali sotteso al funzionamento dei servizi di IA generativa offerti dal titolare.

12

Con riferimento al trattamento dei dati personali attraverso servizi che si basano su LLM *(large language model*) l'Autorità ha adottato, ai sensi dell'art. 58, par. 2, lett. a), RGPD e dell'art. 154, comma 1, lett. f), del Codice, un provvedimento con cui ha avvertito un titolare del trattamento che l'accordo di comunicazione dei contenuti editoriali che, secondo notizie stampa, sarebbe stato stipulato con una società che gestisce un noto modello di IA relazionale, avrebbe potuto configurare una violazione delle disposizioni di cui agli artt. 9, 10, 13, 14 e del Capo III del RGPD (provv. 27 novembre 2024, n. 741, doc. web 10077129).

In esito all'indagine conoscitiva in materia di web *scraping* lanciata nel dicembre 2023 (doc. web n. 9972593), l'Autorità ha pubblicato una "Nota informativa in materia di web *scraping*, per finalità di addestramento di IA generativa e di possibili azioni di contrasto a tutela dei dati personali" ai sensi dell'art. 57, par. 1, lett. b), RGPD, con l'obiettivo di fornire ai gestori di siti internet e di piattaforme *online*, sia pubblici che privati, informazioni sul fenomeno della raccolta massiva di dati personali dal web per finalità di addestramento dei modelli di IA generativa ed indicare possibili azioni di contrasto che tali gestori, quali titolari del trattamento dei dati personali oggetto di pubblicazione, potrebbero implementare al fine di prevenire la raccolta di dati da parte di terzi per finalità di addestramento dei modelli di IA (provv. 20 maggio 2024, n. 329, doc. web n. 10020316).

12.5. *"Monetizzazione" dei dati personali*

Il Garante, al termine di una lunga attività istruttoria e di cooperazione europea, ha adottato un provvedimento con il quale ha affrontato il tema della cd. monetizzazione dei dati personali, traendo spunto dall'attività di una società italiana che ha realizzato una piattaforma web che consente agli utenti di mettere a disposizione i propri dati, anche acquisiti mediante portabilità dalla grande distribuzione organizzata e dalle aziende *big tech*, per sottoporli ad arricchimento e profilazione, nonché per veicolare promozioni commerciali. Attraverso la piattaforma, l'utente che conferisce i propri dati personali per le attività sopra indicate percepisce dei proventi economici in proporzione alla quantità di informazioni messe a disposizione e dei contatti promozionali conseguentemente ricevuti. Con il provvedimento, l'Autorità ha ritenuto non corretto l'utilizzo dell'art. 6, par. 1, lett. b), RGPD come base giuridica per il trattamento sopra descritto, affermando che il trattamento dei dati nel caso in argomento sia l'oggetto stesso del contratto e non uno strumento per la sua esecuzione e ribadendo che la "necessarietà" del trattamento deve essere intesa in senso strumentale e non negoziale. L'Autorità ha affermato che, quando il trattamento non è necessario per l'esecuzione di un contratto, è più appropriato che lo stesso si basi sul consenso (artt. 6, par. 1, lett. a) e 9, par. 2, lett. a), RGPD) purché questo sia specifico, inequivocabile, informato, liberamente prestato e sempre revocabile e ha evidenziato il rischio che il modello preso in esame, basato su una remunerazione in cambio di dati, potesse compromettere la libertà del consenso, in particolare per le persone vulnerabili. L'Autorità ha quindi formulato un ammonimento nei confronti del titolare della piattaforma, attesa la novità della materia, che ha indotto a non applicare nei confronti del medesimo titolare una sanzione amministrativa pecuniaria: ha tuttavia imposto il divieto di ogni ulteriore trattamento dei dati acquisiti in forza dei contratti oggetto del provvedimento (provv. 14 novembre 2024, n. 704, doc. web n. 10108848).

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

Nel corso dell'anno di riferimento il settore del lavoro privato e pubblico è stato oggetto di numerosi provvedimenti ed iniziative da parte dell'Autorità di seguito sinteticamente menzionati in un quadro generale e più diffusamente esaminati nei paragrafi successivi.

Sotto il profilo della disciplina in materia di protezione dei dati personali, vale il principio generale, più volte richiamato nei provvedimenti dell'Autorità, per cui nell'ambito di rapporti di lavoro/collaborazione, il datore di lavoro, che riveste la qualifica di titolare del trattamento, può trattare lecitamente i dati personali dei propri dipendenti, di regola, solo se il trattamento è necessario per la gestione del rapporto stesso in base a quanto previsto dalle leggi, dai regolamenti e dalle disposizioni dei contratti collettivi applicabili e/o del contratto di lavoro individuale oppure se è necessario per adempiere a specifici obblighi o compiti posti dalle discipline di settore applicabili (art. 6, par. 1, lett. b) e c), RGPD, con riferimento ai dati cd. comuni, e art. 9, par. 2, lett. b), RGPD con riferimento alle categorie particolari di dati).

Il Garante, nell'ambito dell'attività di controllo nel settore del *food delivery* sui trattamenti di dati personali dei corrieri (cd. *rider*) che effettuano attività di consegna di beni (cibo e altri prodotti) ai clienti, ha adottato un provvedimento nei confronti di una società che organizza l'attività lavorativa degli stessi mediante sistemi algoritmici, nei cui confronti già nel 2021 aveva adottato un provvedimento sanzionatorio e prescrittivo.

Altri interventi rilevanti hanno riguardato l'approvazione del codice di condotta promosso dall'Associazione nazionale delle agenzie per il lavoro avente ad oggetto i trattamenti effettuati dalle agenzie per il lavoro in fase preassuntiva e l'accreditamento del relativo Organismo di monitoraggio di cui all'art. 41 del RGPD.

Numerosi sono stati i provvedimenti adottati, nell'ambito dei trattamenti relativi al rapporto di lavoro, in materia di esercizio dei diritti, in particolare diritto di accesso ai dati *ex* art. 15 del RGPD e diritto alla cancellazione dei dati ai sensi dell'art. 17 del RGPD.

Il Garante si è occupato di verificare la conformità dei trattamenti relativi all'*account* di posta elettronica aziendale individualizzato e quelli effettuati tramite sistemi di videosorveglianza alla disciplina in materia di protezione dei dati personali ed ha adottato molteplici provvedimenti nei confronti di titolari per il trattamento di dati biometrici (riconoscimento facciale) dei lavoratori per finalità di registrazione della presenza in servizio.

Infine, si segnala che l'Autorità è intervenuta in relazione a una violazione di dati personali di circa 25.000 interessati notificata ai sensi dell'art. 33 del RGPD da parte di una società che aveva subito un attacco informatico di tipo *ransomware* con esfiltrazione (e successiva pubblicazione nel *dark web*) di *file* contenenti dati personali.

13.1. *Trattamenti di dati effettuati mediante piattaforme digitali*

Il Garante ha proseguito l'attività di controllo sui trattamenti di dati personali dei corrieri effettuati da soggetti economici italiani che operano sul territorio nazionale nel settore del *food delivery* attraverso piattaforme digitali che organizzano l'attività di consegna di beni ai clienti mediante sistemi algoritmici (v. Relazione 2021, p. 147).

13

In particolare nel 2022 l'Autorità aveva avviato un'istruttoria, avvalendosi anche del Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza, nei confronti di una società già destinataria di un provvedimento nel 2021, a seguito di notizie di stampa relative all'avvenuta disconnessione dell'*account* di un *rider* morto in un incidente stradale avvenuto durante l'effettuazione di una consegna per conto della stessa società.

A seguito di una dettagliata segnalazione di un gruppo di esperti informatici in relazione al funzionamento dell'*app* utilizzata dai *rider*, sono state effettuate approfondite attività di controllo anche sui dati raccolti dalla società attraverso la predetta *app*.

A completamento dell'attività istruttoria il Garante ha accertato che la società aveva effettuato trattamenti nei confronti di un grande numero di *rider* (circa 36.000 attivi alla fine del 2022), attraverso una piattaforma digitale, in violazione di numerose disposizioni del RGPD. In primo luogo, il Garante ha accertato che la società, attraverso la piattaforma digitale, aveva effettuato diversi trattamenti automatizzati dei dati dei *rider* (ai sensi dell'art. 22 del RGPD). Fra tali trattamenti automatizzati, l'attribuzione ai *rider* di un punteggio consentiva di prenotare con priorità il turno di lavoro (*slot*) ed operava sulla base di quattro parametri elaborati dalla piattaforma digitale ed aventi un peso diverso in base alle diverse città di riferimento. In proposito il Garante ha accertato che i *rider* non potevano liberamente prenotare, tra gli *slot* proposti, il turno di lavoro prescelto, posto che alcuni turni, specialmente quelli che garantiscono maggiori occasioni di lavoro e di guadagno, risultavano saturati al 100%, con conseguente impossibilità dell'accesso agli stessi per coloro che ottenevano un punteggio inferiore. Anche attraverso l'algoritmo che consentiva l'assegnazione degli ordini all'interno dello *slot*, la società aveva assunto decisioni, basate unicamente su un trattamento automatizzato, fondato, in questo caso, sull'operatività di cinque parametri.

Inoltre, ulteriori decisioni basate su un trattamento esclusivamente automatizzato erano state assunte dalla società in occasione quantomeno di alcune ipotesi di blocco o disconnessione dalla piattaforma, che si attivavano al ricorrere di condizioni determinate dall'esito del trattamento di dati raccolti ed elaborati dalla piattaforma stessa.

L'Autorità ha verificato che tali trattamenti automatizzati incidevano significativamente sugli interessati aumentando o riducendo significativamente le occasioni di lavoro offerte tramite la piattaforma oppure impedendo di effettuare le prestazioni lavorative oggetto del contratto con il *rider* (nei casi di blocco e disconnessione dalla piattaforma).

All'esito degli accertamenti è stata altresì verificata l'assenza di interventi umani significativi all'interno dei processi decisionali, con conseguente applicazione dell'obbligo per il titolare di adottare misure a tutela dei diritti e delle libertà degli interessati stabilito dall'art. 22 del RGPD: oltre a quanto già espressamente stabilito dal richiamato art. 22, ossia assicurare agli interessati, quantomeno, il diritto di ottenere l'intervento umano nel processo decisionale, di esprimere la propria opinione e di contestare la decisione, anche garantire un'adeguata formazione degli operatori addetti, nonché la possibilità per gli stessi di ignorare, se del caso, l'*output* del processo algoritmico, per evitare la possibile tendenza a farvi automaticamente affidamento, così da preservare una reale significatività all'intervento umano.

È stata inoltre prescritta la verifica periodica della correttezza ed accuratezza dei risultati dei sistemi algoritmici, anche al fine di minimizzare il rischio di errori nonché l'utilizzo di dati eccedenti, non aggiornati o inesatti. La società dovrà poi introdurre strumenti di verifica per evitare usi impropri e discriminatori dei meccanismi reputazionali basati su *feedback*.

Con il provvedimento è stato anche accertato che società terze a cui è stata affidata, in qualità di sub-responsabili del trattamento, la fornitura di servizi connessi all'operatività della piattaforma, avevano trattato dati personali riferiti ai *rider*, tra i quali la posizione

geografica, non necessari rispetto alle finalità perseguite e, talvolta, con modalità di trattamento addirittura non note alla stessa società titolare del trattamento.

In relazione ai dati riferiti alla posizione geografica dei *rider* è emerso, in particolare, che la raccolta e l'invio a terze parti di tali dati era avvenuto anche quando il *rider* non era operativo nel periodo di lavoro assegnato (*slot*), l'*app* era in *background* e, perlomeno fino al 22 agosto 2023, anche quando l'*app* non era attiva.

Ampio spazio è stato poi dedicato alla scarsa trasparenza, in particolare, dei trattamenti automatizzati e dei sistemi algoritmici utilizzati, in violazione del principio generale di trasparenza e correttezza dei trattamenti e dell'obbligo per il titolare di fornire elementi informativi sulle caratteristiche essenziali dei trattamenti stessi (artt. 12 e 13 del RGPD). Il riscontrato *deficit* di trasparenza aveva violato, oltre al RGPD, anche gli specifici obblighi informativi disposti dal legislatore nazionale in caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati nell'ambito del rapporto di lavoro (art. 1-*bis,* d.lgs. n. 152 /1997, introdotto dall'art. 4 comma 1, lett. b), d.lgs. n. 104/2022 di attuazione della direttiva (UE) 2019/1152, mod. con d.l. 4 maggio 2023, n. 48, conv. in l. 23 luglio 2023, n. 85).

L'Autorità ha, inoltre, impartito alla società il divieto dell'ulteriore trattamento dei dati biometrici dei *rider*, in particolare mediante riconoscimento facciale, per essere stato effettuato in assenza delle condizioni di liceità previste dall'ordinamento (art. 5, par. 1, lett. a), 9, par. 2, lett. b, RGPD; art. 2-*septies* del Codice).

Infine, in base all'esame delle complessive attività di trattamento effettuate dalla società nell'ambito di un rapporto di lavoro disciplinato da un contratto-tipo, il Garante ha accertato che la società, pur avendo effettuato un sistematico controllo della prestazione lavorativa svolta dai *rider*, attraverso le impostazioni e le funzionalità di strumenti tecnologici che operano a distanza (piattaforma digitale, *app*, sistemi di registrazione delle comunicazioni), non si era conformata a quanto in proposito stabilito dall'art. 4, comma 1, l. n. 300/1970, posto che non aveva verificato la riconducibilità degli strumenti utilizzati alle finalità tassativamente ammesse dall'ordinamento (esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale), né aveva attivato la procedura di garanzia prevista in caso di sussistenza di una delle predette finalità (accordo collettivo stipulato con le rappresentanze sindacali o, in mancanza, autorizzazione dell'Ispettorato nazionale del lavoro).

Successivamente alla notifica del provvedimento, su richiesta della società che aveva rappresentato di voler cooperare con l'autorità di controllo, il Garante ha accordato una proroga dei termini stabiliti per adempiere alle prescrizioni impartite con il provvedimento (provv.ti 13 novembre 2024, n. 675, doc. web n. 10074601; 19 dicembre 2024, n. 818, doc. web n. 10105535).

13.2. *Il codice di condotta delle agenzie per il lavoro*

Il Garante ha approvato il codice di condotta promosso dall'Associazione nazionale delle agenzie per il lavoro (Assolavoro) all'esito di una lunga e articolata collaborazione con i proponenti nella delicata materia dei trattamenti effettuati dalle agenzie per il lavoro per lo più in occasione delle attività di intermediazione, ricerca e selezione del personale e supporto alla ricollocazione professionale (v. artt. 40 e 41 del RGPD relativi a codici di condotta e controllo sui codici approvati).

Il codice di condotta, composto da 18 articoli e 2 allegati (modelli di "registro trattamenti tipici" e di "Informativa sul trattamento dei dati personali dei candidati"), riguarda i trattamenti di dati personali effettuati in fase preassuntiva, in relazione ai quali

l'esigenza di tutela dei diritti e delle libertà dei candidati è particolarmente avvertita dall'Autorità, considerato anche il rischio che l'accesso alle occasioni di lavoro possa essere condizionato da informazioni idonee ad esporre gli interessati a discriminazioni.

Con riguardo al contenuto del codice di condotta, si segnala in primo luogo l'esclusione, dall'ambito delle categorie di dati lecitamente trattati, delle informazioni non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore, conformemente a quanto previsto in via generale dall'art. 113 del Codice (che richiama gli artt. 8, l. 20 maggio 1970, n. 300 e 10, d.lgs. 10 settembre 2003, n. 276 come condizione di liceità dei trattamenti effettuati). In vista di una possibile assunzione, è pertanto vietato trattare informazioni relative alle opinioni politiche, religiose o sindacali, oppure relative al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, all'età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonché ad eventuali controversie con i precedenti datori di lavoro.

Il codice di condotta precisa poi che, conformemente al principio generale di limitazione della finalità (art. 5, par. 1, lett. b), RGPD), il trattamento dei dati contenuti sui profili *social* dei candidati non può essere basato solo sulla circostanza che tali profili siano "disponibil[i] al pubblico". In ambito preassuntivo le informazioni possono essere raccolte esclusivamente se rese disponibili su canali *social* che abbiano natura professionale, limitatamente alle sole informazioni connesse all'attitudine professionale al lavoro, nel rispetto del principio di minimizzazione (art. 5, par. 1, lett. c), RGPD), e sempre che la raccolta sia "necessaria e pertinente allo svolgimento del lavoro per il quale si effettua la ricerca".

Considerato che i *social network* di natura professionale costituiscono strumenti attraverso i quali gli utenti condividono informazioni relative ai percorsi di studio e di formazione, alle attitudini e alle esperienze professionali, la finalità perseguita dalle agenzie per il lavoro non è incompatibile con tali scopi, sempre che siano rispettati gli altri principi generali del trattamento. Diversamente, è proprio attraverso la consultazione di profili *social* generalisti, finalizzati alle comunicazioni interpersonali tra gli utenti, che è possibile accedere a informazioni il cui trattamento è invece vietato dal nostro ordinamento nel contesto lavorativo e preassuntivo (alla luce di quanto stabilito dal richiamato art. 113 del Codice).

Altro profilo delicato, dal punto di vista della protezione dei dati, riguarda la prassi, invalsa presso le agenzie per il lavoro, di contattare il precedente datore del candidato al fine di verificare e valutare le sue referenze professionali. Considerato che il trattamento di informazioni riferite ad *ex* dipendenti in tale circostanza presenta alcuni rischi per gli interessati (in particolare con riferimento alla base giuridica del trattamento, al rispetto delle discipline antidiscriminazione, all'informativa e ai tempi di conservazione), nel codice di condotta si precisa che le agenzie per il lavoro possono acquisire referenze professionali del candidato presso precedenti datori di lavoro e comunicarle ai propri clienti (per conto dei quali è effettuata la ricerca di personale) solo "previa autorizzazione esplicita del candidato". In ogni caso non possono essere trattate informazioni relative a illeciti disciplinari o a "procedimenti giudiziari che abbiano coinvolto il candidato", ad esclusione dei casi in cui ciò sia previsto da una disposizione di legge.

Qualora le attività di ricerca e selezione di personale si avvalgano di decisioni basate unicamente su un trattamento automatizzato, il codice di condotta precisa che le agenzie per il lavoro dovranno effettuare una valutazione di impatto ai sensi dell'art. 35 del RGPD. Inoltre, alla luce dell'obbligo per il titolare di predisporre misure appropriate per tutelare i diritti e le libertà degli interessati previsto dall'art. 22, par. 2, RGPD, il codice di condotta chiarisce che, all'interno dell'informativa rilasciata agli interessati,

dovranno essere fornite indicazioni relative "ai meccanismi posti alla base dell'automatizzazione" e alle "valutazioni periodiche che vengono poste in essere per verificare l'affidabilità" del sistema automatizzato, anche in relazione "alla correttezza ed accuratezza dei risultati dei sistemi algoritmici nonché per verificare che il rischio di errori sia minimizzato". Tali verifiche devono riguardare altresì la conformità alle disposizioni in materia di divieto di discriminazione.

Con il provvedimento adottato, il Garante ha anche accreditato l'Organismo di monitoraggio al quale è rimessa la verifica del rispetto del codice di condotta da parte degli aderenti, ivi compresa l'adozione di misure correttive o interdittive nei confronti di questi ultimi, fatti salvi i compiti e i poteri attribuiti all'Autorità (provv. 11 gennaio 2024, n. 12, doc. web n. 9983415, in G.U. 6 marzo 2024, n. 55).

13.3. *Riconoscimento facciale per finalità di rilevazione della presenza dei lavoratori*

Nel 2024 il Garante, a seguito di alcuni reclami, ha adottato cinque provvedimenti nei confronti di altrettante società che avevano installato dispositivi biometrici basati sul riconoscimento facciale allo scopo di rilevare la presenza in servizio dei lavoratori che operavano presso lo stesso sito industriale.

In particolare, l'Autorità ha accertato che le società utilizzavano, per la verifica della presenza in servizio dei propri dipendenti, un sistema di autenticazione biometrica basato sul riconoscimento del volto che tra l'altro prevedeva la condivisione del *database* contenente l'elenco dei rispettivi dipendenti (di tre delle predette società) e comunque il trattamento da parte di una delle società dei dati relativi anche ai dipendenti delle altre quattro (in assenza di base giuridica).

Dopo aver chiarito che vi è trattamento di dati biometrici sia in occasione del riconoscimento biometrico che nella precedente fase di estrazione e registrazione delle caratteristiche biometriche (cd. *enrolment*), l'Autorità ha ribadito che i dati biometrici, poiché rientrano nel novero dei dati "particolari", possono essere lecitamente trattati in ambito lavorativo solo se il trattamento "sia autorizzato dal diritto dell'Unione o degli Stati membri […] in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. b), e cons. nn. 51-53 del RGPD).

Il Garante ha pertanto confermato che, allo stato, l'ordinamento non prevede il trattamento di dati biometrici dei dipendenti per finalità di rilevazione della presenza in servizio. Inoltre, in base all'art. 2-*septies* del Codice, i dati biometrici possono essere trattati solo in conformità alle misure di garanzia disposte dal Garante (v. art. 9, par. 4, RGPD).

L'Autorità ha anche ritenuto non conforme ai principi di minimizzazione e proporzionalità del trattamento (art. 5, par. 1, lett. c), RGPD) l'adozione di un sistema di riconoscimento facciale nell'ambito dell'ordinaria gestione del rapporto di lavoro, considerato che al fine di poter contabilizzare le effettive ore di lavoro prestate e di accertare la presenza dei lavoratori sul luogo di lavoro avrebbero potuto essere adottate misure meno invasive per i diritti degli interessati (es. controlli automatici mediante *badge*, verifiche dirette, etc.).

È stato ribadito che i titolari del trattamento, in base al principio di responsabilizzazione, sono tenuti ad osservare i principi generali del trattamento e pertanto non possono limitarsi a fare affidamento su attestazioni di presunta conformità al RGPD che, nel caso concreto, erano state fornite dal produttore e dal fornitore dei dispositivi di riconoscimento facciale.

In conclusione, con i predetti provvedimenti sono state accertate una pluralità di violazioni, relative anche all'omessa informativa, alla mancata adozione di misure di sicurezza e predisposizione di una valutazione di impatto, nonché alla violazione delle disposizioni relative alla designazione dei responsabili del trattamento, effettuate nei

confronti di un numero rilevante di lavoratori (più di 470) (provv.ti 22 febbraio 2024, n. 105, doc. web n. 9995680; n. 106, doc. web n. 9995701; n. 107, doc. web n. 9995741; n. 108, doc. web n. 9995762 e n. 109, doc. web n. 9995785).

In un diverso caso, il Garante, a seguito di un reclamo, ha adottato un provvedimento di divieto nei confronti di una società che aveva installato un dispositivo biometrico basato sul riconoscimento facciale allo scopo di rilevare la presenza in servizio dei lavoratori che operavano presso le due sedi aziendali. A seguito dell'accertamento ispettivo svolto presso la sede della società, è stato verificato che il sistema di rilevamento biometrico coinvolgeva un numero discreto di dipendenti (circa 40 lavoratori impiegati presso le due sedi operative) ed era stato avviato da circa 4 anni.

L'Autorità, ribaditi i principi ormai consolidati nella materia in parola, le condizioni e i presupposti di liceità di cui all'art. 9, par. 2, lett. b), RGPD e art. 2-*septies* del Codice, ha accertato che il trattamento di dati biometrici dei dipendenti era stato effettuato in assenza di un'idonea base giuridica, in violazione dell'art. 9, par. 2, lett. b), RGPD, nonché a fronte di un'informativa inidonea in violazione dell'art. 13 del RGPD ed ha applicato una sanzione amministrativa pecuniaria (provv. 6 giugno 2024, n. 338, doc. web n. 10029500).

13.4. *Violazione di dati personali*

Nell'anno di riferimento il Garante ha adottato un provvedimento nei confronti di una società a seguito della notifica di una violazione di dati personali ai sensi dell'art. 33 del RGPD, relativa a un attacco informatico, di tipo *ransomware,* che ha comportato l'esfiltrazione (e la successiva pubblicazione nel *dark web*) di *file* contenenti dati personali afferenti ai lavoratori dell'azienda (inclusi lavoratori cessati), ai loro congiunti, ai titolari di cariche societarie, a candidati a posizioni lavorative, nonché a esponenti delle imprese intrattenenti rapporti commerciali con la società. Per alcuni dati si è verificata anche la perdita di disponibilità.

La violazione ha riguardato nel complesso circa 25.000 interessati e le categorie di dati personali oggetto di violazione sono state molteplici (dati anagrafici; dati di contatto; dati di accesso e di identificazione; dati di pagamento; dati relativi a condanne penali e ai reati; dati relativi a documenti di identificazione/riconoscimento; dati che rivelano l'appartenenza sindacale; dati relativi alla salute).

In particolare, con il provvedimento in esame, è stata accertata la violazione dell'art. 33 del RGPD in quanto, nonostante la rilevanza del *data breach* subito, il titolare del trattamento aveva trasmesso all'Autorità una notifica delle violazioni incompleta, perché priva degli elementi ritenuti necessari per l'esercizio, da parte del Garante, dei compiti e dei poteri previsti dal RGPD. È essenziale, cioè, che la segnalazione includa tutte quelle informazioni necessarie per individuare le caratteristiche dell'incidente informatico da cui ha avuto origine la violazione dei dati: elementi necessari per consentire al Garante, al verificarsi di una violazione di dati, di esercitare i suoi poteri e appurare che siano state messe in atto le misure tecnologiche e organizzative adeguate alla fattispecie concreta, anche nell'ottica di ripristinare un adeguato livello di protezione dei dati personali violati.

Nel caso specifico, è emerso che nella segnalazione trasmessa dalla società non vi era l'indicazione dei *server* impattati, della tipologia di vulnerabilità sfruttata dall'attaccante e di alcuni elementi in merito alla *kill chain* dell'attacco.

È stata riscontrata inoltre la violazione degli artt. 5, par. 1, lett. f) e 32 del RGDP per non avere la società tenuto una condotta conforme agli obblighi previsti dalla disciplina di protezione dei dati relativamente all'adozione di misure tecniche e organizzative

adeguate a garantire un livello di sicurezza adeguato al rischio. In proposito l'Autorità ha sottolineato come le vulnerabilità sfruttate dagli attaccanti per porre in essere la violazione fossero state da tempo rese note, unitamente alle misure di contenimento, dal Microsoft *Security Response Center* e dall'Agenzia per la cybersicurezza nazionale.

Questa condotta da parte della società aveva violato i principi di protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita di cui all'art. 25 del RGPD, in quanto le predette misure rientrano tra le misure che un titolare del trattamento deve adottare per integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del RGPD, nonché per assicurare che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità del trattamento.

Peraltro, la rilevata adozione da parte del titolare di soluzioni alternative (*workaround*) che, per loro natura, sono da considerarsi temporanee e di emergenza e la conseguente mancata attività di aggiornamento di tutti i sistemi, nonostante non sia stata direttamente la causa dell'attacco perpetrato nei confronti del titolare, li ha senz'altro resi più vulnerabili rispetto ai rischi incombenti.

Per tali motivi è stato accertato che la società, in violazione degli artt. 5, par. 1, lett. f), 25 e 32 del RGPD, non era stata in grado di assicurare, su base permanente, la riservatezza, l'integrità e la resilienza dei sistemi e dei servizi di trattamento e non aveva adottato un'idonea procedura finalizzata a verificare regolarmente l'efficacia delle misure tecniche applicate ad essi.

L'Autorità ha pertanto disposto una sanzione amministrativa pecuniaria oltre a una pluralità di prescrizioni; tra l'altro, ha ingiunto al titolare la predisposizione di una procedura formalizzata per la gestione delle vulnerabilità, che preveda la pianificazione del controllo di tutti gli asset IT dell'organizzazione al fine di rilevare l'eventuale presenza di vulnerabilità note o potenziali nonché l'individuazione delle relative procedure di correzione e mitigazione (provv. 4 luglio 2024, n. 572, doc. web n. 10063782).

13.5. *Esercizio dei diritti*

Diritto di accesso

Con alcuni provvedimenti il Garante ha ribadito che l'omesso o l'inidoneo riscontro (ad es. perché parziale o meramente interlocutorio) all'esercizio del diritto di accesso da parte del lavoratore costituisce violazione dell'art. 15 del RGPD.

Infatti i dati trattati dal datore di lavoro in qualità di titolare del trattamento (nei casi oggetto delle decisioni in esame, le informazioni contenute nel libro unico del lavoro e nel fascicolo personale di valutazione della *performance*, le timbrature delle presenze effettuate mediante il *badge* aziendale) devono essere forniti all'interessato nei termini e con le modalità prescritte dall'art. 12 del RGPD, anche qualora i dati richiesti siano già stati posti nella disponibilità dell'interessato o gli siano già stati consegnati. Il RGPD non prevede alcuna limitazione alle informazioni riferite all'interessato che possono essere oggetto di accesso, anzi consente di presentare più richieste, salva la possibilità per il titolare del trattamento, in caso di richieste "eccessive, in particolare per il loro carattere ripetitivo", di addebitare un contributo spese (v. art. 12, par. 5, RGPD).

La responsabilità del titolare che non risponde alle richieste di accesso ai dati non viene meno, poi, in caso di errori o disguidi nella loro gestione interna all'azienda, posto che spetta al titolare l'adozione di misure anche organizzative volte ad agevolare la presentazione e la gestione delle istanze di esercizio dei diritti (v. art. 12, par. 2, RGPD).

In termini generali, infine, il titolare non può richiedere un formato specifico per le istanze di esercizio del diritto oppure stabilire specifici requisiti che gli interessati debbano osservare nella scelta di un canale di comunicazione per veicolare la richiesta

stessa (v. sul punto linee guida 01/2022 sui diritti degli interessati - diritto di accesso, CEPD, del 28 marzo 2023) (provv.ti 24 aprile 2024, n. 245, doc. web n. 10018813; 26 settembre 2024, n. 589, doc. web n. 10066287).

A seguito di un reclamo con il quale era stato lamentato che, una volta cessato il rapporto di lavoro, il titolare non avrebbe consentito in modo adeguato l'esercizio del diritto di accesso a dati riferiti all'interessato attinenti al rapporto di lavoro, il Garante ha adottato un provvedimento con cui ha disposto una sanzione amministrativa pecuniaria.

È stato accertato che il titolare del trattamento, a fronte dell'istanza di accesso ai dati presentata dal reclamante e reiterata (con integrazioni), aveva fornito un riscontro inidoneo in quanto incompleto: solo nel corso dell'istruttoria svolta dinanzi all'Autorità, infatti, il titolare aveva trasmesso alcune delle informazioni richieste e non indicate in precedenza nonché documentazione non consegnata con il riscontro fornito. Alla luce di quanto prevede l'art. 12 del RGPD ove il titolare ottemperi solo in parte all'istanza di accesso, ossia l'obbligo di informare l'interessato entro un mese dei motivi specifici di tale parziale riscontro nonché di indicare i rimedi esperibili dall'interessato per opporsi, come ricordato anche nelle linee guida 01/2022 sopra richiamate, il Garante ha pertanto accertato che il titolare del trattamento aveva violato gli artt. 12 e 15 del RGPD (provv. 12 dicembre 2024, n. 833, doc. web n. 10107187).

Il Garante ha altresì adottato, nei confronti di una società, un provvedimento con cui ha disposto una sanzione amministrativa pecuniaria per non avere la stessa, in qualità di titolare del trattamento, dato idoneo riscontro all'istanza di accesso *ex* art. 15 del RGPD presentata dal reclamante in merito ad attestati di formazione ed avere pertanto violato anche l'art. 12 RGPD.

Infatti, solo a seguito dell'avvio dell'istruttoria da parte dell'Autorità, la società aveva dichiarato di non essere più in possesso degli attestati richiesti e si era attivata per il recupero degli stessi tramite i soggetti che si erano occupati della formazione per conto del titolare.

Al riguardo, il Garante ha in particolare rammentato che gli attestati di formazione del lavoratore contengono dati personali riferiti allo stesso ai quali l'interessato ha diritto di accedere ai sensi dell'art. 15 del RGPD ed anche in questa occasione ha richiamato le predette linee guida 01/2022 (v. par. 5.2.5, punto 155) (provv. 28 aprile 2024, n. 246, doc. web n. 10021452).

Un caso particolare ha riguardato un reclamo presentato nei confronti di un istituto di credito, alle cui dipendenze il reclamante aveva prestato la propria attività lavorativa, poi oggetto di fusione per incorporazione. L'Autorità, visto l'art. 2504-*bis* c.c. e considerate le prescrizioni in materia di operazioni di fusione e scissione fra società adottate dall'Autorità (provv. 8 aprile 2009, doc. web n. 1609999), ha accertato la violazione in capo alla società incorporante per non avere fornito idoneo riscontro all'istanza di accesso ai dati contenuti nel fascicolo personale. Tale istanza, in particolare, era stata formulata per conoscere quali informazioni potevano aver dato origine ad una sanzione disciplinare nei suoi confronti.

L'Autorità ha avuto modo di chiarire, in primo luogo, che sulla base delle disposizioni di cui agli artt. 12 e 15 del RGPD, non vi è necessità per gli interessati di indicare un motivo o una particolare esigenza per giustificare le proprie richieste di esercizio dei diritti, né risulta riconosciuta al titolare del trattamento la possibilità di chiedere i motivi della richiesta. In secondo luogo, si è precisato che, rispetto al formato con cui i dati devono essere resi disponibili all'istante, spetta al titolare del trattamento, nell'ambito del principio di *accountability*, il compito di individuare la forma più completa e soddisfacente con cui riscontrare le istanze di accesso. Nel caso di specie, la consegna

della documentazione contenente i dati personali del reclamante sottesa al procedimento disciplinare costituiva l'unica modalità idonea a consentire l'accesso secondo i principi di correttezza e trasparenza (provv. 7 marzo 2024, n. 137, doc. web n. 10007853).

In due distinti casi, l'Autorità ha poi accertato la violazione degli artt. 12 e 15 del RGPD in capo a due titolari del trattamento che avevano motivato il rifiuto all'accesso ai dati da parte di *ex* dipendenti per il timore che potessero essere carpiti segreti aziendali.

L'Autorità, all'esito dei rispettivi procedimenti, tenuto conto che la restrizione al diritto di accesso prevista dall'art. 15, par. 4, RGPD è sì riferita al "segreto industriale e aziendale e [al]la proprietà intellettuale", ma che essa non deve comportare il diniego a fornire all'interessato tutte le informazioni, anche alla luce del cons. 63 del RGPD, ha evidenziato la necessità per il titolare del trattamento di operare un bilanciamento tra i contrapposti interessi, adottando misure appropriate in grado di mitigare i rischi per i diritti e le libertà altrui, come la cancellazione delle informazioni eccedenti che non si riferiscono all'interessato, nel rispetto del principio di proporzionalità (v. linee guida 01/2022 cit., EDPB, par. 165 e ss.) (provv.ti 20 giugno 2024, n. 380, doc. web n. 10043600; 27 novembre 2024, n. 732, doc. web n. 10101221).

Diritto di cancellazione

Costituisce oggetto di ulteriore casistica sottoposta all'Autorità l'omesso o inidoneo riscontro del datore di lavoro a richieste di cancellazione ai sensi dell'art. 17 del RGPD per lo più presentate da *ex* dipendenti con riguardo alla casella di posta elettronica aziendale di tipo individualizzato assegnata in costanza del rapporto di lavoro.

La risposta all'esercizio del diritto di cancellazione deve avvenire nei tempi certi e nei modi previsti dall'art. 12 del RGPD. Anche qualora il titolare ritenga di non dare corso alla cancellazione perché il persistente trattamento della casella di posta elettronica sarebbe necessario "per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria" (art. 17, par. 3, lett. e), RGPD), in ogni caso è tenuto a rispondere all'interessato indicando i motivi per i quali non ritiene di dare corso all'istanza, e informando altresì circa i rimedi previsti dall'ordinamento avverso tale decisione (in proposito così stabilisce l'art. 12, comma 4, RGPD) (provv. 24 gennaio 2024, n. 40, doc. web n. 9993105; il provvedimento è stato impugnato davanti al giudice competente).

Omessa cancellazione dell'*account* e controlli illegittimi

Il Garante, nel corso degli accertamenti avviati nei confronti di una società, oltre all'omesso riscontro alla richiesta di cancellazione della casella di posta elettronica aziendale di un *ex* dipendente, ha anche verificato che il disciplinare interno relativo all'utilizzo della posta elettronica e della navigazione in internet nel contesto lavorativo prevedeva la sistematica raccolta e conservazione, per sei mesi, dei *log* della posta elettronica, della navigazione in internet e dei dati relativi ai servizi di telefonia, riservando alla società la possibilità di effettuare controlli, benché "occasionali", su base individuale.

Tale regolamentazione dei trattamenti effettuati è stata ritenuta non conforme al principio generale di minimizzazione (art. 5, par. 1, lett. c), RGPD) in relazione alle dichiarate finalità di "prevenire o correggere malfunzionamenti del […] sistema nonché garantire l'efficienza dello stesso", nonché per "motivi di sicurezza" e per "motivi tecnici e/o manutentivi […] o per finalità di controllo e programmazione dei costi aziendali".

Inoltre la sistematica e massiva raccolta e conservazione di dati raccolti, attraverso strumenti tecnologici utilizzati dai lavoratori, aveva comportato la violazione degli artt. 113 e 114 del Codice che richiamano come condizione di liceità dei trattamenti effettuati in ambito lavorativo il rispetto di quanto stabilito dagli artt. 4 e 8, l. n. 300/1970 in materia di controlli a distanza e sulla raccolta di dati non pertinenti rispetto alla valutazione dell'attitudine professionale del lavoratore (v. artt. 5, par. 1, lett. a) e 88 del RGPD) (provv. 12 dicembre 2024, n. 771, doc. web n. 10096474; il provvedimento è stato impugnato davanti al giudice competente).

13

A seguito della presentazione di un reclamo, l'Autorità ha svolto una complessa attività istruttoria volta a verificare la persistente operatività di un *account* di posta elettronica di tipo individualizzato, successivamente all'interruzione del rapporto di lavoro, nonché l'accesso alla corrispondenza in transito sull'*account*. Nella specie il reclamante aveva lamentato un accesso al suo *account* di posta elettronica da parte della società attraverso l'utilizzo di alcune *e-mail* nel corso di un giudizio instaurato dinanzi al giudice del lavoro.

All'esito dell'istruttoria, è stato accertato che la società disponeva di un *software*, attraverso il quale era possibile effettuare il *backup* del contenuto delle caselle di posta elettronica in vigenza del rapporto di lavoro/collaborazione, conservarne il contenuto in modo sistematico e automatico per un periodo di tempo pari a tre anni dopo la cessazione dei rapporti lavorativi.

Sebbene la società avesse dichiarato, nel corso del procedimento, che l'utilizzo del *software* rispondeva all'esigenza di garantire la sicurezza dei sistemi informatici, in realtà l'Autorità ha verificato che tale strumento aveva reso possibile ricostruire anche minuziosamente e a distanza di tempo l'attività lavorativa del dipendente. Tanto che, nel caso specifico, la società aveva analizzato le *e-mail* presenti sull'*account* del reclamante, verificato il contenuto e avviato il contenzioso.

Di conseguenza, l'Autorità, oltre a ribadire che la sistematica conservazione delle *e-mail*, effettuata per un considerevole periodo di tempo (nel caso di specie per tre anni successivamente alla cessazione del rapporto) e dei *log* di accesso alla posta elettronica e al gestionale utilizzato dai lavoratori, non è conforme alla disciplina di protezione dei dati in quanto non proporzionata e non necessaria al conseguimento delle dichiarate finalità di sicurezza della rete informatica e di continuità dell'attività aziendale, ha anche evidenziato che tale trattamento è idoneo a consentire un'attività di controllo sull'attività dei lavoratori in violazione di quanto previsto dall'art. 4, l. n. 300/1970, norma richiamata dall'art. 114 del Codice.

Pertanto, l'Autorità ha disposto una sanzione amministrativa pecuniaria per le violazioni degli artt. 5, par. 1, lett. a), c) ed e), 13 e 88 del RGPD e art. 114 del Codice (provv. 17 luglio 2024, n. 472, doc. web n. 10053224).

A seguito della presentazione di un reclamo da parte di due interessati, il Garante ha rilevato che la società titolare del trattamento non si era limitata a mantenere in essere, successivamente alla cessazione del rapporto di lavoro, gli *account* assegnati ai reclamanti, contestualmente attivando un messaggio di risposta automatico volto ad informare i terzi della imminente disattivazione degli *account* e della possibilità di contattare altri e diversi indirizzi *e-mail*, ma aveva direttamente acceduto (tramite il presidente del consiglio di amministrazione, rappresentante legale della società) al contenuto degli *account* mantenuti attivi successivamente alla cessazione del rapporto di lavoro.

L'Autorità, nel merito, ha precisato che non era sufficiente a fare venire meno l'illiceità del trattamento la circostanza per cui il rappresentante legale si sarebbe limitato a ricercare comunicazioni provenienti da uno specifico gruppo societario e relative a rapporti aziendali. Infatti, la ricerca delle comunicazioni ritenute pertinenti era pur sempre avvenuta successivamente all'accesso alla totalità dei messaggi contenuti nelle caselle di posta.

L'Autorità ha inoltre precisato che anche i dati esteriori delle comunicazioni stesse e i *file* allegati, oltre al contenuto dei messaggi di posta elettronica, riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente (artt. 2 e 15 Cost.).

La condotta tenuta dal titolare del trattamento si era posta pertanto in contrasto con i principi di liceità, di minimizzazione e di limitazione della conservazione di cui all'art. 5, par. 1, lett. a), c) ed e), RGPD.

Nel caso di specie, sono stati ritenuti violati il principio di minimizzazione poiché il titolare non si era limitato a trattate dati adeguati, pertinenti e limitati alle finalità consentite ed anche quello di limitazione della conservazione in ragione delle tempistiche di cancellazione degli *account* in questione.

È inoltre risultata assente un'idonea informativa in merito all'attività che il datore di lavoro avrebbe effettuato, successivamente alla cessazione del rapporto di lavoro, sugli strumenti elettronici assegnati ai reclamanti, secondo la *ratio* dell'art. 13 del RGPD.

Oltre a irrogare una sanzione pecuniaria, con il provvedimento in esame è stato richiesto al titolare di comunicare le iniziative intraprese al fine di predisporre un sistema di disattivazione automatica, dopo la cessazione del rapporto di lavoro, degli *account* di posta elettronica aziendale individualizzati nonché al fine di conformarsi a quanto previsto dall'art. 13 del RGPD nonché di fornire un riscontro adeguatamente documentato ai sensi dell'art. 157 del Codice (provv. 7 marzo 2024, n. 140, doc. web n. 10009004).

Trattamento di dati contenuti in bollettari ed esercizio dei diritti

Nell'anno di riferimento il Garante ha adottato un provvedimento nei confronti di una società per avere trattato alcuni dati di due lavoratori all'interno di propri bollettari, successivamente alla cessazione del rapporto di lavoro, non avendo fornito un idoneo riscontro alle istanze di esercizio dei diritti presentate dai reclamanti.

In particolare, l'Autorità ha accertato che la società aveva continuato a trattare i dati dei reclamanti (iniziale del nome e cognome per esteso) all'interno dei propri bollettari – segnatamente nell'intestazione di questi ultimi, nell'ambito dei recapiti tecnici della società da potere contattare – anche successivamente alla cessazione del rapporto di lavoro dei reclamanti. Ciò era avvenuto in assenza di una idonea base giuridica, quindi in violazione dell'art. 6 del RGPD quale corollario del principio di liceità del trattamento enunciato dall'art. 5 par. 1, lett. a), RGPD.

Inoltre è stato accertato che la società aveva violato gli artt. 12, 17 nonché il principio di correttezza (art. 5 par. 1, lett. a), RGPD) in quanto, a fronte dell'istanza di cancellazione presentata dai reclamanti, pur avendo comunicato agli istanti che non avrebbe più utilizzato i vecchi bollettari, aveva, invece, continuato ad utilizzarli unitamente ai loro dati personali. La società aveva inoltre violato gli artt. 12 e 15 del RGPD in quanto non aveva fornito idoneo riscontro all'istanza di accesso agli attestati di formazione di un corso frequentato dai reclamanti.

In proposito è stato rilevato che, ove la società non fosse stata in possesso del documento richiesto, avrebbe dovuto fornire riscontro all'istanza dei reclamanti limitandosi a comunicare loro i motivi del diniego nonché la possibilità di presentare reclamo al Garante o ricorso all'Autorità giudiziaria ordinaria.

L'Autorità ha inoltre ricordato che il RGPD non impone agli interessati alcun requisito riguardo al formato della richiesta di accesso ai dati personali e, nel richiamare le già menzionate linee guida 01/2022 sul diritto di accesso, ha evidenziato come l'istanza di accesso possa essere presentata da un terzo, essendo rimessa al titolare la verifica dell'identità del terzo che agisce in nome e per conto dell'interessato e della sua autorizzazione (punti 80, 81 delle linee guida cit.); peraltro, non è necessario che l'istanza di esercizio del diritto di accesso contenga il riferimento all'art. 15 del RGPD se comunque è chiaro il contenuto della stessa (punto 50 delle linee guida cit.).

È stato infine rammentato l'orientamento della giurisprudenza di legittimità, ripreso costantemente dal Garante, in base al quale la posizione giuridica soggettiva del lavoratore di accedere al proprio fascicolo personale costituisce un diritto soggettivo tutelabile che trae la sua fonte dal rapporto di lavoro (provv. 24 gennaio 2024, n. 41, doc. web n. 9993531; il provvedimento è stato impugnato davanti al giudice competente).

13.6. *Trattamenti illeciti di dati particolari riferiti ai lavoratori*

Dati relativi alla vita sessuale

Una società aveva inserito, in una contestazione disciplinare contenente informazioni tratte da una relazione investigativa, elementi dai quali si evinceva l'esistenza di una relazione personale e intima tra un dipendente e un'altra persona, peraltro direttamente identificata con nome e cognome.

Anche alla luce delle particolari circostanze del caso concreto, le informazioni trattate sono state ritenute dall'Autorità idonee a rivelare aspetti relativi alla vita sessuale degli interessati. Tale riferimento è stato pertanto ritenuto in contrasto con i principi generali di proporzionalità e minimizzazione, considerato che la contestazione disciplinare conteneva già elementi sufficientemente dettagliati, anche con riguardo ai riferimenti di tempo e di luogo, per consentire al lavoratore di difendersi efficacemente nel procedimento disciplinare.

Inoltre, il trattamento di dati "particolari" era avvenuto in assenza di alcuno dei requisiti per i quali l'ordinamento lo consente in ambito lavorativo (art. 9, par. 2, lett. b), RGPD), anche alla luce del richiamato divieto di trattare informazioni che non siano rilevanti ai fini della valutazione dell'attitudine professionale del dipendente, considerati i rischi di discriminazione ordinariamente connessi a tali trattamenti.

Il Garante ha infine ritenuto che la possibilità di conoscere l'esistenza di una relazione personale riguardante il dipendente, tramite la consultazione del profilo Facebook di quest'ultimo, non potesse essere indicata come liceità del trattamento, posto che la pubblicazione di informazioni sui canali *social* avviene per perseguire finalità (comunicazione interpersonale) diverse da quelle legate all'esecuzione della prestazione lavorativa (provv. 20 maggio 2024, n. 333, doc. web n. 10060901. Il provvedimento è stato impugnato - In pendenza del giudizio di opposizione contro il provvedimento, non è applicata la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione.)

Dati relativi allo stato di salute

Il Garante ha accertato la violazione degli artt. 9, par. 2, lett. b), RGPD; 41, comma 1, lett. b) e comma 2, lett. c), d.lgs. n. 81/2008 nonché del divieto per il datore di lavoro di effettuare accertamenti sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente (art. 5, l. n. 300/1970) per avere una società contattato telefonicamente il medico di medicina generale che aveva redatto certificati medici relativi ad una dipendente.

Oggetto della conversazione telefonica (in base a quanto emerso) sarebbero state le richieste di certificazione di malattia redatte dal medico di base, nonché le "cure e le indicazioni" prescritte dal medico alla reclamante, in relazione allo stato di salute di quest'ultima. Inoltre il datore di lavoro avrebbe rappresentato al medico le difficoltà organizzative e gestionali causate dalle assenze della reclamante. L'Autorità ha, a tale ultimo proposito, stabilito che le legittime esigenze di organizzazione e pianificazione dei turni di servizio non possono pregiudicare la tutela della salute del dipendente garantita dall'ordinamento proprio dall'operato di personale medico dotato di autonomia e competenza professionale (provv. 13 novembre 2024, n. 676, doc. web n. 10088943).

A seguito della presentazione di un reclamo nei confronti di un'associazione medica, l'Autorità ha anche accertato la violazione della disciplina in materia di protezione dei dati personali, riferita in particolare al trattamento dei dati relativi allo stato vaccinale del dipendente nel contesto dell'emergenza epidemiologica da COVID-19.

Il Garante ha sottolineato che, nell'ambito del rapporto di lavoro, la deroga al divieto di trattamento dei cd. dati particolari (prevista nell'ipotesi di cui all'art. 9, par. 2, lett. b), RGPD), non è stata in alcun modo intaccata dalla legislazione speciale legata all'emergenza sanitaria; ha quindi ribadito che il datore di lavoro non può chiedere, ai propri dipendenti, di fornire informazioni sul proprio stato vaccinale o copia di

documenti che comprovino l'avvenuta vaccinazione anti COVID-19. Pertanto, il mancato rispetto della procedura di accertamento dell'inadempimento dell'obbligo vaccinale, disciplinata in maniera molto dettagliata dal d.l. n. 44/2021, ha reso illecito il trattamento effettuato dall'associazione medica (provv. 23 maggio 2024, n. 326, doc. web n. 10043459).

13.7. *Pubblicazione di dati in internet*

A seguito della presentazione di un reclamo, l'Autorità ha accertato la violazione della disciplina di protezione dei dati personali da parte di una fondazione che aveva disposto la pubblicazione sul proprio sito web di due determinazioni recanti provvedimenti disciplinari adottati nei confronti del reclamante e di altri quattro dipendenti.

Nel caso di specie, l'Autorità ha stabilito che la pubblicazione dei provvedimenti disciplinari sul sito web della fondazione costituiva un'operazione non adeguata, non necessaria e non pertinente rispetto alla finalità di gestione del rapporto di lavoro, oltre a non essere prevista da nessuna norma di legge – in violazione, quindi, dei principi e dei requisiti generali che presiedono ogni trattamento di dati personali nel contesto del rapporto di lavoro – tenuto conto anche della particolare delicatezza che connota le informazioni relative alle valutazioni e alle contestazioni disciplinari, trattandosi di dati che incidono (soprattutto se di carattere negativo) sulla dignità professionale del dipendente.

L'Autorità ha, quindi, dichiarato illecito il trattamento perché effettuato in assenza di idonei presupposti di liceità, in violazione dell'art. 6 del RGPD e dell'art. 2-*ter* del Codice, nonché dei principi generali di liceità, correttezza e trasparenza di cui all'art. 5, par. 1, lett. a), RGPD (provv. 13 novembre 2024, n. 679, doc. web n. 10092909).

13.8. *Dati di lavoratori e clienti trattati tramite sistemi di videosorveglianza*

In materia di videosorveglianza, a seguito di un reclamo, l'Autorità ha delegato al Nucleo speciale tutela *privacy* e frodi tecnologiche l'accertamento ispettivo presso una società che svolge attività ricettiva. Si è quindi accertato che la società, in qualità di titolare del trattamento, aveva effettuato un trattamento di dati personali, per mezzo di impianti di videosorveglianza, in violazione della disciplina specifica in materia di protezione dei dati nonché, più in generale, delle disposizioni dell'ordinamento in materia di sorveglianza dei lavoratori.

La società, infatti, aveva ripreso aree sulle quali veniva svolta l'attività lavorativa dei lavoratori e frequentate dai clienti della struttura in assenza di una idonea informativa, quindi in violazione dei principi di trasparenza e di correttezza.

In merito all'indicazione, contenuta nell'informativa, del consenso come base giuridica per il trattamento dei dati dei lavoratori, l'Autorità ha precisato che, di regola, il consenso non può costituire idonea base giuridica nell'ambito del rapporto di lavoro a causa dell'asimmetria che caratterizza il rapporto datore di lavoro-lavoratore.

I trattamenti conseguenti all'impiego degli strumenti tecnologici nei luoghi di lavoro, da cui può derivare un controllo indiretto sull'attività lavorativa, trovano la propria base giuridica nella disciplina di settore di cui all'art. 4 della l. n. 300/1970, disposizione che perimetra, in modo uniforme a livello nazionale, l'ambito del trattamento consentito in ogni contesto lavorativo (pubblico e privato) e costituisce nell'ordinamento interno una disposizione più specifica e di maggiore garanzia (nel senso di cui all'art. 88 del RGPD), la cui osservanza è condizione di liceità del trattamento. In conformità a quanto

13

dichiarato dalla giurisprudenza di legittimità, l'art. 4, l. n. 300/1970 tutela interessi di carattere collettivo e superindividuale, pertanto anche il consenso eventualmente prestato dai singoli lavoratori all'installazione di impianti non è equivalente alla necessaria attivazione della procedura con le rappresentanze dei dipendenti o, in mancanza, sotto il controllo dell'autorità pubblica (v., tra le altre, Cass., sez. III pen., 8 maggio 2017, n. 22148 e 17 dicembre 2019, n. 50919).

Nel corso dell'accertamento, è stato rilevato che la società, attraverso i predetti sistemi di videosorveglianza installati, aveva ripreso l'attività lavorativa dei propri dipendenti senza avere espletato le procedure di garanzia richieste dall'art. 4 della l. n. 300/1970 richiamato dall'art. 114 del Codice. In particolare, gli impianti di videosorveglianza riprendevano, conservando per 48 ore, aree esterne (accessi alla struttura e parcheggi), piscine sia coperte che scoperte e gli spogliatoi, sia quelli per i clienti sia quello riservato ai dipendenti.

In proposito l'Autorità ha ribadito, conformemente alla prevalente giurisprudenza di legittimità, che anche le aree nelle quali transitano o sostano – talora continuativamente – i dipendenti (ad es. accessi alla struttura e ai garage, zone di carico/scarico merci, ingressi carrai e pedonali), qualora sottoposte a videosorveglianza, sono soggette alla piena applicazione della disciplina in materia di protezione dei dati personali.

La condotta della società pertanto non è risultata conforme, fino al rilascio dell'autorizzazione da parte dell'Ispettorato del lavoro, al principio di liceità del trattamento (art. 5, par. 1, lett. a), RGPD in relazione all'art. 114 del Codice) e all'art. 88 del RGPD. Poiché, come rilevato, numerose telecamere di videosorveglianza erano state installate nei locali adibiti a spogliatoio per i clienti e, una di queste, anche nello spogliatoio riservato ai lavoratori, l'Autorità ha ritenuto tale condotta in violazione dei principi di liceità e minimizzazione dei dati (art. 5, par. 1, lett. a) e c), RGPD in quanto lesiva della riservatezza e della dignità delle persone che utilizzavano i predetti spogliatoi; questi ultimi, infatti, sono luoghi, per natura, caratterizzati da una particolare aspettativa di riservatezza e di tutela della intimità e dignità della persona, anche alla luce delle disposizioni vigenti dell'ordinamento civile e penale.

È stato inoltre accertato che la telecamera installata all'interno dello spogliatoio dei dipendenti era posizionata in modo da riprendere direttamente anche il rilevatore utilizzato dai lavoratori per attestare la propria presenza in servizio e per di più, considerata la sua collocazione, la sua presenza non era percepibile agli interessati. Tale condotta è stata considerata in violazione del principio di correttezza (art. 5 par. 1, lett. a), RGPD) e in assenza di una valida condizione di liceità del trattamento (art. 6 del RGPD per i dati cd. comuni).

Considerato altresì che l'installazione di telecamere orientate sui sistemi di rilevazione delle presenze configura una forma di controllo diretto e sistematico dell'attività lavorativa, è stato sottolineato come, anche a seguito delle modifiche apportate alla l. n. 300/1970, dall'art. 23, d.lgs. n. 151/2015, il controllo diretto e mirato sull'attività lavorativa, non è, allo stato, consentito dall'ordinamento e dal quadro costituzionale, oltre a non poter essere inquadrato nel novero delle tassative finalità ("organizzative e produttive", "di sicurezza del lavoro" e "di tutela del patrimonio aziendale") per il perseguimento delle quali tali sistemi possono essere lecitamente impiegati, in base alla richiamata disciplina di settore (considerando 4 e artt. 5 e 88, par. 2, RGPD; artt. 114 del Codice e 4, l. n. 300/1970). L'installazione della predetta telecamera è risultata, inoltre, eccedente rispetto alle finalità perseguite (rilevazione della presenza in servizio e computo degli orari di lavoro), anche sotto il profilo della gradualità delle misure limitative adottabili nei confronti dei lavoratori nonché in violazione del principio di proporzionalità e di minimizzazione dei dati per avere utilizzato contestualmente il *badge* e la telecamera in modo funzionale all'attestazione della presenza in servizio del

lavoratore (artt. 52 della Carta dei diritti fondamentali dell'Unione europea e art. 5, par. 1, lett. c), RGPD).

Inoltre la società non aveva aggiornato (quantomeno fino alla presentazione della copia dello stesso) il registro delle attività di trattamento, con le informazioni relative al trattamento dei dati dei clienti e lavoratori effettuato mediante i sistemi di videosorveglianza installati.

Con il provvedimento in esame il Garante, oltre ad avere adottato una sanzione amministrativa pecuniaria, ha prescritto al titolare, ai sensi dell'art. 58, par. 2, lett. d), RGPD, di conformare allo stesso i propri trattamenti, con riferimento alla corretta predisposizione dei documenti contenenti l'informativa (provv. 12 dicembre 2024, n. 772, doc. web n. 10107146).

13.9. *Trattamento di dati di un lavoratore da parte di un sindacato*

Il Garante si è pronunciato per la prima volta sui poteri delle singole componenti di una rappresentanza sindacale unitaria (RSU) alla luce della disciplina in materia di protezione dei dati personali.

In particolare, a seguito di un reclamo con il quale era stata lamentata la comunicazione a opera di una struttura sindacale, parte di una RSU, al datore di lavoro di un appartenente a tale RSU, di presunte condotte scorrette di quest'ultimo relative all'utilizzo di permessi sindacali, l'Autorità, posto che i diritti, i compiti e le prerogative attribuiti alle RSU sono disciplinati da norme di legge e, in base a queste, dalla contrattazione collettiva a livello nazionale e aziendale, ha accertato che, nel caso di specie, in base al reg. interno della RSU di appartenenza del reclamante, spettava alla RSU, quale soggetto sindacale unitario, valutare la conformità o meno ai principi di correttezza e buona fede dell'operato dei componenti e, se del caso, adottare una censura. Inoltre, è compito della medesima rappresentanza unitaria comunicare la censura adottata sia al lavoratore che al datore di lavoro.

Per questi motivi, la componente sindacale aveva violato il principio generale di liceità dei trattamenti di dati personali (art. 5, par. 1, lett. a), RGPD) e aveva comunicato dati al datore di lavoro del reclamante, in assenza della specifica condizione applicabile al caso di specie, ossia la necessità del trattamento "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" (art. 6, par. 1, lett. c), RGPD) (provv. 12 settembre 2024, n. 551, doc. web n. 10065938).

13.10. *La protezione di dati nell'ambito del rapporto di lavoro pubblico*

Nel corso del 2024, sulla base di reclami, segnalazioni e richieste di parere, l'Autorità si è attivata per affrontare diversi temi correlati alle attività effettuate sui dati personali nel rapporto di lavoro da soggetti pubblici ovvero da soggetti privati che svolgono compiti di interesse pubblico.

Essi interessano, in particolare, i trattamenti di dati legati alle tecnologie impiegate nella gestione del rapporto di lavoro nelle sue varie fasi, inclusa quella del reclutamento mediante procedure concorsuali; quelli volti ad assicurare la salute e la sicurezza sui luoghi di lavoro o comunque effettuati in occasione dell'assolvimento di obblighi derivanti da specifiche normative di settore, come la disciplina in materia di trasparenza dell'azione amministrativa; quelli compiuti da ordini professionali nel quadro dei procedimenti per l'accertamento del possesso del requisito professionale della vaccinazione anti SARS-CoV-2.

13.11. *Trattamenti di dati personali mediante dispositivi tecnologici*

13.11.1. Metadati e posta elettronica nel contesto lavorativo

Con riguardo al documento di indirizzo sui programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati (provv. 21 dicembre 2023, n. 642, doc. web n. 9978728), l'Autorità, tenuto conto di alcune richieste di chiarimenti pervenute in seguito alla sua pubblicazione, specie in ordine ai tempi di conservazione dei metadati generati o raccolti nell'ambito dei sistemi di posta elettronica, ha avviato una consultazione pubblica volta ad acquisire osservazioni e proposte da parte dei datori di lavoro pubblici e privati o di altri soggetti a vario titolo coinvolti da siffatti trattamenti (provv. 22 febbraio 2024, n. 127, doc. web n. 9987885).

All'esito della consultazione, l'Autorità ha adottato una versione aggiornata del documento di indirizzo in questione, anche nella duplice prospettiva di chiarirne l'ambito di applicazione, promuovendo la consapevolezza, in capo ai datori di lavoro titolari del trattamento, delle scelte tecniche e organizzative, nonché di prevenire iniziative e trattamenti di dati in contrasto con la disciplina in materia di protezione dei dati e delle norme che tutelano la libertà e la dignità dei lavoratori.

Pur in linea di continuità con la precedente impostazione del documento, da cui comunque non discendono nuovi adempimenti o responsabilità per i datori di lavoro, la versione aggiornata ha inteso, in particolare, chiarire: la nozione di metadati, distinguendoli, tra l'altro, dalle informazioni contenute nel corpo dei messaggi di posta elettronica o comunque integrate in tali messaggi; l'arco temporale di conservazione dei metadati, al quale si ritiene applicabile il comma 2, art. 4, l. n. 300/1970, evidenziando che l'attività di raccolta e conservazione dei soli metadati/*log* necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, all'esito di valutazioni tecniche e nel rispetto del principio di responsabilizzazione, può essere di norma effettuata – senza attivare le procedure di garanzia di cui al comma 1 dell'art. 4 della l. n. 300/1970 correlato all'art. 114 del Codice – per un periodo limitato a pochi giorni, di regola non superiore a 21, salva la possibilità di estendere il periodo in questione in presenza di particolari condizioni da comprovarsi adeguatamente in applicazione del principio di responsabilizzazione (v. art. 5, par. 2, RGPD), in ragione della realtà tecnica e organizzativa del titolare; il ruolo dei fornitori di servizi di posta elettronica, chiamati a contribuire a far sì che i titolari del trattamento possano adempiere ai loro obblighi di protezione dei dati, contemperando le esigenze di commercializzazione su larga scala dei propri prodotti con la conformità degli stessi ai principi del RGPD (provv. 6 giugno 2024, n. 364, doc. web n. 10026277).

13.11.2. Sistemi di videosorveglianza

A seguito della segnalazione di una lavoratrice, che lamentava l'installazione di una telecamera nell'atrio del comune di cui era dipendente in prossimità dei dispositivi di rilevazione delle presenze, l'Autorità ha accertato che, attraverso l'utilizzo delle immagini registrate, l'ente aveva contestato alla dipendente alcune violazioni dei propri doveri d'ufficio, tra cui il mancato rispetto dell'orario di servizio. La telecamera in questione era stata installata per asseriti motivi di sicurezza, a seguito di alcune aggressioni ai danni di un assessore e di un'assistente sociale. Il comune non aveva, tuttavia, assicurato il rispetto delle procedure di garanzia previste dalla disciplina in materia di controlli a distanza e aveva utilizzato le immagini di videosorveglianza per adottare un provvedimento disciplinare nei confronti della lavoratrice, ponendo in essere un trattamento di dati personali in assenza di base giuridica e comunque in maniera non conforme al RGPD rispetto ai principi di liceità, correttezza e trasparenza, limitazione della finalità, in

contrasto con gli artt. 5, par. 1, lett. a) e b), 6, 12, 13 e 88 del RGPD, nonché con l'art. 114 del Codice in riferimento all'art. 4, commi 1 e 3, l. n. 300/1970. L'Autorità – che, contrariamente a quanto sostenuto dal comune, non ha ritenuto comprovato che il predetto trattamento potesse trovare il proprio fondamento nel quadro giuridico che regola l'impiego di sistemi di videosorveglianza per la tutela della cd. sicurezza urbana (v. art. 5, comma 2, lett. a), d.l. 20 febbraio 2017, n. 14) – ha, altresì, ingiunto al comune di fornire a tutti gli interessati (lavoratori e visitatori presso la sede comunale) un'idonea informativa sul trattamento dei dati personali trattati mediante la telecamera installata (provv. 11 aprile 2024, n. 234, doc. web n. 10013356; v. anche *Newsletter* 21 maggio 2024, doc. web n. 10015453).

13.12. *Trattamento di dati per finalità di instaurazione e gestione del rapporto di lavoro*

Anche con riguardo alle fasi prodromiche all'istaurazione del rapporto di lavoro, nell'ambito di procedure concorsuali o selettive, e, più in generale, nel contesto della gestione del rapporto stesso, il Garante, sulla base di istruttorie avviate a seguito di reclami presentati da dipendenti pubblici o da altri interessati che prestano la propria attività lavorativa presso soggetti pubblici e enti che perseguono finalità di interesse pubblico, ha accertato l'illiceità di taluni trattamenti.

13.12.1. Trattamento di dati nell'ambito di procedure concorsuali

Con un reclamo presentato da un partecipante al concorso pubblico bandito dall'INPS, era stata lamentata la pubblicazione sul sito web dell'Istituto di vari atti e documenti tra cui gli elenchi degli ammessi e non ammessi alle prove (scritta e orale) e la lista dei partecipanti, riportante la valutazione dei titoli e, per ciascun candidato, il punteggio conseguito. Il Garante ha ricordato che i soggetti pubblici, quando operano nello svolgimento di procedure concorsuali, devono trattare i dati personali degli interessati nel rispetto delle norme di settore applicabili. Di conseguenza, non è possibile pubblicare *online* dati dei partecipanti ai concorsi non previsti dalla legge. Peraltro, il trattamento in questione non può trovare fondamento nelle disposizioni del bando di concorso, in quanto l'atto amministrativo generale, pur essendo richiamato dall'art. 2-*ter* del Codice, non può contravvenire ovvero modificare le norme sovraordinate di riferimento, potendo soltanto integrare l'ordinamento nel sistema della gerarchia delle fonti di diritto interno. Non sono infatti consentiti livelli differenziati di tutela della protezione dei dati personali, né su base territoriale né a livello di singola amministrazione, specie quando la materia sia già stata oggetto di bilanciamento e di uniforme trattamento da parte del legislatore a livello nazionale (provv. 11 aprile 2024, n. 235, doc. web n. 10019523; v. anche *Newsletter* 6 giugno 2024, doc. web n. 10022928).

All'esito di ulteriori accertamenti, l'Autorità ha adottato un provvedimento nei confronti del medesimo Istituto per la pubblicazione *online* delle graduatorie finali relative allo stesso concorso. In particolare, queste graduatorie, presenti sul sito istituzionale, contenevano diverse informazioni di dettaglio attinenti a vicende personali e familiari dei partecipanti, esponendo le persone a possibili danni sul piano reputazionale. Tra le informazioni diffuse – alcuni dati anagrafici, insieme a punteggi e titoli di precedenza e di preferenza assegnati – figurava, altresì, la specifica indicazione dell'ammissione con riserva, comprensiva anche delle causali relative alla salute, di oltre 5 mila interessati tra vincitori e idonei. In tale occasione, il Garante ha avuto modo di riaffermare che la pubblicazione delle graduatorie deve avvenire nel rispetto delle

norme di settore applicabili con riguardo ai soli dati dei vincitori necessari ad assicurare la pubblicità e la trasparenza. L'Autorità ha pertanto sanzionato l'Istituto, disponendo la misura correttiva della limitazione del trattamento (provv. 26 settembre 2024, n. 588, doc. web n. 10076453; v. anche *Newsletter* 3 dicembre 2024, doc. web n. 10076607).

In un altro caso, un comune aveva pubblicato sul proprio sito web la graduatoria intermedia redatta all'esito di una prova preselettiva, riportando l'elenco dei candidati ammessi e non ammessi alla successiva prova scritta. Nonostante le richieste di rimozione da parte di un interessato, il documento era rimasto accessibile per un lungo periodo di tempo ed era stato indicizzato dai motori di ricerca. Nel rilevare che il quadro normativo di riferimento prevede che siano pubblicate le sole graduatorie definitive dei vincitori di concorso e non anche gli esiti delle prove intermedie o dei dati personali dei concorrenti non vincitori o non ammessi, il Garante, svolta l'attività istruttoria, ha accertato che la pubblicazione era avvenuta in assenza di un'idonea base giuridica. Nell'ambito della stessa istruttoria è altresì emerso che il predetto comune si avvaleva di una società esterna per la gestione del sito web istituzionale e per l'amministrazione dei profili di accesso al sito medesimo. Accertata l'omessa regolazione, ai sensi dell'art. 28 RGPD, del rapporto intercorrente tra il comune e la predetta società operante come responsabile del trattamento, il Garante, anche tenuto conto della più recente giurisprudenza di legittimità al riguardo (cfr., in particolare, Cass., sez. I civ., sent., 18 dicembre 2023, n. 35256), ha, altresì, rimarcato come il comune avesse messo a disposizione della società i dati personali degli utenti del sito web e degli altri interessati a cui si riferivano i dati ivi pubblicati in assenza di un'idonea base giuridica, dando luogo a una comunicazione illecita di dati personali. Contestualmente, il Garante ha, altresì, accertato che, in carenza di un accordo ai sensi dell'art. 28 RGPD, la società aveva trattato i predetti dati senza specifici e autonomi presupposti di liceità per legittimare il trattamento (provv.ti 20 giugno 2024, n. 372, doc. web n. 10039471 e n. 373, doc. web n. 10039553).

Analogamente, il Garante ha accertato che un altro ente aveva pubblicato sul proprio sito web istituzionale una graduatoria intermedia, recante gli esiti dei colloqui tecnici professionali di ciascun candidato, attraverso l'indicazione delle formule "idoneo" (con annessa specificazione del punteggio), "non idoneo" o "assente". Tenuto conto che, alla luce della disciplina di settore applicabile, sopra richiamata, che prevede unicamente la pubblicazione delle graduatorie finali e non anche degli atti intermedi, l'Autorità, rilevando l'assenza di un'idonea base giuridica del trattamento in questione, ha adottato un provvedimento sanzionatorio nei confronti dell'ente (provv. 17 ottobre 2024, n. 613, doc. web n. 10075259).

A seguito di un reclamo, il Garante ha accertato la pubblicazione da parte di un comune di un verbale di concorso contenente i dati personali del reclamante (compreso il voto di laurea) in maniera non conforme alla disciplina *ratione materiae* applicabile, che prevede la pubblicazione delle sole graduatorie finali dei vincitori di concorso e non anche degli atti interni alla procedura, quali i verbali redatti dalle commissioni comprendenti i dati personali dei candidati. Inoltre, il comune aveva fornito tardivamente riscontro a una richiesta dell'interessato di esercizio del diritto di cancellazione dei propri dati personali dal sito web istituzionale dell'ente e di deindicizzazione dai motori di ricerca di tale documento. Per questi motivi, il Garante ha adottato un provvedimento sanzionatorio nei confronti del comune (provv. 4 luglio 2024, n. 404, doc. web n. 10050145).

In un altro pronunciamento, il Garante si è occupato del caso di un comune che, ancorché per mero errore, aveva pubblicato sul proprio sito web istituzionale un

allegato a un provvedimento riportante i dati personali del reclamante e di altri partecipanti a una procedura concorsuale. Al riguardo, il Garante ha evidenziato che anche la presenza di uno specifico regime di pubblicità non può comportare alcun automatismo rispetto alla diffusione *online* di dati personali, né una deroga ai principi in materia di protezione dei dati. Per tali ragioni, l'ente è stato destinatario di un provvedimento sanzionatorio (provv. 14 novembre 2024, n. 696, doc. web n. 10080746).

A seguito di un reclamo, il Garante ha sanzionato un comune per aver pubblicato sul sito istituzionale una graduatoria recante l'indicazione delle generalità e del punteggio attribuito ai singoli dipendenti relativamente alle procedure interne finalizzate alle progressioni economiche del personale. In coerenza con gli orientamenti dell'ANAC, le procedure selettive interne che determinano un passaggio di livello nell'ambito della stessa area o categoria (cd. progressioni orizzontali) sono, infatti, escluse dall'ambito oggettivo di applicazione dell'art. 19 del d.lgs. n. 33/2013, relativo alle graduatorie finali per l'assunzione di nuovo personale. Infatti, le procedure di carattere meritocratico connesse alla valutazione dell'apporto individuale del lavoratore, come nel caso di specie, non sono soggette al principio del pubblico concorso, differentemente dalle progressioni finalizzate al passaggio di qualifica, consistenti nell'inquadramento in un'area superiore (cd. progressioni verticali), che avvengono attraverso procedure comparative, determinandosi in tal caso una novazione oggettiva del rapporto di lavoro assimilabile all'assunzione. L'Autorità ha, pertanto, ritenuto che la pubblicazione delle graduatorie e degli allegati, contenenti i dati personali del reclamante e di circa un centinaio di partecipanti, avesse dato luogo a una diffusione dei dati personali in assenza di un'idonea base giuridica (provv. 27 novembre 2024, n. 729, doc. web n. 10097341).

13.12.2. FAQ in materia di oblio oncologico e assenze per motivi di salute

A seguito dell'emanazione della l. 7 dicembre 2023, n. 193 (disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone che sono state affette da malattie oncologiche), l'Autorità ha pubblicato specifiche FAQ in materia di oblio oncologico con l'obiettivo di prevenire le discriminazioni e tutelare i diritti delle persone che sono guarite da malattie oncologiche. In particolare, alcune FAQ sono finalizzate a fornire chiarimenti e indicazioni a datori di lavoro pubblici e privati.

Nel richiamare l'espresso divieto per i datori di lavoro di richiedere ai dipendenti informazioni sulla patologia oncologica, nei termini previsti dalla nuova normativa, il Garante ha ribadito che le preesistenti norme nazionali più specifiche e di maggior tutela (art. 88 e cons. 155 del RGPD e art. 113 del Codice, che richiama l'art. 8, l. n. 300/1970 e l'art. 10, d.lgs. n. 276/2003) già prevedono che il datore di lavoro non possa, di regola, conoscere le specifiche patologie sofferte dall'interessato sia in precedenza che in costanza di rapporto di lavoro. Peraltro, in coerenza con le disposizioni vigenti in materia di salute e sicurezza sui luoghi di lavoro, il medico competente è per legge l'unico legittimato a trattare in piena autonomia i dati personali di natura sanitaria indispensabili per tutelare la salute e la sicurezza dei luoghi di lavoro (FAQ n. 12). È stato, inoltre, ribadito che, seppure nell'ordinaria gestione del rapporto con il dipendente e ai fini della giustificazione dell'assenza dal servizio del lavoratore per l'effettuazione di una qualunque prestazione specialistica (anche relativa a eventuali patologie oncologiche), il datore di lavoro sia legittimato ad acquisire la documentazione ad essa riferita, la stessa non deve recare informazioni diagnostiche o la specifica prestazione sanitaria effettuata o altri dettagli da cui sia possibile risalire alla patologia sofferta. Il datore di lavoro deve comunque astenersi dall'utilizzare per altre finalità eventuali informazioni di dettaglio contenute nella documentazione prodotta dal

dipendente (v. art. 2-*decies* del Codice; FAQ n. 13) (*Vademecum* 9 agosto 2024, doc. web n. 10044898).

13.12.3. Ordini delle professioni sanitarie. Comunicazione a terzi di dati trattati nell'ambito dei procedimenti per l'accertamento del requisito vaccinale

Alcuni reclami hanno riguardato il trattamento illecito di dati personali da parte di ordini professionali del settore sanitario nell'ambito dei procedimenti per l'accertamento del possesso del requisito vaccinale anti SARS-CoV-2, ai sensi dell'art. 4, d.l. 1° aprile 2021, n. 44, convertito in l. 28 maggio 2021, n. 76. In particolare, si trattava di comunicazioni di dati personali a soggetti terzi (enti pubblici o singoli professionisti) non previste da tale disciplina di settore, in maniera non conforme ai principi sia di liceità che di correttezza e trasparenza, nonché in assenza di una base giuridica.

In un caso, un ordine provinciale dei medici chirurghi e degli odontoiatri, aveva inviato ad alcuni soggetti pubblici (assessore regionale, questore, sindaco, direttore generale e direttore sanitario di un'azienda sanitaria) una nota in cui si dava atto della sospensione della reclamante per mancanza del requisito vaccinale, dando luogo a una comunicazione illecita (provv. 22 febbraio 2024, n. 110, doc. web n. 10006933).

Un ordine provinciale dei tecnici sanitari di radiologia medica e delle professioni sanitarie tecniche, della riabilitazione e della prevenzione aveva, invece, inviato un'*e-mail* al reclamante e ad altri quaranta professionisti, al fine di chiedere loro di fornire gli estremi del proprio datore di lavoro per comunicare la sospensione dall'albo in ragione del mancato possesso del requisito vaccinale anti SARS-CoV-2. Ciò è avvenuto inserendo in chiaro gli indirizzi di posta elettronica personali di tutti i destinatari, consentendo così la reciproca conoscenza degli stessi e, implicitamente, dell'informazione circa il mancato possesso del requisito vaccinale anti SARS-CoV-2. L'ordine è stato, pertanto, destinatario di un provvedimento sanzionatorio per aver posto in essere una comunicazione di dati personali in assenza di base giuridica (provv. 9 maggio 2024, n. 288, doc. web n. 10026235).

L'Autorità si è poi occupata del caso di un ordine di medici veterinari, che, dopo aver ricevuto da un ordine di un'altra provincia alcune deliberazioni concernenti la sospensione di professionisti per mancanza del requisito vaccinale, ha inoltrato via *e-mail* a tutti i propri iscritti copia integrale di dette deliberazioni, in assenza di un idoneo presupposto di liceità (provv. 22 febbraio 2024, n. 102, doc. web n. 10006478).

13.12.4. Comunicazione di dati personali a terzi nei contesti lavorativi

Sulla base di una segnalazione di un ispettorato territoriale del lavoro, il Garante ha avviato un'istruttoria nei confronti di un patronato che aveva consentito a un *ex* dipendente di continuare ad accedere a dati personali dell'utenza, inclusi quelli relativi a categorie particolari, trattati dal patronato nello svolgimento dei propri compiti e attività anche di interesse pubblico. Sul presupposto che tale soggetto, che continuava a prestare la propria attività lavorativa presso il patronato in maniera irregolare, non avesse più titolo per trattare i dati personali in qualità di autorizzato al trattamento (v. art. 29 del RGPD), l'Autorità ha sanzionato il patronato per aver messo a disposizione di tale soggetto "terzo" (art. 4, n. 10, RGPD) i dati personali dell'utenza, in maniera non conforme ai principi sia di liceità che di correttezza e trasparenza, nonché in assenza di base giuridica (provv. 24 aprile 2024, n. 243, doc. web n. 10019389).

A seguito di un reclamo e di una segnalazione, nonché sulla base di notizie di stampa, l'Autorità ha appreso che una lettera dell'allora Ministro per la pubblica amministrazione, relativa alle opportunità di formazione messe a disposizione nel quadro del cd. piano strategico per la valorizzazione e lo sviluppo del capitale umano della p.a., era stata

inviata a mezzo *e-mail* dal Dipartimento della funzione pubblica, per il tramite INPS, a indirizzi di posta elettronica personali di dipendenti pubblici. Al fine di individuare tali indirizzi, l'Istituto aveva identificato lo *status* di dipendente pubblico dalle denunce retributive UNIEMENS-ListaPosPA, ottenendo così anche i codici fiscali degli interessati; tramite tali dati, era risalito al nome, al cognome e all'indirizzo di posta elettronica eventualmente forniti dagli stessi in qualità di utenti registrati alla sezione *my*INPS del sito web dell'Istituto per fruire dei servizi ivi offerti all'utenza, non necessariamente in quanto lavoratori ma in qualità di cittadini e utenti che a vario titolo si avvalgono dei servizi in questione. Il Garante ha ritenuto che l'utilizzo di tali dati di contatto privati ai fini dell'invio della predetta lettera si ponesse in contrasto con l'aspettativa degli utenti del portale circa il trattamento dei propri dati, i quali, anche in considerazione dell'informativa fornita loro dall'Istituto al momento della raccolta dei dati, confidavano che gli stessi sarebbero stati utilizzati esclusivamente ai fini dell'erogazione degli specifici servizi richiesti attraverso il portale.

Il trattamento in questione, posto in essere, peraltro, in assenza di una sufficiente trasparenza nei confronti degli interessati, non poteva nemmeno considerarsi necessario, atteso che la medesima finalità avrebbe potuto essere perseguita attraverso modalità meno invasive, ossia senza fare ricorso a trattamenti di dati personali, ad esempio diramando la predetta lettera alle amministrazioni pubbliche e invitando le stesse, in qualità di datrici di lavoro, ad informare i dipendenti con propri canali (posta elettronica istituzionale; intranet; bacheche; ecc.). Tenuto conto di tutte le circostanze del caso e specialmente del fatto che la lettera in questione aveva natura istituzionale ed era stata inviata comunque per finalità rivolte all'interesse collettivo, l'Autorità ha ritenuto sufficiente ammonire entrambi i contitolari del trattamento (provv.ti 24 gennaio 2024, n. 31, doc. web n. 9992914 e n. 32, doc. web n. 9992986).

All'esito di un'istruttoria relativa a un reclamo presentato da un lavoratore in servizio presso un ufficio della motorizzazione civile, il Garante ha accertato che il predetto ufficio aveva inviato una nota alla prefettura e alla questura territorialmente competenti, rendendo loro noti dati personali del reclamante (ossia la circostanza che lo stesso avesse rappresentato di essere in possesso di un porto d'armi e la sussistenza di un contenzioso con il datore di lavoro), nonché menzionando per esteso la diagnosi riportata in certificati medici prodotti dal reclamante nell'ambito del predetto contenzioso. Nell'evidenziare che, ai fini della tutela della sicurezza pubblica, la disciplina di settore demanda ai professionisti sanitari – e non, invece, al datore di lavoro – l'obbligo di effettuare le necessarie segnalazioni alle autorità competenti in merito a malattie di mente o gravi infermità psichiche incompatibili con il possesso del porto d'armi, il Garante ha ravvisato l'assenza di base giuridica della comunicazione dei dati personali del reclamante nei confronti dei predetti soggetti. È stato, inoltre, ritenuto che l'ufficio della motorizzazione avesse trattato, in assenza di base giuridica, le informazioni restituitegli dalla questura, anche in questo caso senza i necessari presupposti di liceità, relative al pregresso possesso del porto d'armi da parte del reclamante. Per tali ragioni, il Garante ha dichiarato l'illiceità dei predetti trattamenti (provv.ti 6 giugno 2024, n. 335, doc. web n. 10037819 e n. 336, doc. web n. 10037849).

In un caso oggetto di reclamo, una dipendente di un'azienda ospedaliera aveva inviato un'*e-mail* al direttore dell'unità organizzativa presso la quale prestava servizio per comunicare la propria indisponibilità a coprire un turno lavorativo per motivi di salute, specificando la sintomatologia sofferta, ancorché senza specificare la connessa patologia. Il direttore, nel rispondere a tale *e-mail*, aveva messo in copia per conoscenza il direttore generale dell'azienda, così ponendo in essere una comunicazione di dati personali, anche relativi alla salute, che non era necessaria al fine di consentire all'amministrazione

di assumere le necessarie iniziative per riprogrammare i turni di lavoro. Il Garante, valutate tutte le evidenze del caso, ha adottato un provvedimento di ammonimento nei confronti dell'azienda (provv. 9 maggio 2024, n. 270, doc. web n. 10025870).

Un comune aveva, invece, trasmesso tramite *e-mail* una comunicazione contenente riferimenti espliciti a patologie di un dipendente e alla sua condizione di beneficiario delle tutele previste dalla l. n. 104/1992, non solo all'interessato ma anche a colleghi dello stesso. Considerando che il datore di lavoro è tenuto a prevenire l'indebita circolazione di dati personali relativi al singolo dipendente anche all'interno della propria organizzazione, limitando la possibilità di trattare tali dati esclusivamente al personale autorizzato in ragione del ruolo ricoperto e delle mansioni assegnate per la gestione del rapporto di lavoro, il Garante ha rilevato che la condotta posta in essere aveva dato luogo a una comunicazione illecita di dati personali relativi alla salute, in violazione dei principi di liceità, correttezza e trasparenza, nonché minimizzazione dei dati (provv. 26 settembre 2024, n. 606, doc. web n. 10068155).

Ancora, a seguito di un reclamo, il Garante ha censurato la condotta di una società operante nel settore della sanità, atteso che, in occasione dell'invio di una *e-mail* a due dipendenti finalizzata a pianificare le presenze nel periodo estivo, aveva fatto esplicito riferimento alla fruizione da parte di una delle stesse delle agevolazioni previste dalla l. n. 104/1992. Tenuto conto che anche il mero riferimento a normative che disciplinano benefici per l'assistenza e l'integrazione delle persone con disabilità può rivelare informazioni sullo stato di salute di un interessato e che, in ogni caso, l'esigenza di assicurare la continuità e l'efficienza organizzativa di uffici e amministrazioni non può giustificare la comunicazione ai colleghi delle specifiche causali di assenza di taluni di essi, il Garante ha dichiarato illecita la comunicazione dei dati in questione (provv. 19 dicembre 2024, n. 796, doc. web n. 10102504).

In altro contesto, un dipendente, appartenente a una forza armata, ha rappresentato di essere stato sottoposto a visita di idoneità psico-fisica presso la commissione medica competente a seguito della quale veniva giudicato non idoneo al servizio militare. Successivamente il verbale della commissione medica, comprensivo, oltre che del giudizio di inidoneità, anche della diagnosi e di tutte le visite mediche effettuate, nonché della terapia in corso, veniva acquisito e poi trasmesso a diversi uffici del corpo di appartenenza. Al riguardo, il Garante ha ricordato che le predette commissioni mediche e i professionisti sanitari competenti sono i soli soggetti legittimati per legge a svolgere le attività di trattamento necessarie alla verifica delle condizioni psico-fisiche del lavoratore ai fini delle valutazioni in merito all'idoneità all'attività lavorativa, nel rispetto degli specifici limiti e presupposti stabiliti dalla disciplina di settore applicabile che costituisce la base giuridica dei relativi trattamenti.

Di conseguenza, tenuto conto delle circostanze del caso concreto, il Garante ha ritenuto di ammonire il titolare del trattamento (provv. 23 maggio 2024, n. 303, doc. web n. 10132199).

In un altro caso, il Garante, tenuto conto delle risultanze emerse dall'istruttoria, ha ritenuto di ammonire un ministero per aver comunicato per errore dati personali di un lavoratore, anche relativi allo stato di salute, a un avvocato che non rappresentava più lo stesso, disponendo, invece, l'archiviazione del procedimento in relazione a un motivo di reclamo attinente alla circolazione dei dati personali del reclamante tra articolazioni dello stesso ministero (provv. 19 dicembre 2024, n. 797, doc. web n. 10102287).

13.12.5. Trattamento di dati personali relativi all'orientamento sessuale del dipendente

Un profilo estremamente rilevante è stato affrontato dal Garante in occasione di un'istruttoria avviata, a seguito di reclamo, nei confronti di un ministero che, avendo

acquisito, sulla base di una segnalazione, informazioni in merito alla vita privata e all'orientamento sessuale di un proprio dipendente, aveva utilizzato le stesse a fini disciplinari. Al riguardo, l'Autorità ha ricordato che i comportamenti assunti dai lavoratori al di fuori dello svolgimento dei propri compiti e mansioni e non interferenti, neanche in via indiretta, con l'esecuzione della prestazione lavorativa, afferiscono alla vita privata degli stessi.

In particolare, il Garante ha sottolineato che le informazioni relative alla vita sessuale e all'orientamento sessuale sono da considerarsi delicate in tutti i contesti di trattamento e, pertanto, beneficiano di una tutela rafforzata, attenendo alla dimensione intima della persona ed essendo, per tali motivazioni, del tutto inconferenti rispetto all'esecuzione della prestazione lavorativa.

Pertanto, per effetto della disciplina lavoristica e di protezione dei dati (v. artt. 8 della l. n. 300/1970 e 113 del Codice, che costituiscono norme più specifiche e di maggior tutela previste dall'ordinamento nazionale ai sensi dell'art. 88 del RGPD), è fatto divieto al datore di lavoro di effettuare trattamenti aventi ad oggetto tali dati del lavoratore, anche per il fine di prevenire discriminazioni nel delicato contesto lavorativo e professionale. Preso atto che il ministero aveva già disposto l'archiviazione del procedimento disciplinare in questione, il Garante ha comunque dichiarato l'illiceità del trattamento posto in essere (provv. 24 aprile 2024, n. 268, doc. web n. 10021491).

13.13. *Diffusione* online *di dati personali dei lavoratori*

Rimane elevato il numero di reclami nei confronti di amministrazioni in merito alle pubblicazioni di atti e documenti contenenti dati personali di lavoratori sui siti web istituzionali, più esattamente nelle sezioni Amministrazione trasparente o Albo pretorio, peraltro in molti casi indicizzate sui motori di ricerca (cfr. par. 4.4.2).

Con riferimento ad un reclamo, il Garante ha accertato che una Camera di commercio industria artigianato e agricoltura aveva pubblicato sul proprio sito web istituzionale, ancorché a causa di un mero errore umano, copia di una deliberazione della propria giunta, con la quale si prendeva atto dell'esito di un giudizio in sede civile, promosso dal reclamante nei confronti del medesimo ente camerale in relazione a vicende connesse al rapporto di lavoro. Ciò aveva comportato la diffusione *online* delle predette informazioni relative al reclamante, il quale era identificato mediante riferimento al nome e al cognome, riportati in chiaro. Inoltre, atteso che le sentenze sono soggette a pubblicità anche nei termini di cui all' art. 51 del Codice, l'indicazione in chiaro degli estremi della sentenza avrebbe potuto consentire a terzi di venire a conoscenza anche dell'integrale contenuto della stessa, ricollegando le vicende oggetto di contenzioso all'identità del reclamante. Successivamente, la Camera di commercio aveva pubblicato la medesima deliberazione oscurando le generalità del reclamante, il quale era, tuttavia, ancora identificabile, in ragione dei riferimenti in chiaro all'Autorità giudiziaria che aveva emesso la sentenza, al numero di registro generale del procedimento, nonché al numero e alla data di pubblicazione della stessa. Il Garante ha, pertanto, adottato un provvedimento sanzionatorio nei confronti della Camera di commercio per aver diffuso i dati personali del reclamante in maniera non conforme al principio di liceità, correttezza e trasparenza, nonché in assenza di una base giuridica (provv. 22 febbraio 2024, n. 99, doc. web n. 10000804).

Analogamente, un comune aveva pubblicato sul proprio sito web istituzionale deliberazioni contenenti informazioni riguardanti, in particolare, vicende derivanti dalla cessazione del rapporto di lavoro in essere con il reclamante, tra cui l'atto di

accoglimento delle dimissioni volontarie, il piano di congedo ordinario e l'atto di conferimento di incarico a un avvocato, con l'indicazione di nome e cognome del reclamante che aveva citato in giudizio il comune. L'ente aveva poi pubblicato ulteriore documentazione riguardante il reclamante riportando le sole iniziali del nome e cognome dello stesso, anche facendo riferimento agli estremi di documentazione già pubblicata in precedenza, in cui erano menzionate le generalità complete dell'interessato. È stato, altresì, rilevato che in uno dei documenti pubblicati vi erano riferimenti indiretti all'adesione del reclamante a un'organizzazione sindacale. L'Autorità ha, pertanto, adottato un provvedimento sanzionatorio nei confronti dell'ente (provv. 17 ottobre 2024, n. 612, doc. web 10073751).

Un'azienda sanitaria aveva, invece, pubblicato sul proprio sito web istituzionale alcune delibere, i relativi allegati e ulteriore documentazione contenente dati personali di dipendenti, riferiti ai compensi liquidati per prestazioni aggiuntive, alla fruizione di congedi sindacali, alla mancata partecipazione a turni di servizio in ragione di specifiche limitazioni funzionali connesse a motivi di salute, nonché alla specifica indicazione nel cd. piano di lavoro dei giorni di congedo per malattia, contrassegnati con la lettera "M". Sul punto, il Garante ha ricordato che anche le informazioni relative all'assenza per malattia rientrano nella nozione di dato relativo alla salute, indipendentemente dalla circostanza che sia contestualmente indicata esplicitamente la diagnosi. Nell'affermare, inoltre, che, come previsto dalla disciplina in materia di trasparenza, i dati relativi alle somme liquidate a titolo di prestazioni aggiuntive effettuate da singoli dipendenti devono essere pubblicati al fine di dare pubblica evidenza dei livelli di premialità nella distribuzione dei premi e degli incentivi al personale, solo in termini di valori in forma aggregata degli importi liquidati e non, invece, fornendo il dettaglio analitico dei compensi accessori percepiti individualmente dai dipendenti, l'Autorità ha adottato un provvedimento sanzionatorio nei confronti del titolare del trattamento per aver diffuso dati personali, anche particolarmente delicati, in quanto relativi allo stato di salute e all'appartenenza sindacale, in assenza di base giuridica (provv. 27 novembre 2024, n. 730, doc. web n. 10100956).

Più in generale, molti casi affrontati nel corso del 2024 hanno riguardato la diffusione *online* di atti e documenti contenenti dati personali dei lavoratori. Il Garante, nel dichiarare l'illiceità del trattamento, in ragione dell'assenza di un'idonea base giuridica, ha adottato numerosi provvedimenti, di seguito sintetizzati, concernenti la pubblicazione, sul rispettivo sito web istituzionale, da parte di:

- un comune, di una delibera contenente dati personali del reclamante relativi alle dimissioni dello stesso, alla rispettiva qualifica, alla data dell'ultimo giorno lavorativo, alle ore lavorate e all'ufficio di appartenenza (provv. 12 dicembre 2024, n. 768, doc. web n. 10102355);
- un'azienda sanitaria, di una delibera riguardante l'approvazione dell'albo "aziendale" di avvocati esterni che recava in allegato, oltre all'elenco dei professionisti inseriti nell'albo, anche quello dei professionisti esclusi, con l'indicazione accanto ad ogni nominativo delle ragioni dell'esclusione, quali il non essere stato iscritto all'albo degli avvocati per l'arco temporale richiesto per la partecipazione alla selezione, il non aver presentato il *curriculum vitae* e il non aver presentato la domanda entro i termini previsti (provv. 13 novembre 2024, n. 666, doc. web n. 10084453);
- un ateneo, del nominativo di una dipendente, specificando il ruolo dalla stessa ricoperto all'interno dell'amministrazione (provv. 23 maggio 2024, n. 302, doc. web 10033086);
- un istituto scolastico, di decine di determinazioni dirigenziali riguardanti aspetti organizzativi legati alla continuità dell'attività didattica e alla gestione del rapporto di

lavoro con l'interessata, con particolare riguardo ai giorni di assenza dal servizio della reclamante e di altro personale scolastico (provv. 24 gennaio 2024, n. 35, doc. web n. 9987578).

13.13.1. Dati personali di lavoratori in banche dati pubbliche

Oltre a rendere i prescritti pareri (peraltro favorevoli) su tre schemi di decreto del Ministero del lavoro e delle politiche sociali che disciplinano aspetti attinenti al trattamento di dati relativi alla salute per finalità di previdenza e assistenza in diversi settori (schema di decreto del Ministero del lavoro e delle politiche sociali attuativo degli artt. 25 e 26 del d.l. 7 maggio 2024, n. 60, che regola tra l'altro l'utilizzo di strumenti di IA per l'abbinamento ottimale delle offerte e delle domande di lavoro inserite sul Sistema informativo per l'inclusione sociale e lavorativa (SIISL); schema di decreto del Ministero del lavoro e delle politiche sociali che approva le linee guida denominate assegno di inclusione - linee guida per la definizione dei Patti per l'inclusione sociale; schema di decreto del Ministero del lavoro e delle politiche sociali di cui all'art. 10 del d.lgs. 124/2004, relativo al Portale nazionale del sommerso (PNS) - cfr. par. 4.2), il Garante ha espresso parere favorevole in merito a due schemi di decreto del Ministero della salute, attuativi l'uno del d.lgs. 5 agosto 2022, n. 137, e l'altro del d.lgs. 5 agosto 2022, n. 137, e relativi alla segnalazione di incidenti gravi e incidenti diversi da quelli gravi che coinvolgono rispettivamente i dispositivi medici e quelli medico-diagnostici in vitro, da parte degli operatori sanitari, pubblici o privati, effettuata direttamente o tramite la struttura sanitaria coinvolta o, a seconda dei casi, dagli utilizzatori e dai pazienti. Al riguardo, nell'ambito delle interlocuzioni informali intercorse durante l'istruttoria, tra i numerosi profili evidenziati anche rispetto al trattamento dei dati di pazienti e operatori sanitari, il Garante ha rimarcato, in particolare, che il trattamento dei dati degli operatori sanitari contenuti nel modulo *online* previsto per le predette segnalazioni dovrà basarsi su una chiara definizione dei ruoli dei soggetti a vario titolo coinvolti sul piano del trattamento dei dati personali; che, tramite il predetto modulo, dovranno essere raccolti i soli dati personali adeguati, pertinenti e limitati in rapporto alla finalità perseguita; che i dati acquisiti nell'ambito delle procedure di autenticazione informatica mediante gli strumenti di autenticazione previsti dallo schema di decreto ai fini della compilazione del modulo dovranno comprendere esclusivamente il codice fiscale, il cognome e il nome del soggetto che effettua la segnalazione, nel rispetto del principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c), RGPD (provv.ti 14 novembre 2024, n. 693, doc. web n. 10079161 e n. 694, doc. web n. 10107752).

14 Le attività economiche

14.1. *Trattamento di dati personali in ambito assicurativo*

Nel 2024 sono pervenute all'Autorità numerose segnalazioni e reclami riguardanti il settore assicurativo, per lo più in tema di esercizio dei diritti nei confronti delle compagnie assicurative, nonché su argomenti già esaminati dal Garante negli anni passati (tra cui, in particolare, quello della conoscibilità, da parte di chiamati all'eredità e di eredi, dei dati identificativi dei beneficiari di polizze stipulate in vita da persone decedute - v. Relazione 2023, p. 162).

Proprio in materia di esercizio dei diritti, si segnala l'adozione di un provvedimento di ammonimento nei confronti di una compagnia di assicurazioni che non aveva fornito un riscontro idoneo, nel termine previsto dall'art. 12, par. 3, RGPD, a un'istanza di accesso ai dati personali formulata ai sensi dell'art. 15 del RGPD (provv. 14 novembre 2024, n. 705, doc. web n. 10105702); in particolare la compagnia, anziché fornire all'interessata i dati personali contenuti nella documentazione riferita al sinistro che aveva coinvolto il veicolo di sua proprietà, le aveva comunicato di avere provveduto – come da sua richiesta – alla loro cancellazione. Successivamente, nel corso dell'istruttoria, la società ha invece aderito all'istanza della reclamante, precisando che quanto accaduto – che comunque doveva considerarsi un fatto accidentale e isolato – era imputabile all'errore di un operatore del *back office* e di avere avviato successivamente adeguati interventi formativi.

Rete dei RPD nel settore assicurativo

L'Autorità ha altresì avviato i lavori della rete dei RPD nel settore assicurativo.

A seguito, infatti, della fruttuosa iniziativa concernente l'attività degli RPD in ambito bancario, il Garante ha intrapreso, in collaborazione con ANIA e IVASS, un'analoga iniziativa allo scopo di realizzare un'interazione continua rispetto ai complessi temi che caratterizzano il trattamento dei dati nel settore assicurativo. Il 5 novembre 2024 si è tenuto l'incontro inaugurale dei lavori della rete, a seguito del quale è stato predisposto un questionario da sottoporre ai RPD aderenti, allo scopo di avere una fotografia rappresentativa del ruolo del RPD nelle imprese operanti in ambito assicurativo in Italia, avviare una riflessione sulle eventuali difficoltà operative riscontrate nello svolgimento dei compiti assegnati e individuare le iniziative da assumere per consentire di superarle.

14.2. *Trattamento di dati personali in ambito bancario-finanziario e sistemi di informazioni creditizie*

Agenzie di cancellazione

Con provv. 19 dicembre 2024, n. 802 (doc. web n. 10106904), l'Autorità ha applicato una sanzione pecuniaria e disposto l'adozione di misure correttive nei confronti di una società che offre servizi consulenziali nel settore del credito; si tratta, in particolare, di una cd. agenzia di cancellazione che opera nei confronti di coloro che hanno fatto ricorso a forme di finanziamento rateali senza riuscire ad onorare le scadenze periodiche (cumulando quindi ritardi nel pagamento delle relative rate), proponendo agli stessi di agire – in nome e per conto loro – nei confronti dei gestori

dei sistemi di informazioni creditizie (CRIF S.p.a., EXPERIAN S.p.a., CTC) o della Banca d'Italia per ottenere la cancellazione o la rettifica delle posizioni negative registrate a loro carico. All'esito di un'articolata attività istruttoria e di un accertamento ispettivo, sono state rilevate diverse violazioni della normativa in materia di protezione dei dati personali.

In primo luogo il trattamento dei dati dei clienti da parte della società è risultato illecito in quanto effettuato in violazione dei principi generali di lealtà, correttezza e trasparenza e di limitazione della conservazione di cui all'art. 5, lett. a) ed e), RGPD. È stato infatti accertato che la società, che pure si avvale di un *database* di oltre 70.000 clienti, non aveva fornito agli stessi l'informativa prevista dall'art. 14, parr. 1 e 2, RGPD, ne aveva individuato precise tempistiche di conservazione dei dati personali trattati, sia con riferimento a coloro che, sottoscrivendo un contratto di mandato, si erano avvalsi dei servizi della società, sia con riferimento a quanti avevano invece semplicemente richiesto informazioni, senza poi instaurare alcun rapporto contrattuale con la stessa.

È stato inoltre rilevato che la società, nell'espletamento della sua attività, si era avvalsa della collaborazione di altri soggetti (persone fisiche e giuridiche) in violazione dell'art. 28, parr. 1 e 3, RGPD che individua i presupposti di liceità dei trattamenti posti in essere da un responsabile del trattamento per conto del titolare.

Nel provvedimento in questione, l'Autorità ha poi rivolto una particolare attenzione alla figura del RPD posto che, nel caso di specie, la società aveva provveduto a designare quale RPD il rappresentante legale della società medesima, in violazione degli artt. 37 e 38 del RGPD.

Al riguardo, il Garante, dopo aver rilevato che di tale designazione non era stata data comunicazione all'Autorità (in violazione dell'art. 37, par. 7, RGPD), ha evidenziato che, anche alla luce delle linee guida sui RPD adottate dal Gruppo di lavoro Art. 29 il 13 ottobre 2016 (emendate il 5 aprile 2017), i requisiti di cui agli artt. da 37 a 39 e al cons. 97 rendono il ruolo di RPD del tutto incompatibile con quello di rappresentante legale della società presso la quale è designato; ciò in quanto il medesimo soggetto che determina i mezzi e le finalità dei trattamenti non può avere la necessaria indipendenza per esercitare anche i compiti di sorveglianza – sull'osservanza della disciplina e sulle politiche del titolare in materia di protezione dei dati personali – previsti dall'art. 39, par. 1, lett. b), RGPD. Ciò trova conferma ulteriore nel complesso delle disposizioni di cui all'art. 38 del RGPD laddove si prevede che il titolare e il responsabile del trattamento si assicurano che il RPD non riceva alcuna istruzione, per quanto riguarda l'esecuzione dei propri compiti, e riferisca direttamente al vertice gerarchico del titolare o del responsabile del trattamento.

Il Garante ha rilevato, infine, il mancato rispetto del principio generale di *accountability* che incombe sul titolare del trattamento con particolare riguardo all'onere di attuare un sistema organizzativo e gestionale contraddistinto da misure reali ed efficaci di protezione dei dati nonché comprovabili (v. anche cons. 74 del RGPD). Nel caso specifico, non vi era stata una corretta e puntuale predisposizione degli adempimenti imposti dal RGPD (nel caso di specie informativa, definizione dei rapporti con i soggetti terzi a cui è affidato il trattamento per conto del titolare – responsabili del trattamento –, corretta designazione del RPD) né erano state implementate procedure e prassi organizzative atte a conformare i trattamenti alla disciplina di riferimento (quali, ad es., tra quelle indicate dall'Autorità quali misure correttive, definizione dei tempi di conservazione dei dati e di procedure per la cancellazione automatica dei dati).

Esercizio dei diritti degli interessati

Ancora nel 2024, la materia dell'esercizio dei diritti degli interessati e, in particolare, del diritto di accesso ai dati personali, è stata oggetto di diversi interventi dell'Autorità

14

che, a seguito di reclami presentati dai cittadini, ha adottato provvedimenti correttivi nei confronti di diversi istituti di credito.

Si segnala, in particolare, il provv. 14 novembre 2024, n. 706 (doc. web n. 10091751) con il quale è stato definito il reclamo proposto dal cliente di una banca cui quest'ultima aveva negato l'accesso al *file* audio relativo alla telefonata intercorsa con il servizio clienti (al quale lo stesso, vittima di una operazione fraudolenta, aveva chiesto il blocco dei codici di accesso al proprio conto corrente).

Nel corso dell'istruttoria, l'istituto di credito aveva ritenuto di poter soddisfare l'istanza di accesso del reclamante trasmettendo allo stesso, anziché il *file* audio di interesse, la trascrizione dei dati contenuti in quella porzione di registrazione riferita alle dichiarazioni rese dal reclamante all'operatore del *call center*; ciò in ragione della necessità di tutelare la riservatezza del soggetto terzo coinvolto (l'operatore telefonico) tanto più che – come sostenuto dalla banca – il "dato voce" del cliente era sostanzialmente irrilevante rispetto alla finalità realmente perseguita (ottenere il rimborso integrale della somma fraudolentemente sottratta).

In merito, a prescindere dal fatto che nel corso del procedimento il reclamante aveva dichiarato di non essere più interessato a ricevere le registrazioni oggetto del reclamo, l'Autorità ha evidenziato che, nel caso di specie, ferma restando la corretta valutazione dei diritti e delle libertà dei terzi, il *file* audio in questione poteva essere trasmesso all'interessato nella sua forma originaria. Ciò alla luce delle definizioni di "dato personale" e di "trattamento" di cui all'art. 4 del RGPD, nonché di quanto previsto nelle linee guida 01/2022 sui diritti degli interessati-Diritto di accesso adottate dall'EDPB il 28 marzo 2023 (linee guida cit., par. 4.2.1, punti 105-106 e art. 15, par. 4, RGPD).

Tra i numerosi reclami relativi al mancato o tardivo riscontro da parte di istituti di credito alle istanze presentate dagli interessati ai sensi degli artt. 15 e ss. del RGPD, si segnalano anche due provvedimenti dell'Autorità riguardanti l'esercizio del diritto di accesso ai dati del *de cuius* di cui agli artt. 15 del RGPD e 2-*terdecies* del Codice (provv.ti 7 marzo 2024, n. 160, doc. web n. 10009296; 9 maggio 2024, n. 363, doc. web n. 10044553). In entrambi i casi, il titolare del trattamento aveva omesso di fornire tempestivo riscontro all'istanza di accesso ai dati riferiti al congiunto deceduto in violazione dell'art. 12, par. 3, RGPD.

Si tratta di fattispecie ricorrenti, già esaminate dall'Autorità negli anni precedenti (v. Relazione 2023, p. 163) e rispetto alle quali gli istituti di credito, in via generale, stanno sempre di più apprestando misure organizzative e formative necessarie ad evitare il ripetersi di violazioni similari.

L'Autorità, esaminate le due situazioni e preso atto che nel corso del procedimento le richieste degli interessati erano state pienamente soddisfatte, ai fini della determinazione della sanzione da comminare ha tenuto conto degli elementi previsti dall'art. 83, par. 2, RGPD, tra cui, in particolare, l'assenza di precedenti violazioni a carico della banca per una fattispecie analoga; ciò ha comportato l'applicazione di sanzioni diverse per la medesima violazione.

Sempre in materia di esercizio dei diritti, è stato presentato al Garante un reclamo con il quale l'interessata aveva rappresentato di non avere ricevuto riscontro alla richiesta avanzata a una banca e a una società di *leasing*, volta a conoscere le motivazioni alla base del diniego, ricevuto dalla predetta società, in merito alla stipula di un contratto di noleggio a lungo termine di un'auto e all'inserimento del proprio nominativo nella "lista dei cattivi pagatori".

A seguito di un'articolata attività istruttoria e di accertamenti ispettivi *in loco*, nei confronti sia della banca (capogruppo), sia della società (appartenente allo stesso

gruppo bancario), il Garante ha definito il reclamo con due distinti provv.ti, adottati il 6 giugno 2024, n. 340, doc. web n. 10042684 e n. 341, doc. web n. 10043007.

Dall'attività istruttoria è emerso che il diniego al finanziamento e l'inserimento del nominativo dell'interessata nella *black list* erano stati determinati dall'esito negativo risultato dalla verifica della situazione reddituale della cliente effettuata dalla banca ai fini della stipula del contratto di noleggio con la società tramite il Sistema SCIPAFI (Sistema pubblico di prevenzione del furto di identità istituito dal d.lgs. n. 141/2010, il cui funzionamento è disciplinato dal decreto del MEF 19 maggio 2014, n. 95). Dalle dichiarazioni rese dalla banca e dalla società e dall'esame della documentazione, era emerso che, in base ad un accordo (cd. *Data Processing Agreement*) con ciascuna delle società controllate che avevano agito quali titolari del trattamento, la banca aveva operato in qualità di responsabile, eseguendo determinate tipologie di servizio, per conto del titolare, comprensive anche di attività di trattamento dei dati personali quali "le attività di verifica sulla correttezza dei dati personali inseriti da soggetti interessati a noleggiare un autoveicolo".

L'Autorità ha ritenuto illecito tale trattamento, rilevando che, all'epoca dei fatti, la banca era autorizzata ad accedere a SCIPAFI esclusivamente per lo svolgimento della propria specifica attività (art. 30-*ter*, commi 7 e 7-*bis*, d.lgs. n. 141/2010) e non avrebbe potuto accedervi per conto della società, neppure agendo in qualità di responsabile. La società, infatti, non rientrava tra i soggetti legittimati all'accesso a SCIPAFI né direttamente, né indirettamente tramite i soggetti aderenti al Sistema; analogamente non era autorizzata ad acquisire né a trattare i dati presenti in SCIPAFI, anche se rielaborati e resi disponibili alla società tramite una *watchlist* creata dalla banca, ai fini della valutazione della stipula del contratto di autonoleggio.

L'Autorità, inoltre, nell'evidenziare che, ai fini della valutazione di una richiesta, l'accesso a SCIPAFI consente la verifica dell'autenticità dei dati contenuti nei documenti (di identità o reddituali) presentati dall'interessato confrontandoli con quelli conservati nel Sistema, ha rilevato, nel caso di specie, un ulteriore profilo di illiceità, dal momento che tale accesso era stato effettuato senza avere previamente acquisito dall'interessata la dichiarazione dei redditi, documento indispensabile per effettuare il suddetto confronto.

In relazione al profilo della trasparenza, il Garante ha rilevato che l'informativa resa dalla società all'interessata era generica e non idonea a consentire la chiara individuazione della tipologia di dati trattati, della loro origine e delle specifiche modalità di consultazione delle banche dati. Sebbene la società avesse documentato, nel corso del procedimento, l'aggiornamento della propria informativa, il Garante ha accertato che la versione precedente era inadeguata rispetto ai requisiti normativi.

All'esito dell'attività istruttoria, l'Autorità ha rilevato, pertanto, illeciti i trattamenti posti in essere dalla società in relazione agli artt. 5, par. 1, lett. a), 13 e 28 del RGPD, e dalla banca in relazione agli artt. 5, par. 1, lett. a) e 28 del RGPD e ha comminato rispettivamente sanzioni pecuniarie pari a euro 250.000,00 e 1.000.000,00.

La sicurezza dell'accesso ai dati bancari

Anche nel corso del 2024, l'Autorità ha ricevuto un numero significativo di reclami e segnalazioni concernenti il trattamento dei dati degli interessati nell'ambito dell'attività bancaria, in molti casi definiti mediante note dipartimentali, riguardando i diversi aspetti che regolano il rapporto tra banca e cliente, già oggetto di precedenti provvedimenti del Garante (in particolare, provv. 25 ottobre 2007, n. 53, doc. web n. 1457247).

Molti reclami e segnalazioni hanno riguardato accessi indebiti ai dati dei clienti da parte di dipendenti degli istituti di credito per finalità proprie o per la comunicazione a terzi non autorizzati. Si tratta di un fenomeno da tempo all'attenzione del Garante che, già con il provv. 12 maggio 2011, n. 192 (doc. web n.1813953), aveva prescritto

l'adozione di misure rigorose volte ad impedire illecite operazioni di trattamento ai danni dei clienti.

In particolare, con il citato provvedimento era stata disposta la tracciabilità di ogni operazione di accesso ai dati dei clienti – sia che tale operazione comporti movimentazione di denaro, sia che si tratti di semplice consultazione (operazioni di mera visualizzazione, cd. *inquiry*) – attraverso l'implementazione di sistemi di *alert* idonei a rilevare comportamenti anomali o a rischio. Ciò ha lo scopo di consentire alla stessa banca di individuare tempestivamente chi abbia effettuato il trattamento dei dati dei clienti e il momento in cui ciò è avvenuto.

In molti casi, queste istanze sono state definite senza l'avvio di procedimenti in quanto, all'esito dell'attività istruttoria avviata, è emerso trattarsi di accessi avvenuti nell'ambito della corretta operatività della banca.

L'Autorità, tuttavia, tenuto conto del tempo trascorso dall'adozione del citato provvedimento e anche sulla base delle notifiche di *data breach* pervenute da parte degli istituti bancari, ha comunque avviato una complessa attività di verifica, attraverso lo svolgimento di diverse ispezioni, sull'implementazione dei sistemi di *alert*, sulle modalità e i sistemi di controllo degli accessi dei dipendenti e sul rispetto delle comunicazioni inviate al Garante e agli interessati, in caso di violazioni di dati. Gli esiti di tali attività consentiranno, nel 2025, di avere un quadro esaustivo sull'adeguatezza delle misure adottate dai diversi titolari del trattamento e sull'eventuale necessità di introdurre dei correttivi.

Trattamento dei dati nei Sistemi di informazione creditizia (SIC)

L'Autorità ha ricevuto numerose segnalazioni relative al trattamento dei dati personali nei sistemi di informazione creditizia (SIC), con particolare riferimento al profilo del preavviso di segnalazione da inviare all'interessato al verificarsi del primo ritardo e prima dell'inserimento dei dati nei SIC e ai tempi di conservazione dei dati nei SIC (diversi a seconda che il rapporto censito sia stato stipulato o meno e, in caso positivo, che abbia o meno un andamento regolare).

In tutti i casi esaminati sono state richiamate le disposizioni contenute nel codice di condotta in materia di informazioni creditizie, adottato inizialmente dal Garante il 12 settembre 2019 e approvato in via definitiva con provv. 6 ottobre 2022, n. 324 con il quale è stato accreditato il relativo Organismo di Monitoraggio-OdM (doc. web n. 9818201).

Nella quasi totalità delle fattispecie esaminate, non sono risultate comprovate violazioni della normativa in materia di protezione dei dati personali.

Rete dei RPD nel settore bancario

Nel corso del 2024, è proseguita l'attività del Gruppo di lavoro rete dei RPD nel settore bancario; in particolare, nel corso di alcuni incontri che si sono svolti alla presenza di ABI, degli RPD della rete e del RPD di Banca d'Italia, sono state affrontate diverse questioni che necessitano di approfondimento e confronto (tra cui, l'applicazione della cd. normativa sull'antiriciclaggio) ed è proseguita l'attività volta alla realizzazione di informative omogenee e semplificate, da rendere anche mediante l'utilizzo di icone standardizzate.

Nell'ambito dell'attività effettuata dalla rete dei RPD in tale settore, il 20 febbraio 2024, in occasione di un convegno svoltosi presso ABI, sono stati illustrati i risultati del questionario condotto da ABI, in collaborazione con il Garante, avente l'obiettivo di fornire una "fotografia" delle caratteristiche che connotano il ruolo e l'attività dei RPD in questo ambito (v. Relazione 2023, p. 169-170). L'opuscolo contenente gli atti del convegno e i risultati del questionario sono stati poi pubblicati sui siti del Garante e dell'ABI (doc. web n. 9989892).

Attività di coordinamento con altri organismi europei

Nel contesto delle attività di coordinamento con organismi europei, il sottogruppo *Financial Matters* del CEPD, nell'ambito di un progetto relativo all'utilizzo delle cd.

watchlists per finalità antiriciclaggio e di contrasto al finanziamento del terrorismo, ha predisposto un questionario al fine di ottenere indicazioni in merito al trattamento dei dati personali degli interessati in tale ambito da parte degli istituti di credito quali soggetti obbligati (cfr. 21.1). Tale questionario è stato veicolato, attraverso l'ABI e FEDERCASSE, quali associazioni di categoria del settore bancario, a un campione rappresentativo di istituti di credito. I relativi risultati sono poi stati restituiti all'Autorità in forma aggregata e da questa trasmessi al CEPD per la successiva elaborazione, i cui esiti saranno resi noti nel 2025.

14.3. *Imprese*

Nel corso del 2024, i trattamenti di dati personali effettuati nel settore delle attività a carattere economico hanno impegnato attivamente il Garante in considerazione dell'elevato numero di istanze a vario titolo avanzate.

Gli interventi dell'Autorità sono stati sia di portata generale, in quanto volti a dare piena attuazione alla normativa in materia di protezione dati nonché a dirimere questioni interpretative, sia più puntuali su specifiche fattispecie.

Ruolo del *servicer* e cartolarizzazione dei crediti

Nell'ambito di tale attività, l'Autorità è intervenuta in materia di illiceità del trattamento dei dati dei debitori ceduti a seguito di un'operazione di cartolarizzazione dei crediti (art. 3, l. 30 aprile 1999, n. 130) con due decisioni adottate rispettivamente nei confronti del titolare del trattamento (provv. 17 ottobre 2024, n. 616, doc. web n. 1008442) e del responsabile designato ai sensi dell'art. 28 del RGPD (provv. 17 ottobre 2024, n. 615, doc. web n. 10084403).

I provvedimenti hanno tratto origine da un reclamo con cui l'istante ha segnalato che il *"servicer"* (responsabile *ex* art. 28 del RGPD), incaricato dallo *special purpose vehicle* (titolare del trattamento) del recupero dei crediti oggetto dell'operazione di cartolarizzazione (tra i quali figurava un debito del reclamante), avrebbe utilizzato, quale recapito per contattare quest'ultimo, dati personali (nella specie l'indirizzo *e-mail*) riferiti ad un terzo soggetto estraneo al rapporto di debito. Il tutto senza riuscire a fornire né al reclamante a seguito di istanza di esercizio dei diritti, né all'Autorità in sede di accertamento ispettivo, elementi in ordine all'origine e alle conseguenziali modalità di acquisizione del predetto dato.

L'istruttoria ha evidenziato l'inosservanza, da parte del summenzionato "*servicer*", degli obblighi gravanti sullo stesso ai sensi dell'art. 28, par. 3, RGPD ed in particolare dell'onere di tenere traccia dell'origine del dato di contatto del debitore utilizzato dalla predetta società al fine di sollecitare il pagamento del relativo insoluto. È infatti emersa l'inadeguatezza delle misure tecniche e organizzative implementate dal responsabile nello svolgimento di un'attività rispetto alla quale lo stesso si poneva sul mercato quale operatore leader nel settore; misure, che, sebbene prescritte dal titolare nell'ambito delle istruzioni da questi impartite ai sensi dell'art. 28 del RGPD, non erano state correttamente eseguite.

È stata dunque accertata la violazione, da parte della citata società, dell'art. 28, par. 3, lett. a), e) e h), RGPD con conseguente inadempimento dell'incarico allo stesso conferito; inadempimento che ha comportato, quale diretta conseguenza, l'impossibilità per il titolare di conformarsi alla disciplina di protezione dei dati all'atto del riscontro ad una richiesta di accesso ai dati avanzata da uno dei debitori ceduti. Il Garante ha quindi comminato nei confronti del "*servicer*" una sanzione pecuniaria di euro 60.000,00.

Nei confronti dello "*special purpose vehicle*", titolare del trattamento, è altresì stata

14

Obblighi del responsabile del trattamento e diritti degli interessati

rilevata una residuale responsabilità a titolo di *culpa in vigilando*, per non avere approntato efficaci ed adeguati strumenti di verifica dell'operato del succitato responsabile (art. 5, parr. 1, lett. a) e d) e 2; art. 24 del RGPD). È stata da ultimo rilevata, sempre a carico dello "*special purpose vehicle*", la violazione degli artt. 30 e 37 del RGPD, nonché dell'art. 157 del Codice.

In materia di esercizio dei diritti degli interessati e con specifico riferimento agli obblighi previsti al riguardo in capo al responsabile del trattamento *ex* art. 28 del RGPD, il Garante si è pronunciato nei confronti di una società che si occupa di erogare servizi di telemedicina e gestire per conto di soggetti terzi procedure liquidatorie e di accertamento in occasione di sinistri. Tale pronuncia è stata adottata a seguito del reclamo presentato da un assistito, che aveva lamentato il mancato riscontro da parte della predetta società, operante in tale contesto quale responsabile del trattamento, ad un'istanza di esercizio del diritto di accesso ai dati che lo riguardavano (provv. 13 novembre 2024, n. 676, doc. web n. 10088943).

Il provvedimento ha costituito l'occasione per chiarire che – sebbene il responsabile del trattamento non sia il soggetto deputato a fornire direttamente riscontro alle istanze di esercizio dei diritti presentate dagli interessati ai sensi degli artt. 15-22 e ss. del RGPD – l'art. 28, par. 3, lett. e), RGPD prevede, comunque, che lo stesso debba assistere il titolare in tale frangente (cfr. in merito CEPD, linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del RGPD, adottate il 7 luglio 2021, par. 1.3.5), sulla base del contratto (o di altro atto giuridico) che deve regolamentare il rapporto instauratosi con il titolare anche rispetto a tale specifico profilo.

Nel corso dell'istruttoria è stato accertato che la società non aveva invece reso alcun riscontro all'istanza del reclamante – quantomeno in termini di chiarimenti in ordine al ruolo dalla medesima rivestito rispetto alla disciplina in materia di protezione dei dati personali – né aveva provveduto a veicolare tempestivamente, come stabilito invece attraverso apposite istruzioni nell'atto di designazione, la suddetta istanza al titolare del trattamento, affinché potesse darvi seguito nei termini di cui all'art. 12, par. 3, RGPD.

Tale condotta è risultata in contrasto con l'art. 28, par. 3, lett. e), RGPD ed è stata pertanto applicata dal Garante una sanzione pecuniaria di euro 15.000,00.

Piattaforma informatica per i contratti di mutuo

Con provv. 11 gennaio 2024, n. 58 (doc. web n. 9993548) è stata definita una complessa e articolata istruttoria avviata a seguito di una richiesta di chiarimenti in merito al funzionamento di una piattaforma informatica utilizzata da istituti di credito e notai per lo scambio della documentazione necessaria alla stipula di contratti di mutuo. In particolare, considerato che le modalità operative della citata piattaforma (o "portale") avevano implicato il trattamento di dati personali di diversi soggetti (dati dei mutuatari e di terzi strettamente correlati nonché dati riferiti ai notai), sono state rappresentate alcune criticità in ordine ai rapporti, nei termini di ruoli *privacy*, tra la società titolare della piattaforma, i notai e gli istituti di credito coinvolti.

Dall'attività istruttoria, nel corso della quale sono state acquisite informazioni dalla società che aveva gestito la piattaforma e da alcuni importanti istituti di credito che, avvalendosi della stessa, l'avevano proposta ai notai che volontariamente vi avevano aderito, è emerso un quadro di elevata complessità.

È stato innanzitutto rilevato che ciascuna banca, nel rapporto con la società che aveva gestito il portale e con la quale aveva sottoscritto un contratto di appalto per la fornitura di un servizio (corredato da un apposito *data protection agreement*), aveva operato quale titolare del trattamento provvedendo a preporre la società stessa quale responsabile del trattamento ai sensi dell'art. 28 del RGPD.

Tale società, nell'espletare la sua attività per conto delle banche, aveva posto però in essere un trattamento di dati personali dei notai per una finalità diversa e ulteriore rispetto a quella contrattualmente prevista e per la quale aveva ricevuto le dovute istruzioni (invio di un *report* riepilogativo); ne era derivato che, per quanto ciascun responsabile del trattamento, nello svolgimento dei propri compiti, possa agire con "autonomia di mezzi e di organizzazione" purché nel rispetto delle istruzioni ricevute (cfr. linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento adottate dall'EDPB il 7 luglio 2021), la società, determinando finalità e mezzi dell'ulteriore trattamento effettuato, aveva agito quale titolare del trattamento in questione (art. 28, par. 10, RGPD) e, conseguentemente, violato i principi di liceità del trattamento (tra cui, in particolare, assenza di base giuridica e di informativa).

Nel corso del procedimento, è emersa, altresì, una ulteriore criticità in relazione alla corretta individuazione, da parte della società in questione, della base giuridica legittimante il trattamento dei dati personali dei notai nella fase della registrazione degli stessi al portale e della generazione e gestione delle rispettive credenziali di autenticazione informatica. In particolare, considerato che tale trattamento è necessario per consentire a ciascun notaio di fruire di un servizio di autenticazione informatica funzionale all'accesso al portale, l'Autorità ha rilevato la sussistenza di un rapporto di natura contrattuale tra la società e i notai, con la conseguenza che il trattamento dei dati personali di questi ultimi trova la sua condizione di liceità nell'art. 6, par. 1, lett. b), RGPD (e non nell'art. 6, par. 1, lett. f), come invece individuato dalla società).

All'esito dell'istruttoria l'Autorità ha quindi adottato nei confronti della società un provvedimento di carattere sanzionatorio prescrivendo, altresì, di conformare il trattamento posto in essere alla disciplina in materia di protezione dei dati personali.

Codice di condotta PMI

Sono proseguite le attività di interlocuzione e confronto con le associazioni maggiormente rappresentative delle piccole e medie imprese (PMI) allo scopo di definire, nei vari settori di riferimento, i possibili interventi, anche per offrire chiarimenti e/o semplificazioni rispetto agli adempimenti previsti dalla normativa in materia di protezione dei dati personali.

Il 17 ottobre 2024 il Garante ha approvato il codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di *software* gestionali ovvero il primo codice di condotta con validità in ambito nazionale in un settore altamente specializzato quale quello delle imprese ICT (provv. 17 ottobre 2024, n. 618, doc. web n. 10077212).

Tale codice, la cui adozione è stata proposta dall'unico organismo rappresentativo a livello nazionale dello specifico settore della produzione *software* in Italia, si propone di definire una serie di regole e di misure tecniche ed organizzative volte a garantire che i *software* prodotti e resi disponibili sul mercato dalle imprese aderenti siano sviluppati nel rispetto dei principi di protezione dei dati fin dalla progettazione (*by design*) e per impostazione predefinita (*by default*) assicurando che l'attività delle imprese aderenti durante l'intero ciclo di vita del software, dalla sua progettazione, produzione e sviluppo sino alla sua installazione e messa in esercizio, si conformi ad elevati livelli di protezione dei dati personali.

Oltre a favorire il rispetto del RGPD, il codice si prefigge anche di aumentare la fiducia degli utilizzatori del *software* verso l'adozione di soluzioni gestionali in grado di realizzare la transizione digitale e l'innovazione produttiva.

Con il medesimo provvedimento, il Garante ha contestualmente accreditato l'organismo di monitoraggio, composto da esperti nello specifico settore di riferimento, con particolare riguardo ai profili di protezione dei dati personali.

Progetti europei

Nel corso del 2024, si è concluso il Progetto ARC II finanziato dalla Commissione

europea del quale il Garante è *partner* in collaborazione con l'Università di Firenze (v. Relazione 2023, p. 228; cfr. par. 21.6).

Il progetto, dedicato alle PMI di Italia e Croazia, è volto ad incrementare la conoscenza degli obblighi derivanti dal RGPD e dal quadro giuridico italiano e croato in materia di protezione dei dati personali.

Nell'ambito del progetto sono stati organizzati diversi incontri, da remoto e in presenza, su temi specifici di particolare interesse per le piccole e medie imprese.

Molteplici sono stati i temi approfonditi con gli RPD e personale del settore quali il trattamento dei dati nell'ambito del rapporto di lavoro, l'attuazione dell'*accountability*, i diritti degli interessati, la videosorveglianza e le nuove tecnologie. Inoltre, nel corso dello stesso anno, è stato reso disponibile uno strumento digitale in formato *open source*, in italiano, inglese e croato che, attraverso moduli di apprendimento e questionari, supporterà le PMI nel conformarsi alla normativa in materia di protezione dei dati personali (cfr. par. 21.6).

Nell'ambito del *Coordinated Enforcement Action* (CEF) 2024, il Garante italiano ha condotto anche un'ampia attività di tipo ricognitivo, in coordinamento con le altre autorità europee di protezione dati, sul diritto di accesso dell'interessato ai sensi dell'art.15 del RGPD. L'Autorità ha quindi inviato un questionario a una selezione di titolari del trattamento distribuiti su tutto il territorio nazionale – in particolare del settore energetico, della sanità, delle telecomunicazioni e dell'editoria – al fine di identificare criticità e buone pratiche adottate per garantire la corretta applicazione di tale diritto. I risultati saranno diffusi dal CEPD nell'ambito della propria relazione annuale.

14.4. *Concessionari di pubblici servizi*

Tavolo di confronto con i principali fornitori del settore energetico

Gli interventi normativi susseguitisi in materia di liberalizzazione del mercato dell'energia elettrica hanno impegnato il Garante in un'intensa attività di approfondimento delle disposizioni emanate a tal fine, nonché di collaborazione con l'ARERA, nella prospettiva di valutare le implicazioni connesse al trattamento di dati personali della clientela a seguito della definizione di tale processo, con particolare riguardo alle disposizioni sulla cessazione del Servizio di maggior tutela e sul conseguenziale passaggio *ope legis* di circa 5 milioni di clienti al Servizio a tutele graduali.

In quest'ottica, è stato anche avviato un tavolo di confronto con i principali fornitori del settore energetico direttamente coinvolti dalle nuove regole (ossia le società aggiudicatarie delle aste indette per l'assegnazione del Servizio a tutele graduali e i fornitori esercenti il Servizio di maggior tutela), con l'obiettivo di condividere con gli stessi alcune possibili modalità operative da adottare al fine di tutelare adeguatamente i diritti e le libertà dei soggetti interessati coinvolti.

Sono stati inoltre effettuati diversi incontri presso la sede dell'Autorità ove sono state fornite indicazioni e chiarimenti in ordine, in particolare, ai presupposti di liceità del trattamento dei clienti migrati al Servizio a tutele graduali (art. 6 del RGPD); alle modalità con cui rendere, ai sensi degli artt. 13 e 14 del RGPD, l'informativa alla clientela acquisita in fase di assegnazione del relativo Servizio; al rispetto del principio di conservazione da parte dei gestori cedenti e aggiudicatari dello stesso (art. 5, par. 1, lett. c) ed e), RGPD); agli strumenti per la comunicazione dei dati inerenti alle modalità di pagamento delle bollette, al canale di trasmissione delle stesse e al recapito digitale prescelto dal cliente.

Attività di vigilanza sui trattamenti di dati nel settore dell'energia

Sempre nel settore dell'energia, è altresì proseguita (v. Relazione 2023, p. 174-176) l'attività di vigilanza e di controllo con riferimento alle pratiche illecite dei cd. contratti non richiesti nel mercato libero, ove effettuate per il tramite di trattamenti di dati personali inesatti e non aggiornati.

Al riguardo, l'Autorità si è pronunciata, con provvedimento 17 luglio 2024, n. 440 (doc. web n. 10053211) nei confronti di un fornitore operante su scala nazionale, a seguito della ricezione di numerose segnalazioni e reclami.

In particolare, i reclamanti avevano lamentato di aver appreso dell'attivazione a loro insaputa dei contratti di fornitura, solo successivamente alla ricezione da parte della società di comunicazioni inerenti alla stessa, senza aver mai avuto alcun precedente contatto con il fornitore di energia. In alcuni casi inoltre era stato segnalato l'inesatto o tardivo riscontro del titolare alle richieste di esercizio dei diritti avanzate dagli interessati ai sensi del RGPD.

La pronuncia ha accertato l'illiceità del trattamento dei dati personali di circa 2.300 clienti in considerazione della violazione dell'art. 5, par. 1, lett. a), b), d), e) ed f) e par. 2; dell'art. 12, par. 3; dell'art. 15; dell'art. 24; dell'art. 28 e dell'art. 32 del RGPD.

Dagli accertamenti ispettivi effettuati *in loco*, infatti, era emerso che la società non aveva adottato misure tecniche e organizzative adeguate a prevenire l'utilizzo illecito dei dati dei clienti da parte dei propri agenti porta a porta, rendendo possibile per quest'ultimi l'acquisizione delle generalità degli interessati mediante l'uso di dispositivi personali (ad es. tramite foto del relativo documento di riconoscimento scattata con il telefono), l'utilizzo degli stessi indirizzi *e-mail*/numeri di telefono per diversi contratti anche riferiti a differenti clienti, la trasmissione della documentazione contrattuale ad indirizzi diversi da quello di fornitura.

È altresì risultato inadeguato il sistema di "telefonate di controllo" utilizzato dalla società per la verifica della corretta acquisizione dei dati personali riportati all'interno della proposta contrattuale: nella maggior parte dei casi, infatti, è stato completato il processo di attivazione della fornitura anche ove tali chiamate non erano andate a buon fine per l'irreperibilità della persona contattata.

La società, inoltre, non aveva effettuato alcuna attività di *audit* volta a verificare l'operato delle agenzie designate responsabili del trattamento in ordine agli adempimenti di cui al RGPD, né aveva posto in essere specifiche iniziative finalizzate alla formazione in materia di protezione dei dati personali dei singoli agenti.

Infine, non si era dotata di un sistema idoneo a prevedere, a seguito di un reclamo per attivazione non richiesta (e nelle more della definizione dello stesso), forme di segregazione di ogni ulteriore e diversa attività di trattamento dei dati dei relativi ai clienti, nell'ottica di sospendere in via precauzionale eventuali trattamenti illeciti dei predetti dati per altre finalità (ad es. per finalità di *marketing* o di profilazione). Non sono inoltre risultate conformi al RGPD le *policy* di *data retention* adottate dalla società rispetto ai trattamenti inerenti ai dati della clientela.

Da ultimo, è stato accertato che, rispetto ai reclami inerenti all'esercizio dei diritti *ex* artt. 15-22 del RGPD, il titolare aveva fornito un riscontro inadeguato alle istanze di accesso presentate dagli interessati, limitandosi ad elencare le sole categorie di dati trattate oppure a trasmettere esclusivamente copia dell'informativa *ex* art. 13 del RGPD.

Il Garante ha pertanto irrogato una sanzione pecuniaria pari a euro 5.000.000,00 e ha imposto alla società l'adozione di una serie di misure tecniche e organizzative volte a conformare i trattamenti alla normativa sulla protezione dei dati quali: l'utilizzo di un sistema di "telefonate di controllo" bloccante che consenta di verificare la correttezza

dei contratti acquisiti tramite la rete di agenti; l'implementazione di regole procedurali in relazione alle quali, a fronte della ricezione di volumi anomali di proposte contrattuali, disconoscimenti, reclami per attivazione non richieste, siano effettuate specifiche attività di verifica sulla generalità delle operazioni di contrattualizzazione poste in essere dall'agenzia coinvolta; la previsione di *audit* periodici per la valutazione dell'operato delle agenzie incaricate ai sensi dell'art. 28 del RGPD; l'adozione di procedure che prevedano la tempestiva limitazione, in attesa dell'esito dei successivi controlli, di ogni ulteriore attività di trattamento dei dati personali inerenti a contratti/proposte contrattuali rispetto alle quali sia stato presentato un reclamo per attivazione non richiesta nonché l'individuazione di specifici tempi di conservazione dei dati, distinti per categoria e finalità di trattamento.

14.5. *Attività di recupero crediti*

Numerosi sono stati i reclami e le segnalazioni concernenti il settore del recupero crediti pervenuti nel corso dell'anno talvolta finalizzati alla negoziazione con le società creditrici, invece che a denunciare violazioni della normativa in materia di protezione dati.

Molte istanze sono risultate prive di elementi fattuali o comunque utili a dimostrare eventuali violazioni nelle fasi del recupero crediti come previsto dal relativo provv. generale 30 novembre 2005 (doc. web n. 1213644). Altre hanno riguardato questioni che esulano dall'ambito di competenza dell'Autorità (cfr. artt. 57 del RGPD e 154 del Codice), come nel caso di contestazioni di tipo contrattuale o relative alla stessa sussistenza del debito, che devono essere fatte valere presso il soggetto creditore o di fronte ad altra autorità e non davanti al Garante.

Attraverso note di chiarimento, il Garante ha ricordato le modalità corrette di esercizio dei diritti, in particolare quello di accesso, di opposizione e di cancellazione dei dati personali nelle attività di recupero crediti.

In molti altri casi, sempre attraverso note indirizzate agli interessati, il Garante ha ricordato che il trattamento dei dati personali nell'ambito dell'attività di recupero crediti, nella maggior parte dei casi, trova la sua base giuridica nel legittimo interesse perseguito dal titolare (v. art. 6 par.1, lett. f), RGPD) e non nel consenso dell'interessato, in questo caso del debitore. Di conseguenza non sono state rilevate, di norma, illiceità nei confronti di titolari del trattamento, o di società di recupero crediti da essi incaricate, per avere utilizzato recapiti dell'interessato in relazione ai quali quest'ultimo non aveva preventivamente fornito il consenso; sempre però nel rispetto della normativa e del suddetto provvedimento generale che, ad es., vieta la comunicazione di dati sulla situazione debitoria ai soggetti terzi che non hanno diritto di conoscerla.

Nell'ambito di alcune istruttorie, pur non essendo emersi gli elementi per l'adozione di provvedimenti collegiali, l'Autorità ha comunque esercitato i propri poteri nei confronti dei titolari e responsabili del trattamento (art. 57, par. 1, lett. d), RGPD), con inviti ad adeguarsi o ad aderire, al fine di migliorare le specifiche modalità di condotta nel settore.

In particolare, le indicazioni del Garante sono state tese a prevenire il verificarsi di casi di comunicazioni di dati personali a soggetti terzi e a far adottare ulteriori misure (di vigilanza sull'operato del personale, nonché formative e di sensibilizzazione dello stesso personale) e ogni possibile iniziativa di competenza, volte a garantire l'osservanza della normativa e a rafforzare il livello di tutela degli interessati. Alcune criticità sono infine emerse nello specifico ambito del recupero dei dati di contatto e di ulteriori in-

formazioni sui debitori, in particolare rispetto all'utilizzo di banche dati pubbliche e private, o di agenzie investigative, rispetto alle quali sono in corso attività istruttorie anche di carattere ispettivo.

14.6. *Accreditamento e certificazioni*

Nel corso del 2024 è proseguito il rapporto collaborativo tra il Garante e l'Ente nazionale di accreditamento, Accredia; rapporto già consolidatosi da tempo, a partire dal 2019, a seguito dell'avvio di un tavolo di lavoro con l'Ente sul tema dell'accreditamento e della certificazione ai sensi degli artt. 42 e 43 del RGPD (cfr. Relazione 2019, p. 159). A marzo 2024 è stata infatti rinnovata, per ulteriori cinque anni, la Convenzione sottoscritta tra Garante e Accredia, finalizzata allo scambio vicendevole e regolare di informazioni in merito alle attività di accreditamento, previste dall'art. 43 del RGPD, per il rilascio delle certificazioni ai sensi dell'art. 42; tutto ciò a fronte di una preliminare attività di revisione e di aggiornamento della stessa (cfr. Relazione 2021, p. 187).

Durante l'anno, il Garante ha inoltre fornito informazioni, chiarimenti e supporto in relazione alle prime richieste di accreditamento da parte di alcuni organismi di certificazione nazionali rispetto allo schema Europrivacy adottato il 10 ottobre 2022, con parere 28/2022 dal CEPD, come sigillo europeo per la protezione dei dati a norma dell'art. 42, par. 5, RGPD (cfr. Relazione 2022, p. 183).

Sono altresì proseguite le interlocuzioni a livello nazionale con i soggetti coinvolti a vario titolo nell'istituzione dei meccanismi di certificazione. In tale contesto, nell'agosto 2024, è stato formalmente sottoposto all'attenzione dell'Autorità il primo schema di certificazione a livello nazionale al fine di ottenere l'approvazione dello stesso da parte del Garante ai sensi degli artt. 42, parr. 5 e 58, par. 2, lett. f), RGPD, previo parere di coerenza del CEPD di cui all'art. 64, par. 1, lett. c), RGPD.

15 Altri trattamenti in ambito privato

15.1. *Trattamento di dati personali nell'ambito del condominio*

Nel 2024 si è registrato un significativo afflusso di istanze relative all'ambito condominiale, in prevalenza relative ad argomenti già esaminati e definiti dal Garante ed esposti più volte anche in occasione di precedenti Relazioni.

L'Autorità, in particolare, è tornata ancora una volta a occuparsi della questione relativa alla circolazione dei dati tra i partecipanti alla compagine condominiale.

In un caso oggetto di un reclamo relativo alla installazione di uno spioncino digitale effettuata in assenza di una preventiva informativa agli altri condomini, nel richiamare le regole da seguire per la rilevazione delle immagini mediante sistemi di videosorveglianza, il Garante ha precisato che la presenza di tali apparecchi non deve essere segnalata con un apposito cartello né essere preventivamente approvata dall'assemblea del condominio, essendo i medesimi apparecchi installati per finalità di mero controllo degli accessi (nota 23 dicembre 2024).

Durante la trattazione di un reclamo presentato nei confronti di un amministratore che aveva inviato ai condomini l'atto di citazione relativo al giudizio instaurato dal condominio nei confronti dei reclamanti in cui erano riportati i certificati di residenza dei medesimi e i loro dati personali, l'Autorità ha evidenziato che le informazioni personali riferibili a ciascun condomino possono essere trattate per la finalità di gestione ed amministrazione del condominio; in tale ambito, possono altresì formare oggetto di trattamento anche dati personali di natura sensibile o dati giudiziari, nella misura indispensabile al perseguimento delle medesime finalità. Nel caso di specie i soggetti destinatari della comunicazione oggetto di contestazione erano i partecipanti alla compagine condominiale a cui l'amministratore *pro tempore*, nell'ambito dell'espletamento del proprio incarico, aveva trasmesso l'atto di citazione in quanto afferente al giudizio promosso dal condominio stesso e, dunque, dalla collettività dei condomini (nota 13 dicembre 2024).

All'esito della trattazione di un reclamo con cui era stata lamentata l'installazione di *dashcam* su autovetture all'interno di due condomini, il Garante ha ricordato che, in via generale, in base all'art. 2, par. 2, RGPD il trattamento effettuato da una "persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico" non ricade nell'ambito di applicazione del RGPD, anche alla luce di quanto indicato nel cons. n. 18 del RGPD, ossia che "si considera attività a carattere esclusivamente personale o domestico quella effettuata senza che si realizzi una connessione con un'attività commerciale o professionale" (nota 12 novembre 2024).

Nel definire un altro reclamo con cui veniva lamentata la condotta tenuta dall'amministratore del condominio in occasione dell'invio di comunicazioni di posta elettronica con l'indirizzo *e-mail* degli interessati "in chiaro", è stato ribadito in generale che, pur afferendo il contenuto delle *e-mail* a temi concernenti la gestione e l'amministrazione del condominio, la trasmissione della medesima comunicazione a più destinatari, i cui dati personali (nella specie gli indirizzi *e-mail*) siano visibili in chiaro, non è conforme alla normativa in materia di protezione dei dati personali se non sorretta dai presupposti di liceità di cui all'art. 6 del RGPD (nota 21 febbraio 2024).

15.2. *Trattamento di dati da parte di associazioni e fondazioni*

Numerose le istanze pervenute nel settore del trattamento di dati personali in ambito associativo.

All'esito di un procedimento avviato a seguito di una segnalazione, il Garante ha adottato un provvedimento nei confronti dell'associazione della Croce rossa italiana in relazione alla pubblicazione sul web, effettuata da parte del comitato regionale Molise, di un provvedimento del Commissario straordinario a cui era allegato l'elenco dei nominativi di tutti i soci della Croce rossa del Molise, compresi l'indicazione del codice fiscale, data e luogo di nascita e sezione di appartenenza (provv. 26 settembre 2024, n. 592, doc. web n. 10070596).

Il Garante ha precisato che, allo scopo di contemperare le esigenze di pubblicità e trasparenza con i diritti degli interessati, anche nei casi in cui sussista un obbligo normativo che impone la pubblicazione di un atto o di un documento da parte di un soggetto tenuto agli obblighi di trasparenza previsti dalla disciplina pubblicistica, è comunque sempre necessario verificare che non siano pubblicati dati eccedenti, nel rispetto del principio di minimizzazione previsto dall'art. 5 del RGPD.

I soggetti chiamati a dare attuazione agli obblighi di pubblicazione di atti o documenti previsti nel d.lgs. n. 33/2013 non possono comunque "rendere […] intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione" (art. 4, comma 4, d.lgs. n. 33/2013). Di conseguenza, laddove le finalità di trasparenza possano essere adeguatamente conseguite anche senza diffondere dati personali, gli stessi devono essere rimossi dagli atti e dai documenti oggetto di pubblicazione *online*.

In altri casi, le contestazioni mosse dall'Autorità hanno riguardato i presupposti di liceità del trattamento individuati nell'art. 6 del RGPD.

In particolare, nel corso dell'esame di un reclamo, è stata rilevata l'illiceità del trattamento posto in essere da un'associazione sportiva, alla quale è stato rivolto un ammonimento. L'associazione aveva pubblicato il verbale della seduta del consiglio direttivo con cui veniva deliberata la radiazione del reclamante tramite affissione sulla bacheca situata in un luogo aperto al pubblico.

Nel caso di specie, il trattamento dei dati personali dell'associato non poteva essere sorretto dal presupposto del legittimo interesse invocato dall'ente, in quanto le finalità statutarie di quest'ultimo avrebbero potuto consentire unicamente comunicazioni rivolte "all'interno" dell'ambito associativo (provv. 13 novembre 2024, n. 680, doc. web n. 10105576).

L'Autorità ha ammonito una federazione regionale della confederazione nazionale dell'artigianato e della piccola e media impresa, la quale aveva pubblicato sulla propria pagina internet la notizia del provvedimento di espulsione a carico di uno dei soci (provv. 26 settembre 2024, n. 591, doc. web n. 10071261).

All'esito di un'istruttoria condotta a seguito della notifica al Garante di una violazione dei dati personali (*data breach*), ai sensi dell'art. 33 del RGPD, sono state contestate a un'associazione una serie di condotte relative alla corretta tenuta dei propri sistemi informatici e alle modalità di gestione del *data breach*. Sotto il primo profilo, qualora un'associazione consenta ai propri soci di accedere a un'area riservata del proprio sito internet, è necessario che conservi le loro *password* con tecniche crittografiche adeguate allo stato dell'arte e che, in assenza di tale misura, in caso di violazione dei dati personali conseguente ad un attacco informatico, provveda ad inviare una comunicazione esaustiva e tempestiva per informarne gli interessati.

Per quanto attiene al secondo profilo, è stata riscontrata la mancata adozione di

adeguate misure di sicurezza unitamente alla violazione del principio di integrità e sicurezza e alla tardiva comunicazione del *data breach* agli interessati, nonché la violazione del principio di limitazione della conservazione con riferimento ad alcuni documenti di identità per errore presenti all'interno dei sistemi informatici. L'Autorità ha pertanto adottato un provvedimento sanzionatorio per la violazione degli artt. 5, par. 1, lett. e) e f), 32 e 34 del RGPD (provv. 13 novembre 2024, n. 759, doc. web n. 10109352).

15.3. *Videosorveglianza nel settore privato*

Anche nel 2024 è pervenuto un elevato numero di segnalazioni e reclami riguardanti l'utilizzo di impianti di videosorveglianza da parte di esercizi commerciali, società e piccole imprese.

In continuità con gli orientamenti già consolidati negli anni precedenti, l'Autorità ha adottato diversi provvedimenti sanzionatori nei confronti di imprese individuali e società che avevano effettuato trattamenti di dati personali, per mezzo di impianti di videosorveglianza, in violazione dei principi generali di cui all'art. 5, par. 1, lett. a), RGPD in ragione della violazione dell'obbligo di fornire agli interessati un'idonea informativa, dell'obbligo di non riprendere "aree non di esclusiva pertinenza" come la strada pubblica e/o aree comuni o di proprietà di soggetti terzi, e delle garanzie previste all'art. 4, l. n. 300/1970 richiamato dall'art. 114 del Codice.

L'utilizzo di sistemi di videosorveglianza determina infatti un trattamento di dati personali che deve essere effettuato nel rispetto dei principi generali contenuti nell'art. 5 del RGPD e, in particolare del principio di trasparenza che presuppone che "gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata".

A tale scopo, quindi, il Garante ha ricordato in via generale che il titolare del trattamento deve predisporre idonei cartelli informativi secondo le indicazioni contenute al punto 3.1. del provvedimento in materia di videosorveglianza - 8 aprile 2010 (doc. web n. 1712680) (in tal senso anche le FAQ in materia di videosorveglianza, pubblicate sul sito web dell'Autorità) affinché gli interessati siano resi "consapevoli del fatto che è in funzione un sistema di videosorveglianza".

Nei provvedimenti in questione si è fatto richiamo anche alle linee guida 3/2019 del CEPD, le quali al punto 7) specificano che "le informazioni più importanti devono essere indicate [dal titolare] sul segnale di avvertimento stesso (primo livello) mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello)", e, inoltre, che "Tali informazioni possono essere fornite in combinazione con un'icona per dare, in modo ben visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto (art. 12, par. 7, RGPD). Il formato delle informazioni dovrà adeguarsi alle varie ubicazioni".

L'Autorità è altresì tornata a occuparsi dei trattamenti correlati all'installazione di sistemi di riprese video da parte di persone fisiche per fini esclusivamente personali o domestici. In particolare, richiamati i principi del provvedimento generale del Garante dell'8 aprile 2010 (doc. web n. 1712680), ha chiarito che l'utilizzo di sistemi di videosorveglianza da parte di persone fisiche non ricade nell'ambito di applicazione del RGPD, come previsto dall'art. 2, par. 2, RGPD (e come chiarito dalla Corte di giustizia - CGUE, sez. IV, sentenza 11 dicembre 2014, C-212/13), se il relativo trattamento è effettuato per l'esercizio di attività a carattere esclusivamente personale e domestico, a condizione che l'oggetto della ripresa sia circoscritto alle aree di stretta pertinenza.

Viceversa, il Garante ha sanzionato un soggetto privato per aver installato, presso la propria abitazione, un impianto di videosorveglianza che, a seguito dell'accertamento effettuato dalla Polizia locale, è risultato idoneo a riprendere il portone di ingresso principale di proprietà del titolare e parte della strada pubblica, fino agli spazi prospicienti l'ingresso di un esercizio commerciale posto di fronte all'abitazione del titolare dell'impianto. La ripresa di zone esterne a quelle di pertinenza esclusiva del titolare del trattamento ha determinato infatti un trattamento di dati personali non più ascrivibile al suddetto "esercizio di attività a carattere esclusivamente personale o domestico", ma rientrante nell'ambito di applicazione del RGPD.

Seppure fossero stati prodotti, nel corso dell'istruttoria, elementi atti a dimostrare una personale situazione di disagio connessa al comportamento di persone che frequentano un locale situato di fronte all'abitazione, essi non sono apparsi idonei a legittimare una ripresa costante di aree pubbliche soggette al passaggio di persone.

È stata pertanto ritenuta illecita la condotta posta in essere dal soggetto privato, in quanto contraria al principio di liceità di cui all'art. 5, par. 1, lett. a), RGPD, nonché priva di idonei presupposti di legittimità ai sensi dell'art. 6 del RGPD.

Il Garante ha ordinato al titolare di pagare una somma di denaro a titolo di sanzione pecuniaria e di conformare, ai sensi dell'art. 58, par. 2, lett. d), RGPD, il trattamento dei dati posto in essere limitando la ripresa delle telecamere alle aree di pertinenza e a quelle immediatamente prospicienti (provv. 23 maggio 2024, n. 304, doc. web n. 10043051).

16 Intelligenza artificiale e diritto alla protezione dei dati personali

Con una semplificazione, può affermarsi che, dal punto di vista della regolazione, il 2024 è stato l'anno dell'intelligenza artificiale. A fondamento di questa affermazione stanno, da una parte, il completamento del processo di approvazione del reg. dell'UE sull'IA (reg. (UE) 2024/1689 sull'IA del 13 giugno 2024, che stabilisce regole armonizzate sull'IA e modifica i reg.ti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) n. 2018/858, (UE) n. 2018/1139 e (UE) n. 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828) e, dall'altro, l'adozione della Convenzione-quadro in materia di IA, diritti umani, democrazia e stato di diritto (Convenzione n. 225 firmata a Vilnius il 5 settembre 2024).

AI *Act*

Quanto al reg. UE – i cui tratti essenziali sono stati tratteggiati nella precedente Relazione (p. 187) –, sono noti i plurimi obiettivi (tutti invero ambiziosi) che, (anche) suo tramite, l'Unione mira a perseguire: da un lato, il miglioramento del funzionamento del mercato interno, al fine di prevenire i rischi correlati ad una altrimenti prevedibile frammentazione regolatoria, e la creazione di condizioni e strumenti promozionali (primi fra tutti le *sandbox* regolatorie) volti alla riduzione del *gap* tecnologico rispetto ai più avanzati *competitor* presenti nello scenario globale; dall'altro, assicurare che ciò possa avvenire garantendo livelli elevati di protezione della salute e della sicurezza, come pure dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'UE, unitamente ai valori democratici e le regole dello stato di diritto; non ultima la preoccupazione di assicurare anche la sostenibilità ambientale dei sistemi di IA (notoriamente energivori). In questa prospettiva – non di rado riassunta nella locuzione sintetica "*safe innovation*" – si inscrive allora l'intero intervento normativo, come è noto informato al cd. *risk based approach*; espressione che, semplificando, esige (il rispetto di) regole e misure di garanzia più stringenti (e finanche divieti, seppur circoscritti) quanto più alto si prefigura il rischio per i valori che l'Unione intende tutelare; e, per converso, margini di maggiore libertà nello sviluppo e impiego dell'IA rispetto a sistemi che presentano invece rischi prospettici di minore rilievo.

***Governance* del mercato e dei diritti**

Se non è possibile in questa sede soffermarsi sul dettaglio della nuova disciplina, deve tuttavia riconoscersi (e in questo senso si sono pronunciate le autorità di protezione dei dati europee e, sulla scena nazionale, il Garante) che, nella misura in cui lo sviluppo e l'impiego di sistemi di IA non si esauriscono in una mera (pur rilevante) dinamica di mercato concernente artefatti tecnologici, ma intercettano anche le materie del rispetto di situazioni giuridiche individuali preminenti (diritti e libertà fondamentali) e finanche valori collettivi, quali i meccanismi che assicurano la democraticità degli ordinamenti e la *rule of law*, allora (coerentemente) anche il sistema di *governance* dovrebbe essere adeguatamente calibrato per preservare questi valori e assicurare appropriate forme di tutela all'insegna del principio di effettività. A questa sfida, in un contesto di rapida innovazione tecnologica, è stato chiamato il legislatore dell'Unione con l'AI *Act*, disciplina innovativa da cogliere non isolatamente, ma all'interno di un più ampio orizzonte regolatorio dedicato a disciplinare il contesto digitale con una molteplicità di strumenti che sono venuti affiancandosi alle (più tradizionali) garanzie nel tempo approntate e affinate in materia di protezione dei dati

personali. E in questa prospettiva di promozione di un'innovazione (tecnologica, sociale ed economica) sostenibile, non disgiunta dalla tutela dei diritti fondamentali – così inverando la prospettiva antropocentrica sovente invocata nel *milieu* internazionale –, si sono inscritti, a pochi giorni dalla pubblicazione dell'AI *Act*, i contenuti dell'EDPB *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework*, adottato il 16 luglio 2024 (cfr. par. 21.1).

A.S. 1146

In questo solco si collocano anche i contributi forniti dal Garante in occasione di una pluralità di audizioni parlamentari (indicate nel par. 3.1.1, al quale si rinvia) e, da ultimo, il parere 2 agosto 2024, n. 477 reso alla Presidenza del Consiglio dei ministri su uno schema di disegno di legge recante disposizioni e delega al Governo in materia di IA (doc. web n. 10043532: cfr. par. 3.1.2). Al riguardo, nonostante le menzionate previsioni contenute nell'AI *Act* e i richiamati orientamenti espressi dal CEPD e dal Garante, per quanto riguarda l'ordinamento nazionale deve tuttavia rilevarsi che, allo stato, marcato è lo scostamento dalla previsione contenuta nell'art. 74, par. 8, dell'AI *Act*. Il disegno di legge A.S. 1146 – recante disposizioni e delega al Governo in materia di IA – non ha infatti attribuito al Garante (impregiudicate le attribuzioni del RGPD) alcun ruolo in qualità di autorità di vigilanza del mercato; ciò né rispetto agli ambiti (delicatissimi per quanto riguarda i diritti fondamentali in gioco) individuati dalla disposizione medesima (e indicati nell'All. III AI *Act* ai numeri 1, 6, 7 ed 8), né in relazione ad altri ambiti nei quali pure elevati si prefigurano i rischi per i diritti fondamentali delle persone e i sistemi di IA impiegati che comunque comporteranno il trattamento di dati personali (si tratta, in particolare, dei sistemi di IA ad alto rischio individuati nell'All. III AI *Act*, ai numeri 3, 4 e 5).

La cooperazione tra autorità nell'AI *Act*

Né l'Italia ha ancora provveduto, diversamente da tutti gli ordinamenti nazionali dell'UE che hanno dato attuazione alla disposizione contenuta nell'art. 77, par. 2, AI *Act*, a individuare (entro il 2 novembre 2024, secondo la previsione contenuta nell'art. 77, par. 2, AI *Act*) le autorità di tutela dei diritti fondamentali – e, tra esse, il Garante – chiamato ad interagire all'insegna del principio di leale collaborazione all'interno del più articolato reticolo regolatorio prefigurato dall'AI *Act*. Collaborazione che, mediante opportune forme di coordinamento, ciascuno Stato membro è chiamato ad assicurare (cfr. art. 74, par. 10, AI *Act*) e che si concreta in obblighi di informazione e di consultazione tra le autorità di vigilanza del mercato e le autorità di tutela dei diritti fondamentali secondo le puntuali direttrici individuate da una pluralità di disposizioni dell'AI *Act* di diretta applicazione negli ordinamenti nazionali (cfr. al riguardo le disposizioni contenute negli artt. 77, par. 1; 73, par. 7; 79, par. 1 e 82, par. 1 nonché, con specifico riferimento alla partecipazione alle *sandbox*, nell'art. 57, par. 11, AI *Act*).

CAI

Come si è enunciato nell'*incipit* del presente capitolo, il secondo pilastro regolatorio consolidatosi nel panorama sovranazionale in materia di IA è costituito dalla Convenzione quadro del Consiglio d'Europa sull'IA (n. 225): pur se dotata di un articolato di minor dettaglio (ove comparata all'AI *Act*), essa si caratterizza per l'aspirazione, che ne ha contrassegnato l'intero processo di negoziazione, a fondare un nucleo centrale di principi aventi vocazione globale e non meramente regionale. Come è noto, infatti, la Convenzione è aperta alla ratifica anche agli Stati non appartenenti al Consiglio d'Europa, taluni dei quali hanno partecipato ai lavori che hanno condotto alla sua adozione. Realizzata anche grazie al contributo dei rappresentanti internazionali della società civile, dell'industria e di altre organizzazioni internazionali, la Convenzione ha il suo *focus* nell'enucleazione di una serie di principi di alto livello (e di alto grado di generalizzazione, da adattare ai singoli ordinamenti nazionali) volti ad assicurare che i sistemi di IA possano essere sviluppati ed impiegati nel rispetto dei

diritti umani, della democrazia e dello stato di diritto. Compatibile con l'AI *Act* – di cui mutua l'idea di fondo dell'approccio basato sul rischio consentendo e sposandone i principali concetti chiave (tra gli altri, approccio basato sul rischio, trasparenza lungo la catena del valore dei sistemi di IA, obblighi di documentazione dettagliata per i sistemi di IA ad alto rischio, obblighi di valutazione e gestione dei rischi, strumenti per assicurare un'innovazione sostenibile, previsione di sistemi di *enforcement*), – alla Convenzione gli Stati appartenenti all'UE potranno quindi dare attuazione, perfezionando il processo di ratifica, in virtù della piena attuazione dei principi contenuti nell'AI *Act*.

Un quadro di cooperazione per l'IA

In estrema sintesi, quindi, ciò che traspare da entrambi gli strumenti normativi adottati nel 2024 è la necessità di affrontare le questioni sottese all'introduzione (sempre più estesa) nella società delle tecnologie incentrate sull'IA sulla scorta di principi (per quanto possibile) condivisi nell'arena internazionale. Ed in questa prospettiva si sono collocate le varie iniziative e i diversi tavoli di lavoro presenti a livello internazionale, già oggetto di segnalazione nelle precedenti Relazioni, e nei quali, nell'ambito delle proprie attribuzioni, un ruolo attivo è stato svolto anche dalle autorità di protezione dei dati e, tra esse, dal Garante. Infatti, consapevole della valenza transnazionale dei sistemi di IA e delle implicazioni (anche profonde) sul diritto alla protezione dei dati personali – atteso che parte significativa dei sistemi di IA si fondano o comunque coinvolgono il trattamento di dati personali – anche l'Autorità ha partecipato attivamente ad una pluralità di iniziative di carattere sovranazionale, qui menzionate sinteticamente e per le quali si fa rinvio al cap. 21 ove se ne tratteggiano ulteriori elementi: la *G7 Roundtable of Privacy and Data Protection Authorities* (che ha condotto, in particolare, all'adozione di una Dichiarazione sul ruolo delle autorità di protezione dati nel promuovere un'IA responsabile); i lavori del Gruppo di esperti OCSE su "AI, *data governance and privacy*", nel cui ambito è stato pubblicato nel 2024 l'*Artificial Intelligence Paper* No. 22 dedicato al tema "*Synergies and areas of international co-operation*"; il "*Privacy Symposium: Meeting on State of Artificial Intelligence Regulations, Policies, and Upcoming Challenges*", co-organizzato dal Garante a Roma con la partecipazione dei componenti e dei rappresentanti di altre autorità di protezione dei dati e del CEPD.

Attività provvedimentale

Significativi nella fase attuale – che si contraddistingue per il progressivo farsi, a livello nazionale, di una più articolata cornice normativa (primaria e secondaria) che si misuri con le sfide dell'IA – sono i pareri resi dal Garante: essi hanno riguardato, come anticipato, il disegno di legge in materia di IA, ma anche altri ambiti particolarmente rilevanti, a cominciare da quello della sanità (cfr. par. 5.2), del lavoro – con particolare riferimento al funzionamento del Sistema informativo per l'inclusione sociale e lavorativa (SIISL) (provv. 13 novembre 2024, n. 662, doc. web n. 10079136: cfr. par. 4.2) – e della ricerca (cfr. par. 6.2 e, per rilievi critici rispetto ad una sperimentazione di particolari applicazioni che fanno uso di tecniche di IA nella cd. *smart city*, cfr. par. 4.11). Con riguardo all'attività di *enforcement*, in continuità con gli interventi segnalati nella precedente Relazione, si segnala l'adozione di un provvedimento sanzionatorio nel settore del *food delivery* in relazione al trattamento di dati mediante sistemi algoritmici riferiti ai *rider* (provv. 13 novembre 2024, n. 675, doc. web n. 10074601: cfr. par. 13.1) e di un provvedimento di avvertimento concernente trattamenti suscettibili di essere effettuati per lo sviluppo di modelli linguistici (in italiano) mediante l'impiego di contenuti editoriali (cfr. provv. 27 novembre 2024, 741, doc. web n. 10077129 e par. 12.4).

Tra gli ulteriori fenomeni all'attenzione del Garante possono infine segnalarsi quello del cd. web *scraping* – oggetto di indagine conoscitiva da parte dell'Autorità (doc. web

n. 9972593) all'esito della quale, considerati gli elementi pervenuti, è stata resa disponibile una "Nota informativa in materia di web *scraping*, per finalità di addestramento di IA generativa e di possibili azioni di contrasto a tutela dei dati personali" (cfr. provv. 20 maggio 2024, n. 329, doc. web n. 10020316: par. 12.4) – e il fenomeno dei *deep fake*, ora anche oggetto di segnalazioni al Garante (cfr. cap. 10).

Nella prima parte del 2024 è giunta a conclusione 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), del quale si è dato conto nelle precedenti Relazioni e in forza del quale l'Autorità ha ospitato alcuni dei dottorandi partecipanti al progetto.

È poi stata rinnovata la collaborazione con il Consorzio interuniversitario nazionale per l'informatica - CINI (al quale si è fatto cenno già nella Relazione 2021, p. 195) che ha consentito numerose interlocuzioni e scambi, anche informali, con docenti afferenti al Consorzio e che il Garante reputa di primario rilievo, specie nel contesto dei possibili approfondimenti nel settore dell'IA.

17 Violazioni dei dati personali

Dal 1° gennaio al 31 dicembre 2024 sono state notificate all'Autorità 2.204 violazioni dei dati personali ai sensi dell'art. 33 del RGPD o dell'art. 26 del d.lgs. n. 51/2018 (cfr. parte IV, tab. 9) da parte di soggetti pubblici (22,6% dei casi) e privati (77,4% dei casi). Gran parte delle violazioni dei dati personali è stata notificata per fasi (circa il 66,6% dei casi) con l'invio, in un primo momento, di una notifica preliminare e, successivamente, di una o più notifiche integrative (cfr. parte IV, tab. 10).

In particolare, nel settore pubblico le violazioni dei dati personali hanno riguardato soprattutto comuni, strutture sanitarie e istituti scolastici; nel settore privato sono state coinvolte grandi società del settore delle telecomunicazioni, energetico, bancario e dei servizi, ma anche piccole e medie imprese e professionisti.

La maggior parte delle violazioni dei dati personali notificate ha riguardato la perdita di riservatezza o di disponibilità (anche solo temporanea) dei dati personali (circa 88% dei casi; cfr. parte IV, grafico 11). I fenomeni più frequentemente riscontrati sono stati la diffusione di *malware* di tipo *ransomware*, con compromissione della disponibilità e, in molti casi, della riservatezza dei dati all'interno di sistemi *server* o di postazioni di lavoro di organizzazioni pubbliche e private; l'accesso non autorizzato o illecito ai dati personali trattati all'interno di sistemi informativi; la compromissione di credenziali di autenticazione informatica; la divulgazione accidentale di dati personali a causa di erronea configurazione o utilizzo di piattaforme informatiche o di sistemi *software* di gestione della posta elettronica.

L'attività istruttoria svolta a seguito della notifica delle violazioni dei dati personali ha avuto un duplice obiettivo: quello di esaminare l'adeguatezza delle misure adottate dal titolare del trattamento (o che lo stesso intendeva adottare) per porre rimedio alla violazione dei dati personali o per attenuarne i possibili effetti negativi nei confronti degli interessati, nonché quello di valutare la necessità di comunicare la violazione agli interessati coinvolti, fornendo loro indicazioni specifiche sulle misure da adottare per proteggersi da eventuali conseguenze pregiudizievoli.

Laddove non compiutamente rappresentati dal titolare del trattamento, sono stati acquisiti elementi necessari alla valutazione del rischio derivante dalla violazione oggetto di notifica o dell'adeguatezza delle misure in essere al momento della violazione e di quelle adottate per porvi rimedio, sia attraverso acquisizione documentale, sia attraverso specifiche attività ispettive presso i titolari o i responsabili del trattamento.

Con riferimento ad alcune violazioni dei dati personali rispetto alle quali i titolari del trattamento avevano ritenuto di non dover informare gli interessati coinvolti, l'Autorità, dopo aver valutato la probabilità che le violazioni presentassero un rischio elevato, ha ingiunto ai titolari di provvedervi senza ritardo ai sensi dell'art. 58, par. 2, lett. e), RGPD (cfr. provv.ti 21 marzo 2024, n. 162, doc. web n. 10009836; n. 163, doc. web n. 10009858; n. 164, doc. web n. 10009890; n. 165, doc. web n. 10009874; n. 166, doc. web n. 10009912; n. 167, doc. web n. 10010433; n. 168, doc. web n. 10010449; n. 169, doc. web n. 10010483; n. 170, doc. web n.

10010499; n. 171, doc. web n. 10010521; n. 172, doc. web n. 10010605; n. 173, doc. web n. 10010621; 23 maggio 2024, n. 327, doc. web n. 10037682; 2 novembre 2024, n. 659, doc. web n. 10070521).

Nei casi in cui sono emersi un'inadeguatezza delle misure di sicurezza adottate o il mancato rispetto degli obblighi in materia di violazione dei dati personali da parte del titolare o del responsabile, sono stati adottati provvedimenti correttivi, anche di tipo sanzionatorio. Per maggiori informazioni in merito, si fa rinvio ai parr. 5.4.1 e 5.4.2.

18 Il trasferimento dei dati personali verso paesi terzi

Nel corso del 2024 è stata avviata un'attività volta a verificare il processo di aggiornamento delle norme vincolanti di impresa (BCR), già approvate ai sensi dell'art. 47 del RGPD e rispetto alle quali l'Autorità ha agito in qualità di autorità di controllo capofila (cd. BCR *lead)*.

Tale attività di verifica è stata posta in essere in base a quanto previsto dalla raccomandazione 01/2022 "sulla domanda di approvazione e sugli elementi e sui principi che devono figurare nelle norme vincolanti d'impresa del titolare del trattamento (art. 47 del RGPD)", adottata dal CEPD il 20 giugno 2023 (cfr. Relazione 2023, p. 216).

La citata raccomandazione, infatti, nell'introdurre nuovi requisiti delle BCR nel chiarire il contenuto di quelli già esistenti, ha in particolare stabilito (v. parr. 13 e ss.) che i titolari di BCR approvate in data antecedente alla sua adozione conformino il testo delle predette BCR ai nuovi requisiti entro dicembre 2024, notificando le modifiche all'autorità di controllo capofila.

Il Garante ha inoltre continuato a fornire riscontro alle numerose richieste e ai diversi quesiti pervenuti, concernenti quanto previsto nel Capo V del RGPD. In tale contesto, a seguito della manifestazione di interesse, da parte di un gruppo multinazionale, all'avvio di un procedimento volto all'adozione di BCR, l'Autorità ha fornito alcuni utili chiarimenti in ordine all'ambito di applicazione di tale strumento, invitando il gruppo a valutare con attenzione la natura del trasferimento che sarebbe stato oggetto delle stesse.

All'esito di tale analisi, in ragione dello specifico flusso di dati individuato nel caso di specie dal richiedente – che avrebbe coinvolto in qualità di importatore una sola società affiliata con sede in un paese terzo – il gruppo ha comunicato la decisione di ricorrere alle clausole-tipo di cui all'art. 46, par. 2, lett. c), RGPD come individuate, quali garanzie adeguate ai sensi del Capo V del RGPD, nella decisione di esecuzione UE 2021/914 della Commissione del 4 giugno 2021.

Tale decisione, infatti, reca al proprio interno diverse clausole-tipo di natura contrattuale utilizzabili in base alla tipologia di trasferimento effettivamente posto in essere (da titolare a titolare; da titolare a responsabile; da responsabile a responsabile; da responsabile a titolare). Attraverso la compilazione di uno specifico allegato, è possibile indicare i perimetri dei trasferimenti da porre in essere. Al contempo, le clausole consentono l'adesione da parte di nuove società anche in un momento successivo alla loro sottoscrizione.

19 L'attività ispettiva

19.1. *L'attività ispettiva fra conferme e novità*

L'anno 2024 ha visto la conferma dei positivi risultati che, sul piano numerico, avevano caratterizzato l'attività ispettiva nei dodici mesi precedenti. Infatti, sono state svolte complessivamente 130 attività ispettive: 59 ispezioni sono state effettuate direttamente da personale in servizio presso il Garante, mentre 71 attività sono state delegate al Nucleo *privacy* e frodi tecnologiche della Guardia di finanza.

Queste attività hanno riguardato svariati ambiti di interesse ed hanno seguito, in particolare, le indicazioni di priorità enunciate nelle delibere 29 dicembre 2023, n. 636 (doc. web n. 9981356) e 4 luglio 2024, n. 474 (doc. web n. 10056323) contenenti la programmazione semestrale delle attività ispettive.

Può essere utile, in questa sede, esaminare alcuni dei settori più significativi in relazione ai quali sono state svolte le ispezioni che rappresentano una sorta di "termometro" dei campi di interesse e delle frontiere, anche tecnologiche, verso le quali si concentra e si indirizza l'attività e l'attenzione dell'Autorità.

Naturalmente le indicazioni potranno essere solo generiche per ovvie ragioni di riservatezza, tenendo conto che, per quasi tutte le vicende in questione, le relative istruttorie sono ancora in corso.

- SPID. È proseguito il ciclo di ispezioni finalizzato a verificare la correttezza del procedimento di rilascio e utilizzo dello SPID, con particolare riguardo al profilo della corretta identificazione dei soggetti che intendono usufruirne. Le informazioni e la documentazione, raccolte nell'ambito di questo ciclo ispettivo particolarmente approfondito, hanno consentito di estendere i controlli a tutta la filiera interessata dal procedimento di rilascio, permettendo all'Ufficio di disporre dei necessari elementi conoscitivi per formulare in proposito delle indicazioni specifiche e tecnicamente documentate.

- Impiego di tecnologie innovative. Sono state condotte anche varie ispezioni caratterizzate soprattutto da un intento conoscitivo, volto a mettere il Garante in condizione di valutare la "compatibilità *privacy*" di alcuni dispositivi tecnologicamente avanzati. Tra questi possono essere segnalati i controlli sui dispositivi installati (o sperimentati) presso alcuni comuni ove si registrano consistenti flussi turistici, allo scopo di regolare l'accesso ai centri storici e/o ad altre aree di pregio.

Altri interventi, finalizzati alla verifica della correttezza del trattamento dei dati dei dipendenti, hanno riguardato strumenti di videosorveglianza e controllo dei lavoratori. Infine un'attenzione specifica è stata indirizzata all'installazione di apparecchiature caratterizzate da funzionalità di riconoscimento facciale sperimentate (a scopi sia di elevazione degli standard di sicurezza che di velocizzazione delle operazioni di verifica e transito dei passeggeri) presso alcune società che gestiscono scali aeroportuali aperti al traffico civile.

- Registro elettronico. Una speciale attenzione è stata dedicata ai cd. registri elettronici, ormai capillarmente diffusi presso gli istituti scolastici. In tale ambito, si è avuto particolare riguardo alle molteplici funzionalità a disposizione delle scuole e dei singoli insegnanti, oltre che ai dati personali strettamente connessi allo svolgimento dell'attività didattica ed al monitoraggio del rendimento scolastico.

- Ricerca scientifica e trattamento dei dati in ambito sanitario. Lo sviluppo della sanità elettronica (che ha ricevuto nuovo impulso dopo le esperienze di tipo emergenziale maturate durante il periodo della pandemia da COVID-19) ha comportato la necessità di pianificare adeguate attività di controllo *in loco*.

L'attenzione si è concentrata, in particolare, sulle modalità di redazione e implementazione del cd. *dossier* sanitario.

Diversi accertamenti, volti specificamente a conoscere nuove modalità di acquisizione e trattamento dei dati a fini di ricerca scientifica, hanno riguardato poi alcuni temi di "frontiera" quali le tecniche di pseudonimizzazione e l'utilizzo dei cd. dati sintetici.

- *Data breach.* Negli ultimi anni le violazioni di dati personali comunicate al Garante sono cresciute in misura significativa. Ne è ovviamente derivata la frequente necessità di integrare gli accertamenti tradizionali, svolti attraverso richieste di documenti e interlocuzioni da remoto, con attività ispettive di verifica e controllo svolte *in loco*, così da accedere ai sistemi e agli archivi elettronici dei titolari del trattamento e verificare specificamente la tipologia, la conformazione e il grado di resilienza degli apprestamenti di sicurezza informatica utilizzati.

Molte delle violazioni di questo tipo segnalate all'Autorità hanno riguardato grandi banche dati sia pubbliche che private; le ispezioni condotte hanno, in generale, fatto emergere una debolezza degli apprestamenti volti alla tutela della cybersicurezza, una scarsa efficacia – o addirittura l'assenza – di meccanismi di *alert* ed anche l'insufficienza delle strutture organizzative e tecniche volte a prevenire, intercettare e segnalare queste violazioni.

Numerosi accertamenti sono stati rivolti all'ambito bancario rispetto al quale, a seguito di molte segnalazioni e reclami, è stata confermata la persistente presenza di violazioni interne, addebitabili cioè a dipendenti degli istituti di credito che, in violazione degli obblighi di fedeltà e riservatezza, accedono in modo illegittimo ai dati contabili di clienti e, quasi sempre, li mettono poi a disposizione di terzi non legittimati (familiari non autorizzati, concorrenti commerciali, avvocati e, nei casi più gravi, organizzazioni, anche criminali, interessate alla realizzazione di attività di vero e proprio dossieraggio, anche in chiave ricattatoria).

Le cronache giornalistiche degli ultimi mesi hanno purtroppo fornito molte informazioni in questo senso. Le indagini, anche giudiziarie, in corso hanno dimostrato come a queste informazioni provenienti da soggetti privati si sono spesso aggiunte e intrecciate molte informazioni, parimenti acquisite in modo illecito, presso le più grandi e importanti banche dati pubbliche (*database* dell'Anagrafe tributaria, banche dati dell'INPS e delle forze di polizia, ecc.).

La delicatezza di queste vicende ha indotto il Garante a costituire un'apposita *task force* per meglio evidenziare le problematiche sottese a queste violazioni e proporre le contromisure possibili (cfr. par. 4.9.2).

Ugualmente pericolose sono le violazioni di dati avvenute in ambito sanitario (presso archivi e banche dati di ospedali, laboratori, strutture amministrative socio-sanitarie ecc.); in questi casi, tuttavia, si tratta generalmente di violazioni dovute a soggetti esterni alle strutture colpite. È evidente la particolare delicatezza di queste situazioni, spesso emerse solo al momento dell'invio di messaggi ricattatori da parte degli autori della violazione, a fronte di una frequente e diffusa sottovalutazione da parte delle strutture coinvolte dei rischi connessi a un livello inadeguato di sicurezza informatica.

19.2. *Modalità operative*

Il panorama dei principali ambiti rispetto ai quali si sono svolti gli interventi ispettivi, per quanto parziale e succinto, ha evidenziato la sempre maggiore complessità e delicatezza di queste attività che hanno ormai assunto una costante dimensione interdisciplinare. L'esperienza consueta vede infatti, in sede ispettiva, la contemporanea presenza di almeno tre diverse componenti: il personale del Dipartimento ispettivo che, ai sensi dell'art. 156, comma 7, d.lgs. n. 196/2003 riveste la qualifica di ufficiale di polizia giudiziaria, i funzionari dei dipartimenti giuridici specificamente interessati, per materia, alle problematiche sottese all'ispezione e, infine, i tecnici informatici che assicurano la possibilità di effettuare quegli accessi e quei controlli agli archivi elettronici ed alle banche dati che sono ormai strutturalmente connessi a qualsiasi attività di trattamento.

Sotto questo profilo i controlli effettuati sul campo rappresentano spesso la prima tappa di una complessa analisi tecnica che prosegue presso la sede dell'Autorità e si basa sull'esame attento di documenti, elaborati tecnici, *report* redatti da soggetti incaricati di svolgere *audit* per conto del titolare del trattamento, ecc.

In alcuni casi particolarmente delicati l'esame ha anche riguardato attrezzature informatiche e archivi elettronici fatti oggetto di confisca a seguito di appositi provvedimenti di tipo prescrittivo e sanzionatorio emanati dal Collegio del Garante.

19.3. *La collaborazione con la Guardia di finanza*

È proseguita, nel corso del 2024, la collaborazione istituzionale ormai consolidata con il Corpo della Guardia di finanza sulla base del Protocollo di intesa con il Garante sottoscritto nel 2021. Le decine di interventi delegati all'apposito Nucleo speciale *privacy* e frodi telematiche hanno permesso all'Autorità di moltiplicare la propria presenza sul territorio. Ciò ha consentito di affiancare alle missioni svolte direttamente dal personale dell'Ufficio anche interventi delegati interamente a questo Reparto specializzato.

Si è inoltre intensificata l'attività di scambio con il citato Nucleo attraverso frequenti momenti di incontro e di scambio informativo e formativo. L'obiettivo è infatti quello di migliorare l'osmosi fra Ufficio e Nucleo, diffondendo il più possibile quelle conoscenze specialistiche di carattere giuridico che sono fondamentali per gestire in modo fruttuoso le attività di controllo sul territorio.

20 Il contenzioso giurisdizionale

20.1. *Considerazioni generali*

Tutte le controversie che riguardano l'applicazione della disciplina in materia di protezione dei dati personali devono essere comunicate al Garante, anche se non sono relative all'impugnazione di provvedimenti dell'Autorità (art. 152 del Codice e art. 10, comma 9, d.lgs. n. 150/2011, come modificato dall'art. 17, d.lgs. n. 101/2018).

In relazione a tale incombente informativo, si registra, nel decorso anno una sensibile diminuzione rispetto al 2023: a fronte dei 70 ricorsi nel 2022 e dei 101 del 2023, nel 2024 è stata comunicata all'Autorità la pendenza di 74 ricorsi.

Come rilevato anche negli anni passati, non viene sempre puntualmente adempiuto l'altro obbligo, a carico delle cancellerie, di trasmettere al Garante copia dei provvedimenti emessi dall'Autorità giudiziaria in materia di protezione dati e di criminalità informatica (art. 154, comma 6, del Codice). Tali comunicazioni consentono all'Autorità di avere conoscenza dell'evoluzione della giurisprudenza nazionale in materia di protezione dei dati personali, rappresentando, al contempo, un utile strumento di segnalazione al Parlamento e al Governo degli 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 2024 ha registrato un aumento nella proposizione delle opposizioni a provvedimenti dell'Autorità: 85 a fronte dei 75 ricorsi del 2023.

Nel decorso anno deve altresì essere annotato l'ingresso di 14 ricorsi amministrativi avverso il parere favorevole formulato dal Garante in data 23 maggio 2024 sugli schemi di decreto trasmessi dal Ministero delle infrastrutture e dei trasporti (decreto RENT e decreto FDSE, cfr. par. 4.5).

Nel 2024, inoltre, l'Autorità ha avuto notizia di 92 decisioni dell'Autorità giudiziaria relative ad opposizioni a provvedimenti del Garante, a fronte delle 159 pervenute nel 2023.

In relazione alle pronunzie giurisdizionali sfavorevoli intervenute, si registra la tendenza dei Tribunali di merito, nella maggior parte dei casi, ad accogliere le opposizioni proposte avverso i provvedimenti dell'Autorità sotto il profilo del *quantum debeatur*, ferma restando la conferma nell'*an* della legittimità dell'accertamento delle violazioni in materia di protezione dei dati personali, quale presupposto delle sanzioni irrogate.

Si segnala, altresì, che sono residuali le ipotesi di annullamento integrale dei provvedimenti opposti.

Di seguito si dà conto delle sentenze di maggior rilievo.

Diritto all'oblio e deindicizzazione

Il Tribunale di Gela con sentenza 11 dicembre 2024, n. 50 ha integralmente rigettato il ricorso proposto da due avvocati avverso il provvedimento del Garante 17 luglio 2024, n. 446 (non pubblicato ai sensi dell'art. 24 del reg. del Garante 1° agosto 2013) con il quale l'Autorità aveva archiviato il reclamo dagli stessi proposto, avente ad oggetto la richiesta di rimozione e deindicizzazione di un articolo pubblicato su di un

quotidiano locale, relativo ad un fatto di cronaca giudiziaria riguardante l'attività professionale dei due legali.

Il giudice ha confermato la legittimità del provvedimento opposto ritenendo che nel caso di specie l'annotazione di cui all'art. 64-*ter*, comma 2, disp. att. c.p.p. debba necessariamente operare nei limiti di cui all'art. 17, comma 3, lett. a), RGPD, applicabile alla fattispecie, trattandosi di un fatto di cronaca di interesse pubblico, concreto ed attuale.

Con sentenza 24 settembre 2024, il Tribunale di Napoli ha rigettato il ricorso proposto avverso il provvedimento del Garante 28 settembre 2023, n. 430, doc. web n. 9946736, confermando il principio secondo cui l'art. 64-*ter*, disp. att. c.p.p. non ha innovato il quadro normativo sul diritto all'oblio che, pertanto, continua a costituire un limite alla preclusione dell'indicizzazione, ovvero alla concessione della deindicizzazione. Il giudice ha infatti evidenziato che "La funzione dell'art. 64-*ter* c.p.p. è quella di introdurre una norma processuale che si limita a stabilire un *iter* conseguente ad una sentenza di proscioglimento o di non luogo a procedere ovvero un provvedimento di archiviazione senza introdurre alcun nuovo principio in materia di trattamento dei dati personali".

È stato quindi negato dal Tribunale, in coerenza con la decisione del Garante, il diritto all'oblio dell'interessato in assenza dei presupposti per il suo legittimo esercizio.

Con sentenza 19 febbraio 2024, n. 214, il Tribunale di Como ha respinto l'opposizione proposta da una società avverso il provvedimento 6 luglio 2023, n. 295 (doc. web n. 9926884) con il quale l'Autorità, in accoglimento del reclamo proposto dall'interessato, aveva ordinato la rimozione dai risultati di un motore di ricerca dell'URL associato al suo nominativo e, contestualmente, aveva disposto l'annotazione nel registro interno dell'Autorità, senza valore di precedente, delle misure adottate nei confronti del gestore.

Occorre innanzitutto evidenziare che il giudice ha ritenuto non fondata l'eccezione preliminare concernente il difetto di competenza e/o giurisdizione dell'Autorità, operata dalla società sul presupposto dell'oggetto della domanda di rimozione, asseritamente basata sulla sola tutela dell'onore e della reputazione dell'interessato. Sul punto, il Tribunale ha infatti osservato che il provvedimento impugnato, pur evidenziando profili di illegittimità relativi alla tutela dell'onorabilità delle informazioni contenute sul sito internet, ha enucleato plurime violazioni del RGPD, le quali giustificano la competenza del Garante.

Il giudice ha poi evidenziato che la veridicità delle informazioni riportate sul sito non poteva essere oggetto di valutazione nel giudizio sottoposto al suo esame e che, in ogni caso, la genuinità o meno delle stesse era ininfluente attesa la motivazione posta dal Garante – e dallo stesso giudice condivisa – a fondamento dell'accoglimento del reclamo, nella parte in cui l'Autorità aveva riconosciuto il mancato rispetto del RGPD per non contenere il sito alcun riferimento né all'informativa sull'utilizzo dei dati personali né al titolare del trattamento, oltreché nella parte in cui aveva ritenuto non sussistente alcun legittimo motivo prevalente per procedere al trattamento dei dati personali dell'interessato rispetto al suo diritto all'oblio.

La Corte di cassazione con ordinanza 21 febbraio 2024, n. 4648 ha cassato la sentenza del Tribunale di Padova 31 marzo 2023, n. 649 accogliendo il ricorso proposto dal Garante con il quale era stata lamentata la violazione e/o falsa applicazione da parte del giudice di prime cure dell'art. 4 del RGPD, laddove aveva ritenuto che la targa automobilistica non costituisse un dato personale.

La Corte di legittimità, nel richiamare la propria pregressa giurisprudenza, ha ribadito quindi che "la targa automobilistica è un dato che consente la identificazione diretta del proprietario" specificando che ciò che assume rilievo decisivo in materia di protezione dei dati personali è "il collegamento funzionale, ai fini identificativi, tra i dati personali

20

e la persona fisica, in presenza di condotte astrattamente riconducibili nell'alveo del trattamento".

Nello stesso senso va segnalata l'ordinanza della Corte di cassazione 11 aprile 2024, n. 9880 confermativa della sentenza del Tribunale di Roma 15 novembre 2022, n. 17028, con la quale era stata rigettata l'opposizione proposta da una società avverso l'ordinanza-ingiunzione 22 luglio 2021, n. 293 (doc. web n. 9698597), adottata dal Garante a fronte dell'accertata illiceità del trattamento dei dati personali raccolti attraverso i nuovi parcometri installati sul territorio del Comune di Roma, i cd. parcometri evoluti, i quali registrano targa, localizzazione del veicolo ed orario della sosta.

La Corte di legittimità, sposando la linea difensiva prospettata dall'Autorità, ha confermato la legittimità della sanzione irrogata sia nell'*an* che nel *quantum*. In particolare, la Corte, dando continuità al proprio orientamento, ha ribadito che la targa di un autoveicolo ha natura di dato personale; ha altresì rilevato che l'assenza di nomina del responsabile del trattamento da parte del Comune di Roma (nella specie, titolare del trattamento) non pregiudica la responsabilità della società per l'inosservanza dei doveri di comportamento già accertati, essendo pacifico che la stessa, a prescindere dall'esistenza o meno di detta nomina, abbia agito in qualità di responsabile *ex* art. 28 del RGPD. Invero, il combinato disposto degli artt. 24 e 28 del RGPD, oltreché il principio dell'*accountability* di cui all'art. 5, par. 2, RGPD, impongono al titolare e al responsabile di comprovare l'adozione di misure tecniche ed organizzative adeguate ad assicurare che il trattamento sia effettuato in conformità alla normativa di riferimento, a garanzia della tutela dei diritti e della libertà dell'interessato.

Termini di conclusione del procedimento amministrativo (*ante* 2018)

Il Tribunale di Milano con sentenza 29 aprile 2024 n. 2201 ha parzialmente rigettato l'opposizione proposta da una ricorrente avverso il provvedimento sanzionatorio emesso dal Garante in data 22 maggio 2018, n. 330 (doc. web n. 9018431), per la complessiva somma di euro 600.000,00.

In particolare, il Tribunale, pur avendo ridotto la sanzione irrogata all'importo di euro 450.000,00 – ritenendo che, in coerenza con quanto facoltizzato dall'art. 146-*bis*, comma 4, del Codice, avesse portata deterrente e fosse adeguato al fatto commesso l'aumento del solo triplo – ha integralmente rigettato l'eccezione di nullità del provvedimento impugnato formulata dalla ricorrente per l'eccessiva e, comunque, ingiustificata durata del procedimento.

A tale ultimo riguardo, il Tribunale, rilevato che in ossequio al principio del *tempus regit actum* si applicavano le regole procedimentali delineate dalla l. n. 689/1981 – come espressamente richiamata dall'art. 166, d.lgs. n. 196/2003, nella versione *ratione temporis* applicabile – ha sostenuto, in conformità con quanto espresso dalle Sezioni Unite della Suprema Corte di cassazione con la sentenza n. 9591/2006, che il termine di conclusione del procedimento di adozione delle sanzioni amministrative non può essere stabilito sommando i termini di fase prescritti dagli artt. 14 e 18 della l. n. 689/1981 in quanto "in tal modo verrebbe operata un'arbitraria manipolazione della norma, la quale considera unitariamente il procedimento amministrativo e dispone che il termine per la sua conclusione decorre non dall'esaurimento di ognuno dei vari segmenti che eventualmente lo compongono, bensì dall'inizio di ufficio del procedimento o dal ricevimento della domanda se il procedimento è ad iniziativa di parte". Pertanto, alla luce del quadro normativo vigente al momento dell'adozione del provvedimento impugnato, il Tribunale ha concluso per l'inesistenza di alcuna specifica regola relativa al termine di conclusione del procedimento idonea ad inficiare la legittimità della sanzione irrogata, non potendo neppure essere invocato il principio costituzionale di buon andamento di cui all'art. 97 Cost., a sostegno dell'asserita illegittimità, trattandosi di un principio generale dal quale non è possibile desumere in modo preciso e

determinato il termine di conclusione del procedimento amministrativo.

Con ordinanza della II sez. civile 19 luglio 2024 n. 19951, la Suprema Corte di cassazione, in accoglimento del ricorso proposto dal Garante, ha cassato la sentenza del Tribunale di Parma 24 giugno 2020, n. 575 con rinvio al medesimo ufficio giudiziario, in diversa composizione.

Il giudizio era stato originato dal ricorso proposto da un comune avverso l'ordinanza-ingiunzione 25 giugno 2015 (doc. web n. 4242968), con la quale il Garante aveva intimato il pagamento di euro 4.000,00 a titolo di sanzione pecuniaria per avere l'amministrazione comunale pubblicato sul proprio sito istituzionale l'esito della valutazione preselettiva di una procedura concorsuale pubblica, giusta determinazione del 9 febbraio 2012, contenente i dati personali dei candidati non ammessi e le ragioni dell'esclusione.

Nell'accogliere il primo motivo di ricorso, la Corte di legittimità ha rilevato che in tema di procedure concorsuali pubbliche viene in rilievo la necessità di operare il giusto bilanciamento tra opposti interessi: da un lato, quello alla pubblicità della procedura e di tutti i suoi atti, inclusi quelli relativi alla fase preselettiva e, dall'altro, l'interesse dei candidati di non vedere divulgate le informazioni attinenti alla loro persona, se non per quanto strettamente necessario ai fini dell'assicurazione della regola di trasparenza della procedura selettiva. In tale ottica di bilanciamento, la Suprema Corte ha ritenuto che nel caso di specie l'amministrazione comunale avrebbe potuto diffondere sul proprio sito istituzionale esclusivamente l'esito della valutazione preselettiva del concorso, ma non anche la motivazione di detta esclusione, la quale riferendosi ad un dato personale del candidato "avrebbe dovuto essere resa accessibile ai soli diretti interessati, e dunque al candidato escluso ed agli altri partecipanti alla selezione, mediante opportune procedure di autenticazione".

Telemarketing

Il Tribunale di Roma con sentenza 23 settembre 2024, n. 14407 ha respinto il ricorso proposto da una società avverso il provvedimento del Garante 12 ottobre 2023, n. 479 (doc. web n. 9949453), con il quale l'Autorità aveva irrogato la sanzione pecuniaria pari a euro 70.000,00 per avere la società acquisito numerazioni telefoniche in assenza di un adeguato consenso al trattamento dei dati per finalità di *marketing*.

In particolare, il Tribunale, in armonia con i provvedimenti del Garante in materia, ha ritenuto sussistenti nel caso di specie le violazioni contestate alla società con l'ordinanza opposta, essendo pacifico che la stessa avesse svolto attività di *marketing* omettendo di consultare il registro pubblico delle opposizioni, avvalendosi, tra l'altro, di dati forniti da soggetti terzi in assenza di preventiva verifica delle modalità di acquisizione di tali dati.

Il Tribunale di Milano con sentenza 9 settembre 2024, n. 7946 ha rigettato il ricorso proposto da una società immobiliare avverso il provvedimento del Garante 16 settembre 2021, n. 316 (doc. web n. 9705632), confermando l'illegittimo utilizzo da parte della società di dati reperibili su un profilo LinkedIn per finalità promozionali. In particolare, il giudice, in conformità con un ormai consolidato indirizzo giurisprudenziale, ha ribadito che "il carattere pubblico dei dati non rende lecito un loro indiscriminato utilizzo, poiché la pubblicità o conoscibilità al pubblico nella maggior parte dei casi è finalizzata a soddisfare esigenze differenti da quelle commerciali o promozionali".

Il Tribunale di Firenze con ordinanza 4 aprile 2024 ha integralmente rigettato il ricorso proposto avverso il provv. 13 aprile 2023, n. 184 (doc. web n. 9893718), con il quale il Garante aveva sanzionato una società per avere la stessa svolto attività promozionale violando in maniera grave e reiterata le disposizioni in materia di protezione dei dati, tanto da richiedere anche la confisca del *database* contenente i dati personali degli utenti acquisiti illecitamente.

20

Nel ritenere pienamente validi il provvedimento e la misura della confisca, il Tribunale ha ritenuto che la sanzione comminata ai sensi dell'art. 83, parr. 3 e 5, RGPD (pagamento di una somma fino a euro 20.000.000,00) fosse pienamente proporzionata e attesa la sussistenza di tutte le circostanze aggravanti ed attenuanti prese in considerazione dal Garante, confermando la discrezionalità dell'Autorità di controllo entro la forbice prevista dalla legge.

Ha altresì accertato la legittimità del provvedimento della confisca, rilevando, al riguardo, che "la sanzione della confisca è funzionale a sottrarre alle società coinvolte un consistente patrimonio informativo acquisito illecitamente, impedendo riutilizzi illeciti anche da parte di terzi. Non possono applicarsi ai provvedimenti del Garante che dispongono sanzioni accessorie, in particolare quella della confisca, né l'art. 20, comma 2, l. n. 689/1981 ("Le sanzioni amministrative accessorie non sono applicabili fino a che è pendente il giudizio di opposizione contro il provvedimento di condanna") poiché tale disposizione attiene ad ipotesi di sanzioni accessorie amministrative applicate nell'ambito di un procedimento penale, né l'art. 18, comma 7, della medesima legge, poiché da una lettura sistematica di tale articolo deriva che la confisca ivi prevista sia quella relativa alle cose oggetto di precedente sequestro (come indicato nell'art. 18, comma 3), ai sensi dell'art. 13, comma 2, l. n. 689/1981. Tale ultima disposizione (art. 13) è stata espressamente esclusa dal novero di quelle applicabili nei procedimenti innanzi al Garante (art. 166, comma 7, del Codice)".

Anonimizzazione dei dati sulla salute

Con sentenza 13 maggio 2024, n. 5018 il Tribunale di Milano ha rigettato l'opposizione proposta da una società avverso l'ordinanza-ingiunzione 1° giugno 2023, n. 226 (doc. web n. 9913795), con la quale il Garante aveva irrogato una sanzione pecuniaria pari a euro 15.000,00 oltreché la sanzione accessoria della pubblicazione del provvedimento sul proprio sito web, contestando talune criticità del progetto fornito dalla medesima azienda sotto il profilo delle tecniche di anonimizzazione dei dati relativi alla salute, con particolare riferimento all'inadeguata manifestazione del consenso al trattamento da parte dell'interessato.

Il Tribunale, tornato a pronunziarsi in punto di anonimizzazione, ha ribadito che anche il trattamento che conduce all'anonimizzazione presenta un fattore di rischio intrinseco residuo di re-identificazione, quale che sia la misura tecnico-organizzativa adottata per rendere "anonimi" i dati, e che tale rischio, probabilmente ineliminabile, è destinato ad aumentare nel tempo in correlazione con lo sviluppo della tecnologia. Partendo da tale premessa, il giudice ha quindi confermato il provvedimento impugnato ritenendo indispensabile anche con riguardo ai dati trattati in modo anonimo il consenso esplicito dell'interessato, "non essendo sufficiente, al predetto fine, che tale consenso avvenga sulla base del mancato diniego".

Legittimazione processuale

Il Tribunale di Arezzo con sentenza 17 luglio 2024, n. 671 ha dichiarato inammissibile il ricorso proposto da una persona fisica avverso il provvedimento del Garante 1° giugno 2023, n. 227 (doc. web n. 9917728), conclusivo di un procedimento attivato dall'Autorità a seguito del reclamo proposto dallo stesso ricorrente.

L'interessato, da un lato, aveva contestato la carenza dell'attività istruttoria compiuta dal Garante per essersi questo limitato ad accertare la sussistenza dell'illecito solo in relazione ad uno dei profili reclamati e avendo, tra l'altro, trascurato il coinvolgimento e la responsabilità di soggetti terzi, diversi dal titolare e, dall'altro, aveva rivendicato il suo diritto al risarcimento del danno patito in conseguenza dell'attività illecita posta in essere dall'AUSL e dal terzo.

Il Tribunale, in accoglimento delle eccezioni formulate dal Garante, ha dichiarato inammissibile l'impugnazione del provvedimento opposto ritenendo il rapporto sanzionatorio intercorrente esclusivamente tra l'autorità amministrativa ed il trasgressore,

il solo legittimato a contestare la sanzione irrogata.

Il giudice ha altresì rigettato la domanda risarcitoria formulata in ricorso per difetto di allegazione e prova del danno asseritamente patito, richiamando, al riguardo, il consolidato orientamento della giurisprudenza di legittimità, a mente del quale alla lesione della *privacy* – seppur nella sua veste di diritto fondamentale tutelato dagli artt. 2 e 21 della Carta fondamentale e dall'art. 8 della CEDU – non consegue l'automatica risarcibilità dell'illecito aquiliano "dovendo il pregiudizio morale o patrimoniale essere comunque provato secondo le regole ordinarie, quale ne sia l'entità ed a prescindere anche dalla difficoltà della relativa prova".

Registrazioni di conversazioni private

La Corte di cassazione con ordinanza 16 settembre 2024, n. 24797 ha cassato la sentenza del Tribunale di Venezia 2 dicembre 2021, n. 2286 rigettando nel merito il ricorso originariamente proposto da alcuni dirigenti di una società avverso il provvedimento del Garante 17 giugno 2019, con il quale l'Autorità aveva disposto l'archiviazione del reclamo dagli stessi proposto. Gli originari reclamanti avevano chiesto al Garante di disporre la cancellazione e/o distruzione di un *file* audio contenente una conversazione registrata da un dipendente della società nel contesto di una riunione indetta dalla dirigenza (*file* audio poi ceduto dall'autore ad altri colleghi per la sua produzione in un giudizio di lavoro).

La Corte di legittimità, accertata l'ammissibilità del ricorso incidentale adesivo tardivamente proposto dal Garante sul presupposto che la sua legittimazione processuale "non si riconnette ai diritti disponibili delle parti private, ma ai pubblici interessi che vengono in rilievo nella fattispecie", ha ritenuto che la liceità del trattamento (nella specie, la registrazione della riunione) dovesse essere valutata in ragione dell'uso concretamente fattone, concludendo, quindi, per la legittimità dell'utilizzazione del *file* audio ai fini processuali atteso che "l'utilizzazione dei dati pur senza il consenso dell'interessato è ritenuta lecita quando si tratti di difendere un diritto fondamentale e inoltre, quando i dati siano stati utilizzati in giudizio, come nella specie, è il giudice di quel giudizio a dover bilanciare gli interessi in gioco ed ammettere o meno le prove che comportano il trattamento di dati di terzi, posto che la titolarità del trattamento spetta in questo caso all'autorità giudiziaria e in tal sede vanno composte le diverse esigenze, rispettivamente, di tutela della riservatezza e di corretta esecuzione del processo".

Oscuramento dati nei provvedimenti del Garante

Con sentenza 4 settembre 2024 il Tribunale di Bologna ha respinto il reclamo presentato da una società *ex* art. 669-*terdecies* c.p.c. avverso l'ordinanza 16 luglio 2024 emessa dallo stesso Tribunale a definizione di un procedimento *ex* art. 700 c.p.c., incardinato dalla medesima società al fine di ottenere l'oscuramento di ogni riferimento alla denominazione di *software* e dispositivi da essa prodotti, come contenuti in taluni provvedimenti sanzionatori contro terzi (doc. web n. 9995680, n. 9995701, n. 9995741, n. 9995762 e n. 9995785).

Il Tribunale, in composizione collegiale, nel confermare la decisione del primo giudice ha definitivamente respinto il ricorso cautelare ritenendo che i provvedimenti dell'Autorità non facessero trapelare alcun dubbio circa la liceità dei prodotti, riguardando i riferimenti agli stessi esclusivamente l'utilizzo improprio che ne avevano fatto i titolari multati in punto di violazione della disciplina in materia di protezione dei dati personali: "la lettura dei provvedimenti del Garante con la normale attenzione esigibile da un utente medio esclude qualsivoglia possibile fraintendimento in merito all'oggetto effettivo della violazione accertata e sanzionata, che non è – come detto – il software o il dispositivo riconducibile al "fornitore" (…) ma l'utilizzo che terzi hanno fatto di tali prodotti in violazione delle disposizioni poste in materia di protezione dei dati personali. I provvedimenti del Garante, che contengono la

menzione dei *software* e degli applicativi di cui si controverte anche in adempimento di un dovere istituzionale di informativa corretta e completa, sono privi di possibili equivoci in merito a ciò che è stato effettivamente ritenuto contrario alle disposizioni in materia di *privacy*".

20

Ricorsi avverso cartelle esattoriali

Con sentenza 11 novembre 2024, n. 28920, la Corte di cassazione, in armonia con il consolidato indirizzo giurisprudenziale di legittimità, rammentato che l'art. 18 del d.lgs. n. 101/2018, attuativo del RGPD, ha introdotto un meccanismo di definizione agevolata delle violazioni ancora non definite con ordinanza ingiunzione alla data di applicazione del RGPD medesimo, ha ribadito che in assenza di detta definizione, ovvero in assenza di nuove memorie difensive, il verbale di contestazione, già notificato, si converte *ex lege* in ordinanza-ingiunzione, la quale non necessita di ulteriore notificazione, sicché il *dies a quo* del termine per la proposizione dell'opposizione, del d.lgs. n. 150/ 2011, *ex* art. 10, comma 3, avverso la cartella di pagamento successivamente notificata al trasgressore va individuato non già nella data di sua notificazione, bensì nell'ultimo momento utile per produrre le memorie suddette ai sensi del comma 4 del medesimo articolo, né il destinatario della prima può avvalersi della opposizione cd. recuperatoria.

Altra casistica

Con sentenza 10 dicembre 2024, n. 6696 il Tribunale di Milano ha parzialmente rigettato l'opposizione proposta da due società avverso, rispettivamente, le ordinanze-ingiunzione 1° marzo 2018, n. 128 (doc. web n. 9026802) e 8 marzo 2018, n. 144 (doc. web n. 9072702), adottate dall'Autorità a seguito dell'omesso riscontro da parte delle medesime – destinatarie del provv. 25 febbraio 2016, n. 83 – alla richiesta di informazioni *ex* art. 157 del previgente Codice.

In particolare, il Tribunale, pur riducendo le sanzioni portate dai provvedimenti opposti, ha confermato la legittimità delle ordinanze impugnate ritenendo che l'omesso riscontro delle società alle richieste di informazioni formulate *ex* art. 157 del Codice costituisse fattispecie dell'illecito omissivo proprio prevista dall'art. 164 del Codice, illecito che permane anche nel caso in cui, come nella fattispecie in esame, il provvedimento prescrittivo presupposto (provv. 25 febbraio 2016, n. 83, doc. web n. 4881581) sia stato annullato.

Parimenti, il Tribunale ha ritenuto infondata l'eccezione di nullità delle ordinanze-ingiunzione per difetto di motivazione delle stesse, aderendo, a tal riguardo, alla consolidata giurisprudenza della Suprema Corte di cassazione a mente della quale "l'ordinanza-ingiunzione irrogativa di una sanzione amministrativa non deve avere una motivazione analitica e dettagliata come quella di un provvedimento giudiziario, essendo sufficiente che sia dotata di una motivazione succinta, purché dia conto delle ragioni di fatto della decisione (che possono anche essere desunte "*per relationem*" dall'atto di contestazione) ed evidenzi l'avvenuto esame degli eventuali rilievi difensivi formulati dal ricorrente".

Il giudice ha rigettato anche il terzo motivo di opposizione concernente l'errata applicazione da parte del Garante, nella fase di conclusione del procedimento, dell'art. 157 del Codice, rilevando che la citata disposizione codicistica – in coerenza con il testo dell'art. 16, comma 2, del reg. del Garante n. 1/2007 – non prevede alcuna limitazione temporale al potere dell'Autorità di richiedere informazioni.

Con sentenza 30 ottobre 2024, n. 1024, il Tribunale di Viterbo ha rigettato il ricorso proposto da una persona fisica avverso il provvedimento con il quale l'Autorità non aveva ravvisato un illegittimo trattamento di dati personali da parte di una banca per avere la stessa comunicato all'organo di vigilanza, in adempimento alle disposizioni in materia di antiriciclaggio – e, quindi, in conformità alla normativa vigente al momento dei fatti (d.lgs. n. 231/2007) – i dati identificativi del ricorrente. In

particolare, il Tribunale ha osservato che nel contratto fiduciario stipulato dal cliente con l'istituto di credito era presente: "l'informativa sul trattamento dei dati personali nella quale è espressamente previsto, tra le "finalità del trattamento dei dati" al par. 2, lett. b) "finalità connesse agli obblighi previsti da leggi, da regolamenti e dalla normativa comunitaria nonché da disposizioni impartite da autorità a ciò legittimate dalla legge e da organi di vigilanza e controllo (es. antiriciclaggio, monitoraggio valutario ecc.)".

Il Tribunale di Milano con sentenza n. 2201, pubblicata il 29 aprile 2024, ha accolto l'opposizione proposta da una società avverso il provvedimento del Garante 23 febbraio 2023, n. 54, doc. web n. 9873031, con il quale era stato disposto il divieto di ulteriore trattamento di immagini relative a soggetti coinvolti in una vicenda di cronaca e adottata la misura dell'ammonimento per l'inosservanza delle disposizioni previste in materia di trattamento dei dati personali in ambito giornalistico

In particolare, il Tribunale ha annullato il provvedimento opposto ritenendo che la diffusione delle immagini contestate non integrasse la violazione dell'art. 8 delle regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica, doc. web n. 9067692, non essendo le stesse fotografie "intrinsecamente lesive della dignità degli effigiati" e non ritraenti soggetti in "stato di detenzione" e, quindi, non riconducibili alla categoria delle foto segnaletiche.

Il Tribunale, altresì, ha ritenuto conforme alla disciplina in materia di protezione dei dati personali il trattamento delle immagini contestate, atteso che lo stesso soddisfaceva la condizione di essenzialità dell'informazione rispetto a fatti di interesse pubblico per finalità giornalistiche: "Il trattamento per finalità di cronaca giudiziaria avente ad oggetto la pubblicazione delle immagini in questione, dunque, deve ritenersi strumentale all'esercizio del diritto di cronaca giudiziaria ed essenziale per consentire l'identificazione dei soggetti indagati per gravi delitti e, pertanto, sorretto da idonea base giuridica.".

Pende avverso tale decisione giudizio innanzi alla Suprema Corte di cassazione.

20.3. *Il contributo del Garante nei giudizi in materia di protezione dati*

Conformemente alle comunicazioni fornite dall'Autorità giudiziaria al Garante secondo quanto previsto dalla normativa specifica (art. 10, comma 9, d.lgs. 1° settembre 2011, n. 150, come modificato dall'art. 17 del d.lgs. n. 101/2018 – cfr. par. 20.1) e in linea con gli indirizzi giurisprudenziali al riguardo, anche nel 2024 il Garante ha fornito contributi in giudizi diversi da quelli direttamente attinenti a pronunce dell'Autorità ove ha ritenuto sussistente la necessità di difendere o comunque far valere particolari questioni di diritto.

Al riguardo si consideri che la notifica al Garante dei ricorsi in materia di protezione dei dati personali che non attengono a provvedimenti dell'Autorità amplia la casistica di possibile intervento, anche in relazione a questioni di legittimità costituzionale o di compatibilità europea di leggi, e 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.

In tal senso si segnala il caso comunicato dal Tribunale di Bolzano relativo alla pendenza di un giudizio instaurato da un titolare di alcuni conti correnti presso un istituto bancario al fine di ottenere "i nominativi dei dipendenti, del personale e degli operatori della banca che hanno effettuato gli accessi e le interrogazioni dirette sui conti correnti nel periodo intercorrente tra la data del 31 ottobre 2017 e sino alla data del deposito del presente ricorso, con l'indicazione dell'ambito in cui ciascuno di essi

20

è inserito nell'organizzazione della banca e della mansione specifica che giustifica, in capo allo stesso, il trattamento dei dati del cliente, ed altresì delle causali, giustificazioni e finalità dei singoli accessi".

All'esito di una complessa istruttoria l'Autorità ha trasmesso al giudice un articolato parere in approfondimento della delicata questione. In particolare, richiamando la Corte di giustizia europea, prima sez., sent. 22 giugno 2023 in causa C-579/2021, ha rappresentato al giudice che anche ove la comunicazione all'interessato delle informazioni relative all'identità dei dipendenti del titolare del trattamento fosse indispensabile all'interessato stesso per verificare la liceità del trattamento dei suoi dati personali, essa sarebbe tuttavia tale da ledere i diritti e le libertà di tali dipendenti. Pertanto, in caso di conflitto tra, da un lato, l'esercizio di un diritto di accesso che assicura l'effetto utile dei diritti riconosciuti dal RGPD all'interessato e, dall'altro, i diritti o le libertà altrui, occorre effettuare un bilanciamento tra i diritti e le libertà in questione che, pur tenendo conto dei diritti e delle libertà altrui, non dovrà necessariamente condurre a un diniego a fornire all'interessato tutte le informazioni. In caso di omesso o insoddisfacente riscontro da parte del titolare, l'interessato potrà ottenere tutela amministrativa o giurisdizionale.

L'Autorità ha comunque seguito con attenzione tutti i contenziosi nei quali non ha ritenuto opportuno intervenire, chiedendo alle avvocature distrettuali dello Stato di essere informata sull'evoluzione delle vicende processuali e di ricevere comunicazione in merito agli esiti.

21 Le relazioni comunitarie e internazionali

L'attività del Garante nel 2024 è stata contrassegnata da un notevole incremento sia degli impegni europei, sia di quelli internazionali, nei numerosi tavoli e gruppi di lavoro di cui l'Autorità è parte attiva.

Nel corso dell'anno si sono registrati, infatti, a livello UE, l'intensificazione delle attività del CEPD – che riunisce le autorità dell'Unione europea, dei tre paesi appartenenti allo SEE e il GEPD – e, in parallelo, sul piano internazionale, un considerevole aumento delle attività dei diversi *forum* sovranazionali a cui il Garante partecipa, culminato nell'assunzione da parte dell'Italia della presidenza del G7.

In ambito UE, il CEPD ha adottato il proprio progetto di strategia per il periodo 2024-2027 che si fonda su quattro pilastri principali: a) il miglioramento e la promozione di un'applicazione del RGPD il più possibile armonizzata, anche attraverso l'elaborazione di linee guida su aspetti rilevanti della protezione dei dati; b) il rafforzamento di una cultura comune dell'attività di *enforcement* e di una cooperazione efficace tra le autorità di supervisione; c) la salvaguardia della protezione dei dati nel panorama normativo dello spazio digitale, sempre più variegato e interdisciplinare, e la necessità di garantire efficaci forme di cooperazione tra le autorità competenti nei diversi ambiti di riferimento; d) il rafforzamento del dialogo sulla protezione dei dati nella scena globale ed in particolare nelle comunità internazionali di cui il CEPD è parte.

Sempre con riferimento ai lavori del CEPD, un tratto che ha caratterizzato il 2024 è stato il notevole impegno profuso nell'elaborazione dei pareri ai sensi dell'art. 64, par. 2, RGPD.

In base a specifiche richieste provenienti da una o più autorità di protezione dei dati su questioni di applicazione generale o che producono effetti in più di uno Stato membro, il Comitato ha infatti adottato cinque pareri, nella stringente tempistica dettata dall'art. 64, par. 3, RGPD, su temi particolarmente rilevanti e complessi, quali la nozione di stabilimento principale, i requisiti del consenso nei modelli di *business* basati sul cd. *consent or pay,* il riconoscimento facciale negli aeroporti, gli obblighi dei titolari che derivano dalla designazione di responsabili e sub-responsabili e l'IA.

Al notevole incremento del lavoro per rispondere alle richieste di parere secondo l'art. 64, par. 2, RGPD, è corrisposto invece un cambio di tendenza, rispetto al passato, con riferimento alle procedure di risoluzione delle controversie di cui all'art. 65 del RGPD, mai attivate nel corso dell'anno.

In ambito internazionale, il Garante ha svolto un ruolo particolarmente attivo ospitando a Roma, il 9-11 ottobre 2024, il vertice delle autorità di protezione dei dati dei paesi del G7. La cd. *Rome Roundtable* ha visto riuniti il Collegio del Garante italiano, le Autorità competenti di Canada, Francia, Germania, Giappone, Regno Unito e Stati Uniti d'America, insieme al CEPD e al GEPD, con l'obiettivo di definire una proposta comune su diversi temi legati alla protezione dei dati, in particolare con riferimento alle strategie per garantire una sicura e responsabile circolazione dei dati personali; per armonizzare le tecnologie emergenti e l'intelligenza artificiale con i diritti e le libertà delle persone; per promuovere una più stretta ed efficace azione di controllo sull'applicazione della normativa in materia di protezione dei dati (cfr. cap. 24).

21

Riguardo alle tematiche che hanno particolarmente caratterizzato l'attività europea e internazionale del Garante, anche il 2024 è stato contrassegnato dal significativo ruolo assunto dall'IA nei diversi settori e dall'emersione di soluzioni normative alle molte sfide per i diritti delle persone sollevate dall'IA: non solamente, a livello UE, è stato adottato l'AI *Act*, che rappresenta il primo regolamento europeo volto a stabilire regole armonizzate sull'IA, ma anche, sul piano internazionale, nell'ambito del Consiglio d'Europa, è stata portata a compimento e aperta alla firma delle Parti la "Convenzione-quadro in materia di intelligenza artificiale, diritti umani, democrazia e stato di diritto", destinata a divenire, una volta entrata in vigore, il primo trattato internazionale legalmente vincolante in questo campo.

Nella riflessione sull'applicazione dei principi di protezione dei dati nel settore dell'IA, una delle questioni più significative ha riguardato il tema della *governance* e del ruolo cruciale giocato dalle autorità di protezione dati in tale settore, ruolo affermato sia dalla dichiarazione 3/2024 adottata dal CEPD il 16 luglio che dalla dichiarazione delle autorità del G7 adottata a Roma l'11 ottobre 2024 (cfr. cap. 16).

L'interazione tra protezione dei dati, diritto della concorrenza e tutela dei consumatori ha continuato a essere un'altra tematica centrale dell'attività delle autorità di protezione dei dati, specie a livello UE, a fronte, da un lato, della proliferazione di normative volte a regolamentare lo spazio digitale europeo e, dall'altro, della necessità di addivenire a forme di cooperazione tra le diverse autorità competenti delineate da tali norme.

Relazione della Commissione europea sull'applicazione del RGPD

In questo contesto, assume particolare rilevanza la seconda relazione sull'applicazione del RGPD, adottata dalla Commissione europea il 25 luglio 2024 ai sensi dell'art. 97 RGPD. Nel documento, la Commissione ha sottolineato come, nonostante le numerose sfide determinate anche da un incessante sviluppo della tecnologia, l'applicazione del regolamento abbia consentito alle persone di ottenere un maggiore controllo sui propri dati e alle imprese di operare in condizioni maggiormente paritarie, oltre a costituire una pietra angolare per la transizione digitale dell'UE, contribuendo all'emersione di elevati *standard* internazionali in materia di protezione dei dati. La relazione, che fotografa lo stato di avanzamento dell'applicazione del RGPD, auspica la tempestiva adozione del regolamento sulle regole procedurali aggiuntive relative all'applicazione del RGPD, e fornisce indicazioni ai diversi attori coinvolti, in particolare le autorità di protezione dei dati, il CEPD, gli Stati membri e i co-legislatori UE, affinché sia favorito il completamento del quadro normativo in materia di protezione dei dati, sia supportato il dialogo con titolari e responsabili per favorire l'applicazione delle norme, e siano sviluppati meccanismi per il trasferimento dei dati e per favorire la cooperazione internazionale.

21.1. *La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dei dati*

Nel corso del 2024 la plenaria del CEPD si è riunita dodici volte, delle quali cinque in presenza. Più di centottanta sono state le riunioni dei sottogruppi e delle *task force* che si occupano dell'applicazione del RGPD e della direttiva *law enforcement* nei diversi settori.

Dichiarazione del CEPD sulla relazione della Commissione

Nella dichiarazione adottata il 3 dicembre 2024, in risposta alla relazione della Commissione, il CEPD ha messo in evidenza la necessità che nell'ambito normativo UE dedicato allo spazio digitale, contrassegnato da molteplici e complesse regolamentazioni, siano garantite certezza giuridica e coerenza con il RGPD. È in questo contesto, peraltro, che si colloca l'attività in corso del Comitato volta a fornire chiarimenti attraverso specifiche linee guida sull'interazione tra il Regolamento sulla protezione dei

dati e altri testi normativi, in particolare l'AI *Act*, la strategia digitale dell'UE e il pacchetto sui servizi digitali. Nella dichiarazione, il Comitato ha altresì annunciato l'intenzione di procedere con l'elaborazione di contenuti per facilitare l'applicazione del RGPD da parte di soggetti non esperti e di piccole e medie imprese, nonché sottolineato la necessità che il lavoro delle autorità di protezione dei dati e dello stesso CEPD, a fronte delle crescenti sfide che richiedono sempre nuove competenze, sia supportato da adeguate risorse.

Anche in linea con la strategia del Comitato e le indicazioni della suddetta relazione della Commissione, il CEPD ha proseguito l'attività interpretativa di concetti-chiave del RGPD. Il Comitato, infatti, attraverso linee guida su aspetti particolarmente rilevanti del RGPD, fornisce indicazioni utili, specie per i titolari e responsabili del trattamento, per agevolare, anche attraverso esempi pratici, l'applicazione della normativa.

Linee guida in materia di legittimo interesse

In tale contesto, è stato portato a termine l'impegnativo lavoro di redazione delle linee guida in materia di legittimo interesse, adottate nel corso della plenaria dell'8 ottobre e poi sottoposte a consultazione pubblica (conclusasi il 24 novembre), al termine della quale il Comitato elaborerà la versione definitiva del documento, prevista per il 2025.

Le linee guida, che intendono fornire chiarimenti sull'interpretazione e sull'impiego del legittimo interesse come base giuridica dei trattamenti ai sensi dell'art. 6, par. 1, lett. f), RGPD, hanno rappresentato una delle priorità del CEPD e la loro importanza strategica e l'urgenza della loro adozione sono state sottolineate anche dalla citata relazione della Commissione europea sull'applicazione del RGPD.

Le linee guida sono suddivise in quattro parti: 1) una parte introduttiva, che sottolinea, tra l'altro, come il legittimo interesse non debba essere considerato come la base giuridica di cui avvalersi in mancanza di altre basi giuridiche, necessitando invece di un'accurata valutazione circa la possibilità di ricorrervi; 2) un'analisi degli elementi di cui i titolari del trattamento devono tener conto nel valutare se avvalersi dell'art. 6, par. 1, lett. f), RGPD, focalizzata sulle tre componenti sequenziali di tale valutazione (esistenza del legittimo interesse, necessità del trattamento per perseguire tale interesse, bilanciamento dei diritti in gioco); 3) l'illustrazione del rapporto tra l'art. 6, par. 1, lett. f) e i diversi diritti dell'interessato; 4) una descrizione di alcuni contesti specifici in cui tale base giuridica potrebbe essere invocata, in particolare nel caso di trattamento di dati personali relativi a minori, per scopi di *marketing* diretto o per la prevenzione di frodi.

Il documento aggiorna il parere 6/2014 del Gruppo Art. 29 (sostituito dal CEPD), alla luce delle novità introdotte, rispetto alla direttiva 95/46/CE, dal RGPD, che ha peraltro recepito alcune delle raccomandazioni fornite a suo tempo dallo stesso Gruppo Art. 29. Inoltre, tiene in considerazione la giurisprudenza della Corte di giustizia, tra cui la recente sentenza C-621/22 riguardo alla qualificazione dell'interesse "legittimo".

Linee guida sull'applicazione dell'art. 5, par. 3 della direttiva *e-Privacy*

Il 7 ottobre 2024, a seguito della consultazione pubblica lanciata a fine 2023 (cfr. Relazione 2023, p. 219), il CEPD ha adottato la versione finale delle linee guida 2/2023 sull'ambito tecnico di applicazione dell'art. 5, par. 3 della direttiva 2002/58/CE. Le linee guida mirano a chiarire quali operazioni, in particolare quali tecniche di tracciamento nuove ed emergenti, siano coperte dalla normativa vigente, nonché a fornire maggiore certezza giuridica ai titolari del trattamento e agli interessati. Il testo finale non presenta modifiche o integrazioni di rilievo; tuttavia, coglie l'occasione per chiarire, tra l'altro, che l'analisi dell'applicazione delle esenzioni all'obbligo di raccogliere il consenso previsto dall'art. 5, par. 3 della direttiva *e-privacy* esula dallo scopo che le linee guida si prefiggono.

Protezione dei dati, concorrenza e tutela dei consumatori

È proseguito il lavoro del Comitato sulle interazioni tra protezione dei dati, diritto della concorrenza e tutela dei consumatori, questione sempre più rilevante a fronte delle crescenti sinergie tra questi diversi ambiti, anche a seguito dei molti interventi normativi

21

a livello UE nell'ambito delle tecnologie digitali e della nota sentenza della Corte di Giustizia "*Bundeskartellamt*" (Causa C-252/21). La strategia dell'EDPB per il 2024-2027 sottolinea infatti la necessità di affrontare il ruolo e l'importanza della protezione dei dati nel contesto interdisciplinare e inter-regolamentare, riaffermando la necessità di promuovere coerenza e cooperazione con altre autorità di regolamentazione responsabili dell'attuazione delle normative UE sul pacchetto digitale, in particolare il *Digital Markets Act* (DMA), il *Digital Services Act* (DSA) e l'*Artificial Intelligence Act* (AI *Act*).

Il CEPD ha dato inizio alla stesura, insieme ai servizi della Commissione europea che si occupano dell'applicazione del *Digital Markets Act*, di specifiche linee guida sull'interazione tra RGPD e DMA. Si tratta di un esercizio innovativo, che vede per la prima volta impegnati congiuntamente il CEPD e la Commissione, volto a fornire indicazioni interpretative su alcune specifiche norme del DMA che presentano punti di intersezione con il RGPD; si considerino, ad es., gli obblighi cui sono tenuti i *gatekeepers* ai sensi dell'art. 5, par. 2 del DMA. L'intento dell'operazione è di facilitare un'applicazione coerente dei due regolamenti e un più efficace perseguimento degli obiettivi dei testi normativi, nel rispetto delle rispettive competenze.

DMA *High Level Group*

Del resto, la necessità che il DMA e altre regolamentazioni settoriali siano attuati in maniera coerente e complementare è già rispecchiata nell'attività del DMA *High Level Group* (HLG). Il Gruppo, istituito ai sensi dell'art. 40 del DMA, riunisce trenta membri nominati da diversi regolatori e reti europee tra cui il GEPD e il CEPD, rappresentato da cinque componenti tra cui il Presidente del Garante Prof. Pasquale Stanzione (v. Relazione 2023, p. 210). L'HLG si è riunito a Bruxelles il 22 maggio 2024. Nel corso della riunione, è stata adottata una dichiarazione in materia di IA ed è stato istituito uno specifico gruppo incaricato di seguire gli sviluppi del rapporto tra le diverse regolamentazioni e di condividere esperienze applicative del DMA anche con riferimento all'IA.

Sempre in merito all'interazione e alla cooperazione in ambito regolatorio, il CEPD ha ritenuto opportuno dedicare una ancora maggiore attenzione a tali temi attraverso la creazione di un nuovo sottogruppo, il *Cross-Regulatory Interplay and Cooperation Expert Subgroup* (CIC ESG), che si dedicherà al rapporto tra la protezione dei dati e i diversi settori del diritto europeo che, pur incentrati sul mercato e orientati all'economia, hanno considerevoli ricadute sulla tutela dei dati e sulle attività delle autorità di supervisione.

Dichiarazione 4/2024 sulla proposta di nuove regole procedurali

Nell'ottica di contribuire alla corretta e più efficiente applicazione dei meccanismi di cooperazione, il CEPD ha continuato a seguire con attenzione gli sviluppi legislativi relativi alla proposta di regolamento, presentata dalla Commissione europea il 4 luglio 2023, che stabilisce norme procedurali supplementari relative all'applicazione del RGPD nei procedimenti relativi a trattamenti transfrontalieri ("proposta"). Con la dichiarazione 4/2024 sui recenti sviluppi legislativi relativi alla proposta, il CEPD, facendo seguito al parere congiunto 1/2023, con il quale, insieme al GEPD, aveva accolto con favore la proposta e formulato raccomandazioni su come perfezionarla (v. Relazione 2023, p. 211), ha fornito ulteriori raccomandazioni ai co-legislatori alla luce degli emendamenti apportati, in prima lettura, dal Parlamento europeo e dal Consiglio dell'Unione.

In particolare, il CEPD ha ribadito la necessità di una base giuridica e di una procedura armonizzata che consentano la composizione amichevole delle controversie in tutti gli Stati membri e si è detto a favore dell'approccio del Consiglio in merito ai diritti dei reclamanti, sottolineando che questi ultimi dovrebbero godere di diritti procedurali nella misura in cui sono in gioco i loro diritti soggettivi. Il CEPD ha anche condiviso l'obiettivo di una maggiore trasparenza e armonizzazione del diritto di accesso, esprimendo al contempo alcune preoccupazioni in merito al concetto di "fascicolo congiunto" (del procedimento) introdotto nel testo del Parlamento poiché ri-

chiederebbe complesse modifiche ai sistemi di gestione dei documenti e di comunicazione utilizzati a livello europeo e nazionale. Ha accolto con favore l'emendamento del Consiglio relativo alla possibilità per l'autorità capofila di rinunciare alla cosiddetta "cooperazione rafforzata" (quella disciplinata, appunto, dal regolamento in questione) quando sono in gioco casi più semplici, ma ha chiesto di chiarire ulteriormente quali siano tali casi e di prevedere che l'opposizione a tale decisione anche da parte di una sola autorità interessata ripristini la cooperazione rafforzata. Il Comitato ha inoltre accolto con favore l'inclusione di termini procedurali aggiuntivi ma flessibili, ricordando nel contempo che gli stessi devono essere realistici.

Trasferimenti di dati - linee guida sull'art. 37 della LED

Il 19 giugno 2024, a seguito della consultazione pubblica, il CEPD ha adottato la versione finale delle linee guida 1/2023 sull'interpretazione dell'art. 37 della direttiva 2016/680 (LED). L'art. 37 disciplina i trasferimenti di dati personali da parte delle autorità dei paesi UE, competenti per le attività di contrasto, verso altre autorità competenti di paesi terzi o organizzazioni internazionali. A seguito delle osservazioni pervenute, la versione finale delle linee guida coglie l'occasione per chiarire uno dei principi generali per il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali previsto dall'art. 35(1)(b) della LED. In base a tale disposizione, i dati personali possono essere trasferiti a titolari del trattamento in un paese terzo o a un'organizzazione internazionale che siano autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (art. 1, comma 1, della LED). Sebbene il cons. 64 della LED faccia riferimento, con riguardo a tali trasferimenti, a responsabili del trattamento in paesi terzi, alla luce della formulazione esplicita e inequivocabile dell'art. 35, par. 1, lett. b), della LED ciò deve intendersi come relativo solo a responsabili del trattamento che agiscano per conto e in conformità alle istruzioni di un'autorità competente nel paese terzo destinataria di dati personali dall'UE. Una deroga al principio stabilito dall'art. 35, par. 1, lett. b), della LED richiederebbe, secondo il Comitato, una disposizione espressa, simile a quella prevista all'art. 39, par. 1, della LED per "altri destinatari" stabiliti in paesi terzi.

Trasferimenti di dati – linee guida sull'art. 48 RGPD

Con l'adozione delle linee guida 2/2024 sull'art. 48 RGPD a dicembre 2024, il CEPD ha completato il quadro delle linee guida relative all'applicazione delle disposizioni relative al Capo V del RGPD dedicato al trasferimento dei dati verso paesi terzi.

L'art. 48 riveste una posizione peculiare in tale contesto, facendo riferimento ai casi in cui le organizzazioni stabilite in UE/SEE ricevono richieste da parte di autorità pubbliche di Paesi terzi volte ad acquisire dati personali. Nelle linee guida, il CEPD ha chiarito le condizioni alle quali i titolari e i responsabili del trattamento possono rispondere alle richieste delle autorità di paesi terzi, tenuto conto che le sentenze o le decisioni delle autorità di paesi terzi non possono essere automaticamente e direttamente riconosciute o eseguite in uno Stato membro dell'UE e che l'eventuale trasmissione di dati sulla base della richiesta ricevuta costituisce un trasferimento ai sensi del RGPD e, in quanto tale, deve essere conforme all'art. 6 (base giuridica) e al capo V (presupposto per il trasferimento). Le linee guida chiariscono che un accordo internazionale può sia costituire una base giuridica che prevedere le necessarie garanzie per il trasferimento e, in sua assenza, o se l'accordo non prevede una base giuridica o garanzie adeguate, potrebbero essere prese in considerazione altre basi giuridiche o altri motivi di trasferimento, in circostanze eccezionali e da valutarsi caso per caso. Sulle linee guida è stata avviata una consultazione pubblica e le stesse potranno essere, se del caso, riviste anche alla luce dei suoi esiti.

Trasferimenti di dati - Revisione di undici decisioni di adeguatezza

Sebbene la Commissione europea non abbia adottato alcuna nuova decisione di adeguatezza ai sensi dell'art. 45 del RGPD nel corso dell'anno, il tema è rimasto all'attenzione del Comitato per via della conclusione, il 15 gennaio 2024, dei lavori di

21

revisione delle undici decisioni di adeguatezza adottate ai sensi della direttiva 95/46/CE. Con una relazione e un documento di lavoro più dettagliato sui singoli paesi interessati (*report* nazionali), la Commissione ha reso noto che i dati personali possono continuare a essere trasferiti dall'UE ad Andorra, Argentina, Canada, Isole Faroe, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera e Uruguay dal momento che tali paesi e territori continuano a beneficiare di adeguate garanzie di protezione dei dati e che, pertanto, le decisioni di adeguatezza a suo tempo adottate rimangono in vigore.

Poiché nessuna decisione di adeguatezza è stata abrogata, modificata o sospesa, il Comitato non è stato chiamato a fornire un parere in merito alla valutazione della Commissione ma, alla luce della propria *expertise* e del ruolo che le decisioni di adeguatezza ricoprono nel contesto della disciplina dei flussi verso paesi terzi, ha analizzato la relazione e i *report* e ha indirizzato, a dicembre 2024, una lettera alla Commissione con la quale ha riconosciuto l'ampio lavoro svolto nell'esaminare la legislazione; al contempo, ha invitato la Commissione a fornire informazioni più trasparenti sulla valutazione effettuata in ordine al rispetto dello stato di diritto nei diversi paesi e a descrivere, nelle prossime revisioni, in modo più omogeneo, le basi giuridiche riconosciute dalle legislazioni interessate, le limitazioni applicabili ai diritti degli interessati, le garanzie relative ai processi decisionali automatizzati, gli impegni internazionali assunti dai diversi paesi e le regole sui trasferimenti ulteriori di dati e sulla loro applicazione pratica.

La revisione è stata la prima occasione per valutare il quadro normativo relativo all'accesso e all'uso dei dati personali trasferiti da parte delle autorità governative degli undici paesi e territori interessati per scopi di *law enforcement* e sicurezza nazionale e, a questo riguardo, il Comitato ha rilevato che l'applicazione pratica delle norme che derogano alle regole di protezione dei dati per scopi di *law enforcement* e sicurezza nazionale e l'impatto sulla valutazione di adeguatezza delle eccezioni di carattere generale al diritto alla *privacy* e alla protezione dei dati, come nei casi di stato di emergenza, richiedono particolare attenzione e monitoraggio nelle future decisioni e revisioni di adeguatezza.

Trasferimenti di dati - Prima revisione del quadro UE-USA sulla *privacy*

Sempre in tema di revisioni delle decisioni di adeguatezza, l'art. 3 della decisione di esecuzione 4745/2023 relativa al livello adeguato di protezione dei dati personali nell'ambito del quadro UE-USA sulla *privacy* dei dati (EU-US *Data Privacy Framework*, di seguito anche DPF UE-USA), adottata dalla Commissione nel luglio 2023, prevedeva che la prima revisione periodica avesse luogo trascorso un anno dalla sua notifica agli Stati membri.

A tal fine, a seguito di alcuni scambi e di una riunione con le autorità statunitensi alla quale, insieme alla Commissione, hanno partecipato cinque rappresentanti del CEPD, la Commissione ha presentato la sua relazione il 9 ottobre 2024, seguita – come già successo in passato in occasione delle revisioni delle precedenti decisioni di adeguatezza – da una relazione del Comitato, adottata a novembre. In questo documento, il CEPD ha preso atto positivamente degli sviluppi verificatisi, dopo l'adozione della decisione di adeguatezza, per dare applicazione a tutti gli elementi previsti nel DPF UE-USA e, per quanto riguarda gli aspetti commerciali, dell'adozione di tutti i passaggi necessari per consentire il processo di autocertificazione delle aziende negli USA. Considerata l'assenza di reclami, la relazione ha tuttavia invitato le competenti autorità statunitensi ad effettuare dei controlli proattivi sul rispetto dei principi del DPF UE-USA da parte delle aziende autocertificate, aumentando le indagini d'ufficio. Il Comitato ha anche invitato il Dipartimento del Commercio a pubblicare una guida pratica sul principio di *accountability* per gli *onward transfers* e sulla nozione di "dati sulle risorse umane" al fine di chiarire la persistente divergenza nell'interpretazione della nozione tra le autorità europee e le istituzioni statunitensi.

Per quanto riguarda l'accesso per fini di *law enforcement* e di sicurezza nazionale da parte delle autorità pubbliche statunitensi ai dati personali trasferiti dall'UE a organizzazioni certificate, la relazione del Comitato si è concentrata sull'effettiva attuazione delle garanzie stabilite dall'*Executive Order* 14086 (E.O.), ovvero i principi di necessità e proporzionalità e il nuovo meccanismo di ricorso, nonché sugli sviluppi pertinenti della legislazione statunitense. Poiché durante la revisione periodica non è stato possibile valutare come i suddetti principi siano stati concretamente interpretati e applicati né testare nella pratica l'effettivo funzionamento del meccanismo di ricorso, per l'assenza di reclami, la relazione ha sottolineato la necessità che la Commissione continui a monitorare attentamente questo aspetto, anche nelle revisioni future.

Sotto il profilo degli sviluppi pertinenti della legislazione statunitense, la relazione del Comitato, nel prendere atto della riforma intervenuta ad aprile 2024, che ha autorizzato per altri due anni l'applicazione dell'art. 702 del *Foreign Intelligence Surveillance Act* (FISA) e ne ha esteso la portata, in merito all'ampliamento della definizione di "fornitore di servizi di comunicazione elettronica", ovvero dei soggetti che potrebbero essere tenuti a divulgare dati personali ai sensi dell'art. 702 del FISA, ha espresso preoccupazione per l'assenza dei requisiti di chiarezza, precisione e accessibilità della nuova disposizione che non consente di identificare chiaramente i soggetti inclusi in tale definizione.

Infine, per quanto riguarda la prossima revisione periodica, il Comitato ha considerato opportuno che la stessa possa avere luogo entro un periodo inferiore a quattro anni.

Il CEPD ha anche adottato una serie di documenti con lo scopo di favorire l'effettiva ed efficace applicazione della decisione di adeguatezza relativa al DPF UE-USA.

Con una nota informativa adottata ad aprile 2024, pubblicata anche sul sito dell'Autorità (doc. web n. 10039130), le persone, i cui dati siano stati trasferiti negli USA dopo il 10 luglio 2023, sono informate in ordine al loro diritto di presentare reclamo per contestare l'eventuale accesso ai dati personali da parte delle autorità di *intelligence* degli Stati Uniti in violazione delle garanzie previste dal DPF UE-USA. La nota è accompagnata da un modello di reclamo che gli individui possono presentare, in modo standardizzato (doc. web n. 10039156), alle autorità statunitensi, per il tramite della propria autorità di controllo, e dal reg. interno che chiarisce i rispettivi compiti delle autorità di protezione dei dati e del segretariato del CEPD riguardo al suddetto meccanismo di reclamo.

Analogamente, per gli aspetti commerciali, il Comitato ha adottato un modello che mira ad agevolare la presentazione di reclami relativi a presunte violazioni del DPF UE-USA da parte di un'organizzazione statunitense in caso di trattamento di dati personali trasferiti dall'EEA, ai sensi della decisione sull'adeguatezza, dopo il 10 luglio 2023 (doc. web n. 10039117). Insieme al modello sono state anche adottate le regole interne relative alla trattazione, da parte del gruppo informale di autorità di protezione dei dati dell'UE (cd. *Panel*), di tali reclami che possono essere presentati, in particolare, quando il trattamento riguarda dati trattati per finalità di risorse umane raccolti nell'ambito di un rapporto di lavoro o qualora l'organizzazione statunitense abbia volontariamente accettato di sottoporsi alla supervisione da parte delle autorità di protezione dei dati nell'Unione.

Sempre con riferimento agli aspetti commerciali della decisione, il Comitato ha inoltre adottato a luglio 2024 due diversi *set* di FAQ che intendono, da un lato, spiegare agli individui cosa è e a cosa serve la decisione di adeguatezza relativa al DPF UE-USA e come presentare i reclami nel caso di mancato rispetto dei principi in esso sanciti da parte delle società importatrici statunitensi e, dall'altro, chiarire alle imprese cosa fare prima di trasferire dati personali a società che si dichiarano parte del *Framework* e come lo stesso funziona.

Primo incontro con le autorità dei paesi adeguati

Il rilievo delle decisioni di adeguatezza nell'assicurare un elevato grado di convergenza delle leggi sulla protezione dei dati anche al di fuori dei confini dell'Unione e nel favorire flussi di dati personali più sicuri è stato riconosciuto in occasione dell'incontro, svoltosi l'8 ottobre 2024, tra CEPD e i commissari e i rappresentanti delle autorità di protezione dei dati dei quindici paesi che sono stati oggetto di una decisione di adeguatezza dell'UE. In tale occasione, e nell'ottica di futuri incontri analoghi, sono state avviate discussioni in merito alla possibilità di porre in essere attività di consultazione multilaterali e di confronto su temi specifici, nonché attività di cooperazione in materia di applicazione delle norme.

BCR

Nel 2024 è stata data applicazione alle nuove raccomandazioni 01/2022 sulla domanda di approvazione e sugli elementi e principi contenuti nelle norme vincolanti d'impresa (BCR) per titolari del trattamento (art. 47 del RGPD), adottate in via definitiva nel 2023 (v. Relazione 2023, p. 216) e, alla luce delle stesse, sono state approvate otto BCR per titolari del trattamento. Sette sono state le BCR per responsabili del trattamento valutate ancora alla luce del WP 257.rev.01.

CEF diritto di accesso 2024

Nel corso del 2024 le autorità di protezione dei dati del SEE (tra cui il Garante) hanno avviato indagini coordinate sulla conformità dei titolari del trattamento alle disposizioni del RGPD in materia di diritto di accesso (CEF *right of access*). Un totale di 1.185 titolari di trattamento costituiti da piccole e medie imprese (PMI) e grandi imprese attive in diversi settori, nonché varie tipologie di enti pubblici, hanno risposto all'azione, a conclusione della quale il CEPD ha adottato una relazione contenente alcune raccomandazioni.

A seguito dell'azione CEF 2024 sono state individuate sette aree di intervento, tra cui in particolare la mancanza di procedure interne documentate per gestire le richieste di accesso. Per ciascuna di tali aree, la relazione fornisce un elenco di raccomandazioni non vincolanti di cui i titolari del trattamento e le autorità di protezione dei dati devono tenere conto.

In ogni caso, due terzi delle autorità partecipanti hanno valutato il livello di conformità dei titolari del trattamento che hanno risposto da "medio" a "elevato" per quanto riguarda il diritto di accesso. Un fattore identificato come importante al riguardo è il volume delle richieste di accesso ricevute dai titolari, nonché le dimensioni dell'organizzazione. Più specificamente, i titolari di grandi dimensioni o che ricevono più richieste hanno maggiori probabilità di raggiungere un livello più elevato di conformità rispetto alle piccole organizzazioni che dispongono di minori risorse. Sono state censite anche alcune buone prassi realizzate da titolari del trattamento, come la messa a disposizione di moduli *online* di facile utilizzo che consentono di presentare facilmente una richiesta di accesso e sistemi *self-service* che permettono di scaricare autonomamente i propri dati personali con pochi *click* e in qualsiasi momento.

Relazione della *Task Force* ChatGPT

Il 23 maggio 2024, il CEPD ha adottato un *Report* sul lavoro svolto dalla *Task Force* ChatGPT, coordinata da una rappresentante del Garante unitamente ad un rappresentante dell'Autorità austriaca, relativo ad una prima interpretazione delle disposizioni del RGPD applicabili in relazione a ChatGPT, il servizio di IA generativa fornito dalla società statunitense OpenAI OpCo LLC. La *Task Force* è stata creata nell'aprile 2023 per promuovere la cooperazione tra le autorità di protezione dei dati personali e le posizioni espresse nel documento derivano dal coordinamento dei membri della *Task Force* finalizzato alla gestione armonizzata delle indagini nazionali relative al servizio ChatGPT. Il *Report* affronta le questioni giuridiche fondamentali legate allo sviluppo, all'implementazione ed all'uso di ChatGPT e le sue implicazioni per la protezione dei dati personali e i diritti fondamentali degli utenti. Il *Report* evidenzia i profili di conformità delle operazioni di trattamento dei dati personali da parte di ChatGPT alle

disposizioni del RGPD, in particolare rispetto ai principi di trasparenza, liceità e minimizzazione del trattamento dei dati personali. Quanto alla liceità, suggerisce di distinguere le diverse fasi del trattamento: i) raccolta di dati per l'addestramento dei modelli LLM, compresi *web scraping* e/o utilizzo di *dataset*; ii) pre-addestramento dei modelli, compreso il filtraggio; iii) addestramento dei modelli; iv) *prompt* e *output* del servizio ChatGPT; v) addestramento del servizio ChatGPT mediante i *prompt* di utilizzo del servizio stesso.

Oltre al principio di liceità del trattamento e della raccolta dei dati per l'addestramento di ChatGPT, il *Report* analizza: i) il principio di correttezza, sottolineando che non dovrebbe esserci alcun trasferimento del rischio, nel senso che i titolari, nella fattispecie OpenAI OpCo LLC, non dovrebbero trasferire i rischi dell'impresa sugli interessati; ii) il principio di esattezza (*accuracy*), specificando che spetta al titolare del trattamento fornire informazioni adeguate sulla natura probabilistica dell'*output* del servizio e fare esplicito riferimento al fatto che il testo generato dal *chatbot* potrebbe essere parziale o inventato; iii) il principio di trasparenza, distinguendo la fase di raccolta di dati per l'addestramento dei modelli (in particolare, in ipotesi di *web scraping* di dati personali da fonti accessibili al pubblico, trova applicazione l'art. 14 del RGPD e potrebbe valere l'esenzione dall'obbligo di informativa di cui all'art. 14, par. 5, lett. b), a condizione che siano pienamente integrati tutti i requisiti di tale disposizione) dalla fase di raccolta di dati durante l'utilizzo del servizio (in tale ipotesi trova applicazione l'art. 13 del RGPD e, in questo contesto, risulta di particolare importanza informare gli interessati che i *prompt* potrebbero essere utilizzati per finalità di addestramento dei modelli sottesi al *chatbot*). Infine, il *Report* sottolinea la garanzia a favore degli interessati dell'esercizio effettivo dei diritti previsti dal RGPD.

Il *Report* è il risultato di valutazioni preliminari che non pregiudicano l'analisi che verrà effettuata dalle singole autorità nazionali nell'ambito delle istruttorie in corso, aperte prima del 15 febbraio 2024, data dalla quale è stato riconosciuto ad OpenAI OpCo LLm lo stabilimento nell'Unione europea (nello specifico, in Irlanda) e da cui decorre l'applicazione del meccanismo dello "sportello unico" di cui all'art. 60 RGPD.

Pareri *ex* art. 64, par. 1, RGPD

- Codice di condotta europeo nel settore della ricerca clinica. Secondo il RGPD, l'adesione a codici di condotta approvati può essere utilizzata come elemento per dimostrare la conformità alle sue disposizioni. In tale ambito, il CEPD ha adottato un parere ai sensi dell'art. 64, par. 1, lett. d), RGPD sul progetto di decisione dell'autorità di controllo francese di approvazione del codice di condotta europeo predisposto dall'*European Contract Research Organization Federation* (EUCROF). Il codice di condotta riguarda le attività di trattamento svolte dalle organizzazioni di ricerca a contratto (CRO) nel settore della ricerca clinica (parere 12/2024). Lo scopo del codice è quello di precisare gli obblighi che, alla luce dell'art. 28 del RGPD, sono in capo alle predette organizzazioni, quando agiscono come responsabili del trattamento nel contesto dell'esecuzione del contratto di servizi tra loro e lo sponsor nell'ambito delle sperimentazioni cliniche e della ricerca non interventistica. L'ambito di applicazione territoriale del codice comprende tutta l'UE, ai sensi dell'art. 40, par. 7, RGPD, e non si estende agli Stati del SEE.

- Requisiti per l'accreditamento degli organismi di certificazione. È proseguita 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, RGPD (cfr. le linee guida del CEPD 4/2018 sull'accreditamento degli organismi di certificazione). Nel 2024 il Comitato ha reso il parere previsto dall'art. 64, par. 1, lett. c), RGPD in ordine al progetto di requisiti aggiuntivi per l'accreditamento degli organismi di certificazione predisposti dall'autorità di controllo svedese (parere 10/2024).

21

- Sigilli europei per la protezione dei dati. Scopo principale dei meccanismi di certificazione della protezione dei dati è quello di contribuire a dimostrare la conformità al RGPD delle attività di trattamento e ad aumentare la trasparenza e la fiducia. La certificazione consente infatti una migliore valutazione del grado di protezione offerto da prodotti, servizi, processi o sistemi utilizzati dalle organizzazioni che trattano dati personali. In tale quadro, il CEPD nel settembre 2022 aveva adottato un parere di coerenza sui criteri di certificazione EuroPriSe, consentendone il riconoscimento in Germania come criteri di certificazione per le operazioni di trattamento da parte di responsabili del trattamento (parere 25/2022 del 13 settembre 2022) (v. Relazione 2022, p. 183). A settembre 2023, il Comitato aveva poi adottato un parere di coerenza sui criteri di certificazione nazionale *Brand Compliance*, rendendoli criteri di certificazione ufficialmente riconosciuti nei Paesi Bassi per il trattamento dei dati da parte di titolari e responsabili (parere 15/2023 del 19 settembre 2023) (v. Relazione 2023, p. 218). A seguito di un aggiornamento di entrambi gli schemi, con due nuovi pareri di coerenza, resi rispettivamente il 18 luglio e il 2 dicembre 2024, il Comitato ha approvato i criteri di certificazione sopra menzionati come applicabili in tutta l'UE/SEE, vale a dire come sigilli europei per la protezione dei dati (pareri 19/2024 e 27/2024). Due nuove certificazioni comuni europee sono state pertanto aggiunte al registro dei meccanismi di certificazione e dei sigilli di protezione dei dati curato dal CEPD in conformità all'art. 42, par. 8, RGPD.

- Meccanismi nazionali di certificazione della protezione dati. Inoltre, nel 2024 il Comitato ha reso diversi pareri ai sensi dell'art. 64, par. 1, lett. c), RGPD per garantire la coerenza e la corretta applicazione di criteri di certificazione nazionali tra le diverse autorità di controllo nell'UE/SEE. In particolare, è stato reso il parere 7/2024 sul progetto di decisione dell'autorità di controllo tedesca del Nord Reno-Vestfalia di approvazione dei criteri di certificazione *EU Cloud Service Data Protection (Auditor)*, consentendone l'utilizzo in Germania per la certificazione dei trattamenti effettuati da fornitori di servizi *cloud*; il parere 18/2024 sul progetto di decisione dell'autorità di controllo austriaca di approvazione dei criteri di certificazione *DSGVO-zt GmbH*, applicabili in Austria per la certificazione di titolari del trattamento; il parere 26/2024 sul progetto di decisione dell'autorità di controllo di Brema di approvazione del *Catalogue of Criteria for the Certification of IT-supported Processing of Personal Data pursuant to Art 42 GDPR (GDPR - information privacy standard)* che sono stati così riconosciuti in Germania per la certificazione di titolari e responsabili del trattamento.

- Schema di certificazione europea della cybersicurezza per i servizi *cloud*. Sempre in materia di certificazioni, è proseguita l'attività di collaborazione tra il CEPD ed ENISA in tema di certificazione europea della cybersicurezza per i servizi *cloud* (v. Relazione 2021, p. 221). Rispetto allo schema di certificazione europeo sviluppato da ENISA in tale ambito (EUCS - *European Cybersecurity Certification Scheme for Cloud Services*), in attuazione del reg. UE 2019/881, con la lettera del 22 luglio, il Comitato ha proposto ad ENISA di creare un gruppo di lavoro congiunto con il compito valutare la possibilità di: elaborare linee guida relative alla protezione dei dati sia per i fornitori di servizi *cloud* che per i loro clienti; assistere le autorità di controllo e i proprietari di meccanismi di certificazione e di codici di condotta ad articolare gli strumenti di conformità previsti dal RGPD con lo schema europeo di certificazione per la cybersicurezza; sviluppare una metodologia di valutazione del rischio che tenga in considerazione i rischi per la protezione dei dati; creare un'estensione dello schema europeo di certificazione per la cybersicurezza che copra i requisiti aggiuntivi correlati al RGPD.

Pareri *ex* art. 64, par. 2, RGPD

Come sottolineato, il 2024 è stato contrassegnato da un impegnativo lavoro di predisposizione di pareri ai sensi dell'art. 64, par. 2, RGPD, norma che consente a ciascuna autorità di controllo (ma anche al presidente del Comitato o alla Commissione) di richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal CEPD al fine di ottenere un parere.

Le questioni sottoposte al CEPD sono state infatti particolarmente complesse ed hanno riguardato importanti nodi concernenti l'applicazione del RGPD.

- Parere sulla nozione di stabilimento principale. Il parere 4/2024 sulla nozione di stabilimento principale e sui criteri per l'applicazione del meccanismo dello "Sportello unico" del 13 febbraio 2024 chiarisce la nozione di "stabilimento principale" del titolare del trattamento nell'UE, in particolare per i casi in cui le decisioni relative al trattamento vengano prese al di fuori dell'Unione. La nozione di stabilimento principale costituisce uno dei pilastri dell'OSS ed è fondamentale per determinare l'autorità di controllo capofila nei casi di trattamento transfrontaliero di dati personali. Il parere chiarisce altresì le condizioni necessarie affinché i titolari del trattamento possano accedere allo sportello unico fornendo ulteriori indicazioni per la determinazione dell'autorità capofila - in particolare, la circostanza per cui il "luogo di amministrazione centrale" di un titolare del trattamento nell'UE può essere considerato uno stabilimento principale ai sensi dell'art. 4, par. 16, lett. a), RGPD solo se in esso si prendono decisioni sulle finalità e sui mezzi del trattamento dei dati e se sussiste il potere di far attuare tali decisioni. Il meccanismo di sportello unico può dunque applicarsi solo se vi è prova che uno degli stabilimenti del titolare del trattamento nell'UE prende decisioni sulle finalità e sui mezzi delle operazioni di trattamento pertinenti e ha il potere di imporre tali decisioni. Ne consegue che, quando tale evidenza non risulta sussistere, non sussiste neppure uno stabilimento principale del titolare del trattamento nell'Unione e non si applica il meccanismo di sportello unico, cosicché ciascuna autorità nazionale può intervenire direttamente nei confronti del titolare in questione.

- Parere sul *consent or pay*. Il parere 8/2024 esamina in particolare i requisiti che il consenso deve avere affinché possa dirsi valido, e in particolare liberamente prestato, nei modelli implementati dalle grandi piattaforme *online* fondati sull'alternativa, offerta all'interessato, tra fornire il consenso al trattamento dei dati che lo riguardano ai fini di pubblicità comportamentale e il pagamento di un prezzo per usufruire del servizio (anche alla luce della sentenza *Bundeskartellamt* della CGUE - C-252/21). Uno dei punti cardine del parere è che, nella maggior parte dei casi, non è possibile per le grandi piattaforme *online* soddisfare i requisiti per un consenso valido, nella misura in cui agli utenti sia lasciata solamente una scelta binaria tra il consenso al trattamento dei dati personali per scopi pubblicitari comportamentali e il pagamento di un corrispettivo.

Tali titolari dovrebbero infatti prendere in considerazione la possibilità di fornire alle persone una "alternativa equivalente" che non comporti il pagamento di un prezzo. Ove i titolari del trattamento scelgano di addebitare un costo per l'accesso alla "alternativa equivalente", dovrebbero considerare altresì l'offerta di un'alternativa aggiuntiva, priva di pubblicità comportamentale, ad esempio fondata su forme pubblicitarie che non comportino il trattamento dati personali o quantomeno si fondino sul trattamento di un numero di dati inferiore.

L'ottenimento di un valido consenso non esime, tuttavia, il titolare dall'obbligo di aderire a tutti i principi di cui all'art. 5 del RGPD, quali la specificità delle finalità del trattamento, la minimizzazione dei dati e la correttezza. Necessità, proporzionalità e *accountability* rimangono parimenti i principi cardine del RGPD che devono sempre essere rispettati. Per poter assicurare che il consenso sia liberamente prestato occorre inoltre tener conto di una serie di criteri tra cui la granularità, il pregiudizio per

l'interessato che deriva dalla mancata prestazione del consenso (quali l'esclusione da un servizio, la mancanza di accesso alle reti professionali o il rischio di perdere contenuti o connessioni) e lo squilibrio di potere tra titolare e interessato. Né può dirsi irrilevante, nella valutazione che i titolari del trattamento devono effettuare, caso per caso, la presenza di uno squilibrio di potere tra l'individuo e il titolare del trattamento, che può essere determinato da diversi fattori, compresa la posizione delle grandi piattaforme *online* sul mercato, la misura in cui l'individuo si basa sul servizio e il pubblico principale del servizio.

Il tema del *consent or pay* sarà oggetto di più ampie linee guida su cui il CEPD ha già cominciato a lavorare, anche raccogliendo i contributi dei molti attori interessati attraverso un evento aperto al pubblico che ha avuto luogo il 18 novembre 2024.

- Parere sul riconoscimento facciale negli aeroporti. Il parere 11/2024 riguarda l'uso delle tecnologie di riconoscimento facciale da parte dei gestori aeroportuali e delle compagnie aeree per lo scopo specifico di snellire il flusso di passeggeri negli aeroporti. Il parere non riguarda quindi l'uso del riconoscimento facciale in generale ovvero per scopi di sicurezza, controllo delle frontiere o da parte delle Forze dell'ordine. Esso muove dalla considerazione che i dati biometrici sono particolarmente sensibili e che il loro trattamento può creare rischi significativi per le persone interessate. In particolare, la tecnologia di riconoscimento facciale può generare falsi negativi, distorsioni e discriminazioni e l'uso improprio dei dati biometrici può anche avere gravi conseguenze per gli individui, come furti di identità e sostituzioni di persona. Pertanto, nel parere, il Comitato invita le compagnie aeree e i gestori aeroportuali a valutare l'impatto del trattamento sui diritti degli interessati e optare, ove possibile, per modalità meno invasive, in grado di raggiungere lo scopo di razionalizzare il flusso di passeggeri negli aeroporti, e che garantiscano al contempo che gli individui abbiano il massimo controllo sui propri dati biometrici.

Nello specifico, il CEPD analizza la compatibilità del trattamento dei dati biometrici dei passeggeri, mediante tecnologie di riconoscimento facciale, con il principio di limitazione della conservazione (art. 5, par. 1, lett. e), RGPD), di integrità e riservatezza (art. 5, par. 1, lett. f), RGPD), di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 RGPD), nonché con gli obblighi di sicurezza del trattamento (art. 32 RGPD). Non viene invece esaminata la conformità del trattamento ad altre disposizioni del RGPD, incluse quelle relative alla liceità del trattamento.

Il parere afferma innanzitutto che non esiste una norma del diritto UE che richieda ai gestori aeroportuali e alle compagnie aeree di verificare che il nome sulla carta d'imbarco del passeggero corrisponda al nome sul suo documento di identità e che tale aspetto può essere regolato da leggi nazionali. Pertanto, laddove non sia richiesta alcuna verifica dell'identità dei passeggeri, non dovrebbe essere eseguita alcuna verifica biometrica, poiché ciò comporterebbe un trattamento eccessivo dei dati.

Viene quindi esaminata la conformità del trattamento dei dati biometrici dei passeggeri rispetto a quattro diverse tipologie di soluzioni tecniche di conservazione del *template* biometrico, che vanno da quella che prevede la conservazione del modello biometrico solo nelle mani dell'interessato a quelle che si basano sulla sua conservazione centralizzata con diverse modalità. In tutti i casi, il Comitato sottolinea che dovrebbero essere trattati solo i dati biometrici dei passeggeri che acconsentono di partecipare al sistema registrando attivamente il proprio modello biometrico.

Alla luce di queste considerazioni, il CEPD rileva che le uniche soluzioni di conservazione che potrebbero essere compatibili con i principi di integrità e riservatezza, protezione dei dati fin dalla progettazione e per impostazione predefinita, nonché di sicurezza del trattamento, sono quelle in cui i dati biometrici sono conservati nelle mani

dell'interessato o in un *database* centralizzato ma con una chiave di crittografia esclusivamente nelle mani di quest'ultimo. Queste soluzioni di conservazione, se accompagnate dall'adozione di un elenco di garanzie minime, raccomandate nel parere, sono le uniche modalità che – ad avviso del Comitato – controbilanciano adeguatamente l'intrusività del trattamento offrendo agli interessati il massimo controllo sui propri dati. Per quanto riguarda il principio di limitazione della conservazione, il Comitato ribadisce che i titolari del trattamento devono assicurarsi di avere una giustificazione sufficiente per il periodo di conservazione previsto e limitarlo a quanto necessario per lo scopo perseguito.

- Parere sugli obblighi dei titolari che si affidano a responsabili e sub-responsabili. Il parere 22/2024 concerne alcuni obblighi in capo ai titolari del trattamento che si affidano a responsabili del trattamento e sub-responsabili del trattamento – derivanti in particolare dall'art. 28 RGPD, nonché dalla formulazione dei contratti tra titolare e responsabile del trattamento – anche con riferimento ai trasferimenti di dati verso paesi terzi. Il parere chiarisce che i titolari dovrebbero avere le informazioni sull'identità (cioè nome, indirizzo, persona di contatto) di tutti i responsabili e sub-responsabili del trattamento prontamente disponibili in ogni momento, indipendentemente dal rischio associato all'attività di trattamento. A tal fine, il responsabile dovrebbe fornire proattivamente al titolare tali informazioni, mantenendole aggiornate.

Il parere si sofferma poi sull'obbligo del titolare di verificare se i (sub)responsabili presentino "garanzie sufficienti" per attuare le misure appropriate stabilite dal titolare stesso e chiarisce che tale obbligo dovrebbe applicarsi indipendentemente dal rischio per i diritti e le libertà degli interessati. Tuttavia, la portata di tale verifica potrebbe variare nella pratica a seconda della natura di tali misure tecniche e organizzative, che possono essere più rigorose o più estese a seconda del livello di tale rischio.

Il Comitato specifica che, sebbene il responsabile del trattamento iniziale debba garantire che i sub-responsabili da esso proposti forniscano garanzie sufficienti, la decisione finale sull'opportunità di servirsene, anche per quanto riguarda la verifica delle garanzie, spetta al titolare del trattamento. A tale riguardo, il parere ritiene che, ai sensi del RGPD, il titolare del trattamento non abbia l'obbligo di richiedere sistematicamente i contratti con i sub-responsabili al fine di verificare se gli obblighi in materia di protezione dei dati previsti nel contratto iniziale siano stati trasferiti lungo la catena di trattamento. Il titolare del trattamento dovrebbe valutare, caso per caso, se sia necessario richiedere una copia di tali contratti o riesaminarli in qualsiasi momento per poter dimostrare la conformità alla luce del principio di responsabilità.

Nel parere, il CEPD affronta inoltre il tema dell'introduzione, nel contratto ai sensi dell'art. 28 RGPD, della formula contenuta nel par. 3, lett. a) dello stesso articolo, che prevede l'impegno del responsabile del trattamento a trattare i dati personali solo su istruzioni documentate del titolare del trattamento, a meno che lo stesso non sia "obbligato a [trattare] dal diritto dell'Unione o dello Stato membro cui è soggetto" – ricordando il principio generale secondo cui i contratti non possono prevalere sulla legge. Alla luce della libertà contrattuale concessa alle parti, il CEPD ritiene che l'inclusione della formula "a meno che ciò non sia richiesto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento" (testuale o in termini molto simili) sia altamente raccomandata ma non obbligatoria, e in ogni caso non esoneri il responsabile del trattamento dagli obblighi derivanti dal RGPD. Inoltre, il Comitato è del parere che la formulazione in questione non possa essere interpretata come un'istruzione documentata da parte del titolare del trattamento.

In tema di trasferimento di dati, il Comitato chiarisce che qualora i trasferimenti di dati personali al di fuori del SEE avvengano tra due (sub)responsabili del trattamento,

conformemente alle istruzioni del titolare, questi è comunque soggetto agli obblighi derivanti dall'art. 28, par. 1, RGPD sulle "garanzie sufficienti", oltre a quelle di cui all'art. 44, per garantire che il livello di protezione non sia compromesso dai trasferimenti di dati personali. Il responsabile/esportatore dovrebbe preparare la documentazione pertinente, in linea con le raccomandazioni 01/2020 del CEPD, e il titolare del trattamento dovrebbe valutare tale documentazione ed essere in grado di mostrarla all'autorità di controllo competente. Per i dati personali trasferiti al di fuori del SEE, il CEPD giudica improbabile che la formulazione "a meno che ciò non sia richiesto dalla legge o da un ordine vincolante di un ente governativo", di per sé, sia sufficiente per conseguire la conformità all'art. 28, par. 3, lett. a), RGPD in combinato disposto con il capo V.

- Parere in materia di IA. Il parere 28/2024, adottato il 17 dicembre 2024, ha riguardato alcuni aspetti relativi ai trattamenti di dati personali nel contesto dei modelli di IA, ed in particolare, in quali circostanze un modello di IA possa essere considerato "anonimo"; in che modo i titolari del trattamento possano dimostrare la validità del ricorso al legittimo interesse come base giuridica per il trattamento dei dati personali per creare, aggiornare e/o sviluppare un modello di IA; quali siano le conseguenze di un trattamento illecito di dati personali nella fase di sviluppo di un modello di IA (*development*) sul successivo trattamento o sul funzionamento del modello di IA (*deployment*). La stesura del parere è stata preceduta da un evento organizzato dal Comitato, aperto agli attori interessati, al fine di raccogliere contributi sulle questioni in esame.

Rispetto alla prima questione, il parere sostiene che i modelli di IA sviluppati sulla base di dati personali non possano essere considerati anonimi e che essi dovrebbero invece essere valutati caso per caso sulla base di criteri specifici; affinché un modello di IA possa essere considerato anonimo, sia la probabilità di estrazione diretta (anche probabilistica) di dati personali, sia la probabilità di ottenere dati personali dalle *query* dovrebbero essere insignificanti, tenuto conto di tutti i mezzi che possono essere ragionevolmente utilizzati dal titolare o da altro soggetto.

Con riferimento alla seconda questione, il parere esamina i diversi criteri a cui devono attenersi i titolari per poter dimostrare, anche qui caso per caso, la validità del ricorso al legittimo interesse come base giuridica dei trattamenti effettuati nell'ambito dell'IA, con particolare riferimento al criterio della legittima aspettativa dell'interessato. Il parere ricorda che non esiste alcuna gerarchia tra le basi giuridiche previste dal RGPD e che spetta ai titolari individuare la base giuridica adeguata per le loro attività di trattamento. Richiama quindi il test in tre fasi che dovrebbe essere condotto nel valutare l'utilizzabilità dell'interesse legittimo come base giuridica, ovvero: 1) identificare l'interesse legittimo perseguito dal titolare o da un terzo; 2) analizzare la necessità del trattamento per perseguire l'interesse legittimo (test di necessità); 3) valutare che sull'interesse legittimo non prevalgano gli interessi, i diritti e le libertà degli interessati (test di bilanciamento).

Riguardo infine alla terza questione, il parere valuta l'impatto della presenza di un trattamento illecito nella fase di sviluppo del modello di IA sui successivi trattamenti relativi alla sua implementazione. Anche in questo caso, l'approccio è casistico e, a seconda delle circostanze, può portare a diverse conseguenze: dall'ordine – da parte delle autorità di protezione dati – di cancellazione dell'intero modello, a misure più morbide che riportino il sistema di IA a liceità.

Dichiarazione sul ruolo delle autorità di protezione dei dati alla luce dell'AI *Act*

Sempre in tema di IA, nella dichiarazione 3/2024 del 16 luglio 2024 il CEPD ha sottolineato la necessità che alle autorità di protezione dei dati personali, con la loro notevole esperienza nella valutazione dell'impatto dell'IA sui diritti fondamentali, sia riconosciuto un ruolo preminente nell'impianto disegnato dall'AI *Act* e che siano designate, in un numero di casi, come *Market Surveillance Authorities* (MSAs), anche al

fine di garantire un migliore coordinamento tra differenti regolatori, assicurando una maggiore certezza giuridica per gli attori interessati e il rafforzamento della supervisione e dell'applicazione sia dell'AI *Act* sia della normativa sulla protezione dei dati. Il Comitato ha in particolare raccomandato che tale designazione avvenga per i sistemi ad alto rischio utilizzati nell'ambito della *law enforcement,* la gestione di confini, l'amministrazione della giustizia e dei processi democratici. Gli Stati membri dovrebbero inoltre considerare la possibilità di designare le autorità di protezione dei dati come MSAs anche per altri sistemi di IA ad alto rischio, suscettibili di avere ripercussioni sulla protezione dei dati. Una volta designate, è auspicabile per il *Board* che tali autorità siano altresì indicate come punto di contatto unico per pubblico e controparti a livello nazionale ed europeo ai sensi dell'art. 70, par. 2, AI *Act*. Inoltre, dovrebbero essere definite chiare procedure per la cooperazione tra MSAs e le altre autorità incaricate di svolgere la supervisione sui sistemi di IA, nonché con riguardo alla cooperazione tra l'Ufficio per l'IA (istituito dall'art. 3, par. 47, dell'AI *Act*), le autorità di protezione dati e il CEPD.

Gruppo di alto livello sull'accesso ai dati per un'efficace attività di contrasto

Nel giugno 2023, la Commissione europea aveva lanciato un Gruppo di alto livello sull'accesso ai dati per un'efficace attività di contrasto, co-presieduto dalla stessa Commissione e dalla presidenza di turno del Consiglio, con l'obiettivo di esplorare le sfide per gli operatori delle forze dell'ordine relativamente all'accesso ai dati e proporre eventuali soluzioni e raccomandazioni. Nel giugno 2024, il Gruppo ha pubblicato 42 raccomandazioni per l'ulteriore sviluppo delle politiche e della legislazione dell'UE allo scopo di migliorare e potenziare l'accesso ai dati per un'efficace attività di contrasto. Le raccomandazioni riguardano "misure di rafforzamento delle capacità", "cooperazione con l'industria e standardizzazione" e "misure legislative" e, in particolare, affrontano tematiche quali la crittografia, la cooperazione con l'industria e tra le forze dell'ordine e la necessità di norme armonizzate sulla conservazione dei dati. Su tali tematiche, il CEPD ha adottato la dichiarazione 5/2024, con cui evidenzia che alcune delle raccomandazioni del Gruppo di alto livello potrebbero causare una grave intrusione nei confronti dei diritti fondamentali, in particolare, quello alla protezione de dati e al rispetto della vita privata e familiare. Per quanto concerne la raccomandazione relativa all'armonizzazione delle norme sulla conservazione dei dati, il Comitato ritiene che un obbligo ampio e generale di conservare i dati in formato elettronico da parte di tutti i fornitori di servizi creerebbe una significativa interferenza con i diritti degli individui. Pertanto, il CEPD si chiede se ciò soddisferebbe i requisiti di necessità e proporzionalità della Carta dei diritti fondamentali dell'UE e della giurisprudenza della CGUE. Riguardo alle raccomandazioni relative alla crittografia, il Comitato fa presente che queste non dovrebbero impedirne l'uso o indebolire l'efficacia della protezione crittografica – come avverrebbe, per esempio, a seguito dell'introduzione di un processo lato *client* che consenta l'accesso remoto ai dati prima che vengano crittografati e inviati su un canale di comunicazione oppure successivamente alla decrittazione effettuata presso il destinatario. Il Comitato evidenzia la necessità di evitare una compromissione della confidenzialità delle comunicazioni anche per garantire che la libertà di espressione e la crescita economica, che dipendono da tecnologie affidabili, siano salvaguardate.

Parere su CSAM

Il CEPD è tornato ad occuparsi della proposta di regolamento della Commissione europea recante norme per prevenire e combattere gli abusi sessuali sui minori. Facendo seguito al parere congiunto CEPD-GEPD sulla proposta, la dichiarazione 1/2024 adottata il 13 febbraio 2024 si concentra su più recenti sviluppi legislativi, in particolare sulla posizione del Parlamento europeo di novembre 2023. Pur accogliendo con favore i numerosi miglioramenti nel testo emendato dal Parlamento UE, non sembrano risolte pienamente le importanti questioni segnalate dal CEPD e dal GEPD relative al

monitoraggio generale e indiscriminato delle comunicazioni private, in particolare in relazione all'emissione degli ordini di rilevamento, i quali, tra l'altro, non si limitano ai materiali pedopornografici (CSAM) già noti alle autorità, nonostante il fatto che le tecnologie utilizzate per rilevare nuovo materiale pedopornografico abbiano dimostrato in passato di avere tassi di errore significativi. Secondo il CEPD andrebbe, pertanto, limitato ulteriormente il rischio che tali ordinanze possano colpire persone che difficilmente saranno coinvolte in reati legati all'abuso sessuale su minori.

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 da diversi anni affidato a rappresentanti del Garante.

- Accesso ai dati finanziari e PSD3. Nella plenaria del 23 maggio è stata adottata la dichiarazione sul pacchetto relativo all'accesso ai dati finanziari e sui servizi di pagamento (PSR) e la revisione della PSD2 (PSD3). Lo *statement* ha l'intento di reagire alle posizioni dei co-legislatori dell'UE sulle proposte, tenendo conto che se da una parte sussiste l'esigenza di garantire una maggiore fruibilità dei servizi finanziari per consentire alle persone una più agevole partecipazione alla vita economica, dall'altra appare essenziale tutelare adeguatamente i dati finanziari, in particolare le operazioni di pagamento, che possono contenere informazioni, anche sensibili, sui diversi ambiti della vita privata degli interessati. La dichiarazione, pur prendendo atto dei profili che nell'*iter* legislativo hanno consentito l'allineamento alle posizioni già espresse dal Comitato nelle linee guida sul rapporto tra PSD2 e RGPD e dal GEPD nei rispettivi pareri, mira a formulare specifiche raccomandazioni perché siano assicurate le dovute garanzie di protezione dei dati nel meccanismo di condivisione dei dati personali tra i diversi attori del settore finanziario a fini di prevenzione delle frodi. Se infatti, come riconosciuto dal cons. 49 RGPD, costituisce un legittimo interesse del titolare del trattamento trattare dati personali strettamente necessari a fini di prevenzione delle frodi, è altresì fondamentale garantire che tali trattamenti siano assistiti da adeguate garanzie e non si rivelino ridondanti ed invasivi.

- Antiriciclaggio e contrasto al finanziamento del terrorismo (AML/CFT). In ambito finanziario è proseguito il lavoro anche sul tema della protezione dei dati nel settore dell'antiriciclaggio (AML) e del contrasto al finanziamento del terrorismo (CFT), con particolare riferimento alle cd. *watchlist*. Tali *database* contengono informazioni sulle attività economico finanziarie di diversi soggetti di cui si avvalgono le cd. *obliged entities*, principalmente enti creditizi e istituti finanziari, per adempiere agli obblighi di monitoraggio dettati dalla normativa AML/CFT. È stato avviato un lavoro di approfondimento anche attraverso questionari interni per raccogliere le informazioni necessarie riguardo alle prassi in tale settore, in vista dell'elaborazione di linee guida.

I settori AML/CFT sono del resto stati oggetti di importanti riforme a livello UE con l'adozione del pacchetto legislativo composto dalla VI direttiva antiriciclaggio (direttiva UE 2024/1640), il reg. *single rulebook* (reg. UE 2024/1624) e il reg. UE 2024/1620 che istituisce una nuova autorità UE, l'AMLA, con poteri di vigilanza in materia di AML/CFT, pubblicato il 19 giugno 2024. In questo contesto, il sottogruppo del Comitato che si occupa di affari finanziari ha più volte incontrato rappresentanti della *European Banking Authority*. L'EBA, nonostante il passaggio delle proprie competenze in materia di AML/CFT alla neo-costituita autorità AMLA con l'entrata in vigore delle nuove norme, proseguirà il proprio mandato fino alla piena operatività di AMLA, anche per assicurare la continuità dell'azione UE in tale settore. Dovrà pertanto essa stessa predisporre proposte per le norme tecniche di regolamentazione che AMLA svilupperà in relazione ad una serie di questioni, in particolare i criteri di individuazione delle

informazioni necessarie alla *customer due diligence*, che hanno un significativo impatto sulla protezione dei dati.

È altresì proseguito il lavoro, infine, che porterà anche in questo caso alla predisposizione di un documento del CEPD sul trattamento dei dati personali effettuato dalle piattaforme di *e-commerce* che impongono agli acquirenti di creare un *account* personale per potere procedere agli acquisti.

21.2. *La cooperazione delle autorità di protezione dati nel settore libertà, giustizia e affari interni*

L'Autorità ha continuato a partecipare attivamente alle riunioni dei gruppi di lavoro in ambito europeo in materia di sicurezza e giustizia.

21.2.1. Comitato di controllo coordinato

Il Comitato di controllo coordinato (CSC) si occupa del coordinamento tra le autorità nazionali di controllo e il GEPD per la supervisione dei sistemi IT su larga scala utilizzati per le attività di cooperazione di polizia e giudiziaria e per la gestione delle frontiere e l'immigrazione.

Nel corso del 2024, si è ampliato ulteriormente il mandato del Comitato. Oltre alle competenze già assegnate al CSC riguardo ai preesistenti sistemi IMI, EUROJUST, EPPO, EUROPOL, SIS, Prüm II, l'attività del Comitato si è estesa ai sistemi informativi VIS, EES ed ETIAS.

Tale ampliamento di competenze del CSC ha comportato un ripensamento dell'organizzazione interna e del metodo di lavoro, specialmente in funzione della prossima operatività dei sistemi EES ed ETIAS di cui si dà conto anche nel prosieguo.

È per tale motivo che il CSC ha condiviso l'opportunità di trattare alcuni temi relativi ai sistemi informativi oggetto di supervisione in modo "specialistico" tramite l'apposita costituzione di *working group*, in modo da poter avere una maggiore efficienza nella loro trattazione, riservando alla plenaria le decisioni più importanti o la trattazione delle questioni più delicate. In merito ai gruppi di lavoro, accanto a quelli al momento già costituiti per i sistemi EES ed ETIAS, dovrebbero in futuro prevedersi dei gruppi specifici per gli altri sistemi e uno di natura orizzontale sull'allocazione dei ruoli di titolare, contitolare e responsabile del trattamento nei sistemi rientranti nel quadro giuridico dell'interoperabilità.

Il CSC ha dedicato specifica attenzione ai temi da inserire nel programma di lavoro per il biennio 2025-2027. Tra le questioni affrontate, meritano di essere menzionate l'analisi dei profili di contitolarità nell'ambito dei trattamenti effettuati tramite sistemi informativi europei su larga scala, la necessità di snellire la procedura per lo svolgimento di ispezioni in modo congiunto (sulla scorta dell'esperienza con verifiche di cui all'art. 36 del reg. SIS) e il tema dell'esercizio dei diritti degli interessati rispetto ai sistemi EES ed ETIAS, *in primis* il diritto di accesso.

21.2.2. EUROJUST

In tema di cooperazione giudiziaria, sono stati predisposti due questionari relativi al Sistema EUROJUST: uno sulle difficoltà nella supervisione da parte delle autorità di controllo e l'altro sulla qualità dei dati nel registro anti-terrorismo (*Counter-Terrorism Register* o CTR). Quanto al primo, alcuni membri del Comitato hanno infatti evidenziato quelle criticità nell'attività di supervisione come derivanti dalle restrizioni imposte dalla normativa di riferimento alle autorità di controllo (cfr., in particolare, l'art. 45 LED e

l'art. 37, comma 6, d.lgs. n. 51/2018). In proposito, si è convenuto di raccogliere informazioni sui principali ostacoli riscontrati dalle autorità al fine di pervenire ad una soluzione condivisa.

Con riguardo invece al registro anti-terrorismo – strumento operativo di supporto delle indagini in materia di terrorismo in quanto consente di trovare i potenziali *match* tra i vari sospettati e di offrire alle autorità nazionali un canale sicuro per comunicare e coordinare i vari procedimenti giudiziari – si è rilevato che, una volta inseriti i dati da parte delle autorità competenti, non viene poi effettuato alcun intervento di aggiornamento per assicurarne la perdurante accuratezza, in ossequio ai principi di minimizzazione ed esattezza dei dati.

La raccolta di informazioni tramite inoltro del questionario sul CTR ai referenti nazionali – per l'Italia, il Procuratore nazionale antimafia e antiterrorismo in conformità a quanto disposto dall'art. 11, comma 2, d.lgs. 23 novembre 2023, n. 182 – non ha sortito i risultati attesi: molti membri del Comitato hanno rappresentato di non aver ricevuto alcun riscontro. È stato comunque deciso di procedere con la redazione di un *report* specifico, prevedendo una particolare voce per quegli Stati membri (fra cui l'Italia) in cui le autorità competenti non hanno fornito le risposte al questionario inoltrato.

21.2.3. EES ed ETIAS

In tema di gestione delle frontiere, asilo e immigrazione, un puntuale approfondimento hanno ricevuto i sistemi informativi *Entry-exit System* (EES) e *European Travel Information and Authorisation System* (ETIAS).

Il Sistema EES, disciplinato dal reg. (UE) 2017/2226 per la registrazione dei movimenti di tutti i cittadini di paesi terzi in entrata e in uscita dallo spazio Schengen che sono ammessi per un soggiorno di breve durata e che sostituisce l'attuale apposizione manuale di timbri sui passaporti, è stato oggetto di primaria attenzione da parte del Comitato, in vista, come già accennato, dell'imminente sua operatività, originariamente prevista per il 2024, ma poi posticipata al 2025.

Per un'analisi degli aspetti più problematici, il Comitato ha seguito il progetto dell'Agenzia europea per i diritti fondamentali (*Fundamental Rights Agency*, FRA) relativo all'impatto del Sistema EES sui diritti fondamentali, che ha riguardato l'analisi di sei Stati membri, inclusa l'Italia e rispetto al quale l'Autorità ha fornito il proprio contributo. Le conclusioni preliminari dello studio sono state presentate nel corso di una tavola rotonda organizzata dall'Agenzia insieme a rappresentanti della Commissione, FRONTEX e del GEPD, nel corso della quale sono stati presentati i due documenti relativi a buone e cattive prassi (*do's and dont's*) sia per le guardie di frontiera che per le autorità competenti in merito all'applicazione del Sistema EES. La pubblicazione del *report* comparativo finale è prevista nel corso del 2025.

Tra gli ulteriori temi all'attenzione del Comitato con riguardo ad EES, si annovera l'obbligo previsto dall'art. 51 del reg. EES sulla campagna informativa, con riferimento alla quale il GEPD e le autorità di supervisione nazionali non hanno ricevuto alcun materiale, né sono state consultate e coinvolte dalla Commissione. Pur prendendo nota delle informazioni fornite da quest'ultima in sede di specifiche interlocuzioni, in particolare con riguardo alla decisione di esecuzione della Commissione del 28 luglio 2022, n. 2022/1337, che stabilisce il modello per fornire informazioni ai cittadini di paesi terzi sul trattamento dei dati personali nel sistema di ingressi/uscite, che deve essere completato dai singoli Stati membri, con tutte le informazioni rilevanti, inclusi i contatti dell'autorità di controllo nazionale e del responsabile per la protezione dei dati, il Comitato ha inviato una seconda lettera alla Commissione al fine di ribadire l'assenza

di coinvolgimento del GEPD e delle autorità nazionali di supervisione in detta attività di informazione, in contrasto con quanto disposto dall'art. 51 del reg. EES, compendiando tutti gli aspetti critici rilevati. Nel frattempo il gruppo di lavoro su EES sta valutando la redazione di un testo informativo per il pubblico relativo agli aspetti sulla protezione dei dati personali connessi al funzionamento di EES al fine di uniformare le informazioni rese dalle singole autorità di supervisione sui propri siti web.

Un ulteriore profilo di approfondimento ha riguardato le *app* connesse al funzionamento del Sistema EES, sia a livello europeo che a livello nazionale. Nello specifico, è stato chiarito che il prototipo dell'*app* (4EES) è stato messo a punto da FRONTEX su incarico della Commissione europea, come *back-end*, ed è stato reso disponibile agli Stati membri per sviluppare il *front-end*, secondo le proprie esigenze. La creazione dell'*app* si iscrive nell'ambito del progetto *Travel to Europe* e l'*app* è uno strumento di pre-registrazione dei dati tramite il sistema nazionale sul *database* EES. L'utilizzo su base volontaria dell'*app* da parte dei passeggeri stranieri (non-UE o non-Schengen) con passaporto biometrico consente di registrare l'immagine del viso, i dati del passaporto e le risposte al questionario sulle condizioni di ingresso. È stato portato a termine un progetto pilota nell'agosto 2024 presso due aeroporti: uno in Svezia e uno nei Paesi Bassi. L'*app* può considerarsi un sistema *self service* in cui non si registrano le impronte digitali (anche se questo aspetto potrà eventualmente essere aggiunto in una fase successiva).

Con riferimento ad ETIAS – introdotto dal reg. (UE) 2018/1240, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi per i cittadini di paesi terzi esenti dall'obbligo di visto per entrare in Europa – l'attività del CSC è stata altrettanto intensa. In particolare, si è rilevato che l'entrata in funzione del sistema è condizionata alla piena operatività di EES e che il quadro giuridico non è ancora del tutto allineato con la disciplina sulla protezione dei dati personali, rendendosi necessario analizzare problemi comuni. A tal fine sono stati istituiti diversi gruppi di lavoro, a cui partecipano alcuni membri del Comitato e che periodicamente riportano al CSC l'esito delle discussioni. A titolo esemplificativo, può citarsi il cd. *Inter-agency* ETIAS *Technical Expert Group on* DPIAs, sulle valutazioni di impatto da condurre a livello centrale e a livello nazionale, in cui sono affrontati, tra gli altri temi, anche la titolarità del trattamento, la metodologia per la valutazione dei rischi e l'individuazione delle misure per mitigarli, la sicurezza dei dati, le funzionalità addizionali per mezzo dell'IA (es. *chat-bot*).

Il Comitato ha altresì inviato alla Commissione – specularmente ad analoga iniziativa del GEPD – una lettera riguardante alcuni aspetti critici relativi all'attuazione del reg. ETIAS, tra cui l'individuazione della disciplina applicabile (RGPD o LED) all'esercizio dei diritti dell'interessato sulla base degli artt. 56 e 64 del reg. ETIAS; la necessità di chiarezza circa l'obbligo di condurre una valutazione d'impatto; le regole di procedura del cd. ETIAS *Screening Board* (cfr. art. 9 reg. ETIAS) al fine di garantire la partecipazione piena alle sue riunioni cd. ETIAS *Fundamental Rights Guidance Board* o EFRGB di cui fa parte il CEPD.

Inoltre, specifica attenzione ha ricevuto l'aggiornamento dei membri del Comitato rispetto all'attività dei rappresentanti del CEPD in seno all'EFRGB, organo indipendente con competenze consultive in materia di diritti fondamentali previsto e disciplinato dall'art. 10 del reg. ETIAS. In particolare, i membri del CSC sono stati informati rispetto ai temi oggetto di discussione in seno all'EFRGB, quali i rischi di discriminazione e il diritto ad un rimedio effettivo, l'utilizzo dei dati per altre finalità e in particolare l'accesso da parte delle autorità di *law enforcement*.

Più in generale, lo studio e l'approfondimento delle questioni ermeneutiche legate al-

l'implementazione del Sistema ETIAS costituiscono l'attività principale del *working group* costituito *ad hoc* in seno al CSC in attuazione del nuovo metodo di lavoro. Tra i temi affrontati può citarsi, a titolo esemplificativo, la questione relativa all'istituzione di un canale comune e sicuro di comunicazione per l'inoltro delle decisioni tra le unità nazionali ETIAS e le autorità di supervisione, da rendersi disponibili a richiesta delle autorità di controllo entro sette giorni (cfr. art. 64, par. 6, reg. ETIAS). Un'altra criticità emersa nell'ambito del gruppo di lavoro sulla valutazione d'impatto per ETIAS, ma con rilevanza generale, su cui è stata avviata una riflessione nell'ambito del gruppo di lavoro e poi del Comitato, riguarda le informazioni che i titolari del trattamento del Sistema ETIAS devono fornire all'interessato con riferimento a una richiesta di accesso ai dati, in considerazione dell'interpretazione della nozione di "destinatario" dei dati ai sensi dell'art. 4, par. 9, RGPD.

21.2.4. EURODAC

Con riferimento al Sistema informativo EURODAC – che si prevede in futuro venga anch'esso ricompreso nell'attività di supervisione del CSC – il Gruppo di supervisione ha approfondito, anche con la partecipazione di alcuni rappresentanti della Commissione, le novità normative introdotte.

In primo luogo, è stato esaminato il nuovo reg. EURODAC 1358/2024, che entrerà in vigore il 12 giugno 2025 e che è stato introdotto per assicurare coerenza con la regolamentazione in materia di asilo e immigrazione (es. proposta di reg. sulla gestione dell'asilo e della migrazione; direttiva sulla protezione temporanea; reg. sul reinsediamento e l'ammissione umanitaria, ecc.), ma anche per garantire l'interoperabilità del Sistema EURODAC con gli altri sistemi informativi di larga scala (quali SIS e VIS).

Tra gli aspetti innovativi, si segnalano: i) nuove regole sull'obbligo di raccogliere dati biometrici (come i dati relativi alle impronte digitali o al volto) tra cui la necessità a livello nazionale di adottare misure amministrative per garantirne il rispetto, inclusa la possibilità di ricorrere a mezzi di coercizione come *ultima ratio*; ii) regole specifiche relative ai minori (la cui età è stata abbassata da 14 a 6 anni per la raccolta dei dati biometrici); iii) la possibilità di collegare gli interessati ai *set* di dati registrati nel *database*; iv) l'ampliamento delle categorie di interessati soggetti a registrazione e dei dati raccolti; v) l'introduzione di *security flags*, nel caso di soggetti che possono porre una minaccia per la sicurezza interna.

Di particolare interesse per il Gruppo di supervisione è stata la questione concernente il rapporto tra il nuovo reg. EURODAC e il reg. 1356/2024 che introduce accertamenti nei confronti dei cittadini di paesi terzi alle frontiere esterne (cd. *Screening Regulation*). Quest'ultimo si applica a 26 Stati membri (in aggiunta a: Svizzera, Liechtenstein, Islanda e Norvegia, con l'esclusione di Irlanda e Cipro per alcuni aspetti) e prevede accertamenti nei confronti dei cittadini di paesi terzi che "senza soddisfare le condizioni d'ingresso di cui all'art. 6 del reg. (UE) 2016/399, hanno attraversato la frontiera esterna in modo non autorizzato, hanno presentato domanda di protezione internazionale durante le verifiche di frontiera o sono sbarcati a seguito di un'operazione di ricerca e soccorso, prima che siano indirizzati alla procedura adeguata" oppure "soggiornano illegalmente nel territorio degli Stati membri se non vi sono indicazioni che tali cittadini di paesi terzi siano stati sottoposti a controlli alle frontiere esterne, prima che siano indirizzati alla procedura adeguata". Per quanto di rilievo rispetto alla protezione dei dati personali, sono stati esaminati in modo specifico gli artt. 14-16 relativi ai controlli sull'identità e sulla sicurezza.

Il Gruppo di supervisione ha esaminato anche i temi da inserire nel programma di lavoro 2025-2027. Tra quelli proposti, si possono ricordare: il problema dei cd. falsi

positivi (*false hits*), una raccolta di buone prassi per le ispezioni a livello nazionale, un approfondimento sull'esercizio del diritto di accesso ai dati da parte degli interessati. Infine, è stato approvato il documento contenente la *checklist* per monitorare l'accesso da parte delle autorità nazionali di *law enforcement* al Sistema EURODAC e sono state condivise alcune esperienze nazionali in merito alle ispezioni e audit condotti dalle autorità di supervisione.

21.2.5. Sistema d'informazione Schengen (SIS)

Relativamente al SIS, diversi sono stati i temi di interesse esaminati nell'ambito dei lavori del CSC. Riguardo agli esiti del questionario sugli *alert* inseriti in SIS, ai sensi dell'art. 36 della decisione 2007/533/GAI (ora reg. (UE) 2018/1862), concernenti la cd. sorveglianza discreta (attivata ed utilizzata normalmente all'insaputa dell'interessato), i relatori hanno presentato il contesto e lo stato dell'arte dei riscontri forniti dagli Stati membri, evidenziando gli aspetti problematici e le possibili attività future, alla luce del duplice obiettivo perseguito attraverso la somministrazione del questionario: da un lato, la raccolta di informazioni e statistiche più specifiche sull'uso delle segnalazioni ai sensi dell'art. 36 da parte delle autorità competenti; dall'altro, data la natura di tali segnalazioni, una indispensabile attività di valutazione della legittimità, delle condizioni di inserimento e mantenimento di tali segnalazioni nel SISII da parte delle autorità di protezione dei dati.

È stato presentato e discusso il *report* sulla gestione dell'esercizio del diritto di accesso da parte degli interessati rispetto a quanto previsto agli artt. 54 e 57, par. 4, reg. 2018/1861, con particolare riguardo alle statistiche che gli Stati membri devono fornire in merito annualmente. Con riferimento agli esiti di detta attività (cfr. par. 8.5.2), è stato evidenziato il mancato invio di tali statistiche in alcuni Stati membri, principalmente per un difetto di collaborazione con le rispettive autorità di polizia. È stato inoltre fornito un aggiornamento sulle attività di audit svolte dalle DPA ogni quattro anni.

Infine, il GEPD ha riferito circa il *report* sull'*audit* che ha effettuato nel corso del 2023 sul Sistema SIS ed il cui rapporto è stato inviato ai membri del Comitato il 19 settembre 2024.

21.2.6. Sistema d'informazione EUROPOL

Relativamente al Sistema EUROPOL, in ordine ai risultati contenuti nel *report* relativo all'attività di *audit* del 2022, il GEPD ha messo in evidenza l'accesso di EUROPOL ai dati PNR per il tramite delle PIUs (*Passenger Information Units*), per lo svolgimento di eventuali attività di investigazione e di identificazione di potenziali "sospetti" o "vittime".

In merito alle linee guida sulla cooperazione tra il GEPD e le autorità nazionali nella gestione dei reclami relativi a EUROPOL, si è ribadito che si tratta di un obbligo che discende dal RGPD e che è ragionevole eventualmente prevedere da parte del GEPD la possibilità di avere informazioni più dettagliate da EUROPOL prima di inviare in via formale la richiesta alle autorità nazionali.

Quanto alle attività di supervisione congiunte e relative ai dati di minori (*under* 15) trattati da EUROPOL, da un'analisi preliminare delle risposte pervenute al relativo questionario fatto circolare fra i 21 Stati interessati è emersa una certa omogeneità. I maggiori problemi riguardano: la conservazione dei dati, la strumentalizzazione dei minori, gli errori di classificazione (es. rispetto a contesti familiari di tipo criminale) e le modalità di verifica dell'età.

Infine, si segnala che il GEPD ha informato il CSC in merito alle priorità di supervisione indicate dal Parlamento europeo attraverso l'EUROPOL *Joint Parliamentary Scrutiny Group* (tra cui l'utilizzo sempre più frequente della cd. *joint operational analysis*

da parte degli Stati membri e il trattamento dei dati biometrici) e all'elaborazione di una formula "neutra" per fornire risposte agli interessati che presentino richieste di accesso al fine di evitare la rivelazione di informazioni sull'esistenza di indagini in corso che li riguardino (sul punto, il CSC dovrà esprimersi attraverso un'apposita consultazione).

21.2.7. Sistema d'informazione Prüm II

Per quanto concerne il cd. Prüm II *Regulation*, il CSC ha invitato un rappresentante della Commissione per la presentazione del nuovo *Prüm Framework*, al fine di prenderne visione ed avviare una prima riflessione sul tema.

21.3. *La partecipazione dell'Autorità in seno al Consiglio d'Europa, all'OCSE e ad altri gruppi di lavoro internazionali*

G7 DPA

Il 2024 è stato caratterizzato dall'intensa attività del Garante per l'organizzazione della quarta Tavola rotonda delle autorità di protezione dei dati G7 che si è svolta a Roma dal 9 all'11 ottobre 2024. Vi hanno partecipato il Collegio del Garante e le autorità competenti di Canada, Francia, Germania, Giappone, Regno Unito e Stati Uniti d'America, insieme al CEPD e al GEPD, oltre a rappresentanti di alcune importanti organizzazioni internazionali (OCSE, Consiglio d'Europa).

Al centro delle discussioni del 2024 vi erano alcune delle sfide più urgenti nel mondo della *data protection*. Basandosi sugli esiti dei precedenti incontri, le DPA del G7 si sono concentrate su tre aree principali: *Data Free Flow with Trust* (DFFT), le implicazioni delle tecnologie emergenti, e la cooperazione in materia di attuazione delle norme in materia di dati personali. In questo contesto, le G7 DPA hanno prestato molta attenzione allo sviluppo etico e affidabile dell'IA, un tema che continua ad accendere il dibattito sulla scena globale. In particolare, con l'invito alla prosecuzione del dialogo, le autorità hanno richiesto garanzie adeguate per i minori nello sviluppo e nell'uso dell'IA, una tecnologia che deve essere progettata in modo da assicurare la loro crescita libera e armoniosa. Pertanto, le DPA hanno adottato una "dichiarazione sull'intelligenza artificiale e i minori" chiedendo un'azione urgente per salvaguardare la *privacy* dei minori. Su questo tema, affrontato anche nell'ambito della riflessione sulle tecnologie emergenti, i Garanti hanno ribadito l'esigenza che la progettazione di tali tecnologie, ancor prima dell'uso, sia tale da porle davvero al servizio dell'uomo.

Nel corso del dibattito è stata poi sottolineata la necessità di adottare politiche sull'innovazione che comprendano anche un'adeguata educazione digitale, fondamentale per la formazione soprattutto dei minori. Il ruolo delle autorità nella regolamentazione dell'IA è stato ritenuto determinate proprio al fine di garantirne l'affidabilità. È stato, infatti, sottolineato come esse dispongano di competenze, oltre che dell'indipendenza necessarie ad assicurare garanzie indispensabili per governare un fenomeno così complesso. Si è, pertanto, concordato sull'opportunità di esprimere ai Governi l'auspicio del riconoscimento di un ruolo adeguato alle autorità di protezione dei dati nel sistema complessivo di *governance* dell'IA. In tale contesto, è stata adottata una dichiarazione che evidenzia il ruolo cruciale delle autorità di protezione dei dati nel garantire che le tecnologie di IA siano affidabili e vengano utilizzate in modo responsabile ("dichiarazione sul ruolo delle autorità di protezione dei dati nel promuovere un'intelligenza artificiale affidabile"). Tale dichiarazione sottolinea l'importanza di allineare lo sviluppo dell'IA alle norme e ai principi esistenti in materia di protezione dei dati. I Garanti, inoltre, hanno deciso di svolgere un monitoraggio sugli sviluppi legislativi dell'IA e il ruolo delle autorità *privacy* all'interno delle rispettive giurisdizioni.

Sul fronte della cooperazione globale le G7 DPA hanno pubblicato un comunicato in cui sottolineano l'importanza di 19 solidi meccanismi di trasferimento transfrontaliero dei dati che proteggano i dati personali. Guardando al futuro, è stato adottato il Piano d'azione 2024/2025 ossia il documento che guarda al futuro del G7 stabilendone i propositi e le aree tematiche che saranno oggetto dei lavori del prossimo anno. È stato ribadito l'impegno a concentrarsi sul DFFT, sulle tecnologie emergenti e sulla cooperazione in materia di applicazione delle norme, come delineato nel comunicato del 2024 parimenti adottato a Roma.

Tutti i documenti sopra menzionati e altri che sono stati approvati nel corso della riunione di Roma sono disponibili sul sito dell'Autorità (G7 dei Garanti *privacy* - 2024, Roma - Garante *Privacy*). Da tali documenti emerge concretamente l'importanza delle autorità di protezione dei dati e la loro capacità di garantire che lo sviluppo digitale sia sempre ispirato alla tutela, anche etica, delle persone e dei diritti legati al loro essere persone dotate di diritti e doveri derivanti dalle radici bimillenarie della cultura che è alla base dei diritti fondamentali dell'UE e delle Carte costituzionali. A conclusione dell'evento i Garanti si sono dati appuntamento al G7 *Privacy* 2025 che sarà ospitato dall'autorità canadese dal 17 al 19 giugno 2025.

- Comitato consultivo della Convenzione 108/1981 (T-PD). Il Comitato, composto da 55 Parti, si è riunito due volte in plenaria (5-7 giugno e 4-6 novembre 2024) e due volte nella sua composizione ristretta (cd. T-PD *Bureau*, 13-15 marzo e 11-13 settembre 2024).

Nella plenaria di novembre si sono tenute le elezioni per il ruolo di presidente, vice presidente e componenti del *Bureau*. Le elezioni sono state caratterizzate da un buon numero di candidati, segno positivo dell'attenzione crescente rivolta da diverse delegazioni alle attività del Comitato. La rappresentante del Garante, avendo esaurito il numero massimo di (tre) mandati in qualità di presidente, ha potuto presentare la candidatura per il posto di componente del *Bureau*, ottenuto all'esito dell'elezione. L'elezione della rappresentante argentina nel ruolo di *Chair*, unitamente ai componenti del *Bureau* provenienti da paesi europei (Italia, Croazia, Finlandia, Germania e Svizzera), America latina (Uruguay) e Africa (Senegal) rispecchia, anche nella composizione geografica del Comitato, la vocazione globale della Convenzione 108.

- La Convenzione 108+. Anche il 2024 è stato contrassegnato da un intenso impegno del Comitato consultivo rivolto alla promozione del Protocollo emendativo della Convenzione 108, che, adottato già nel 2018 al fine di modernizzare il trattato originario in modo da rispondere alle molte sfide per la protezione dei dati provenienti dal mutato scenario tecnologico e globale, necessita di un considerevole numero di ratifiche (trentotto) per poter entrare in vigore. Ratificato finora da trentuno Parti, l'auspicio del Comitato e del segretariato del Consiglio d'Europa è di ottenere in tempi brevi le restanti sette ratifiche, che garantirebbero la piena realizzazione di uno strumento internazionale particolarmente rilevante, dalla portata globale, in quanto aperto all'accessione anche di paesi che non sono parte del Consiglio d'Europa.

Avvicinandosi verosimilmente il momento dell'entrata in vigore della Convenzione modernizzata, il Comitato è tornato a discutere dei meccanismi di monitoraggio introdotti dalla Convenzione 108+ (*evaluation and review mechanism*).

I meccanismi di valutazione dei paesi che intenderanno accedere alla Convenzione modernizzata e di rivalutazione di quelli che saranno già Parti, previsti dalla 108+, modificheranno sensibilmente il lavoro del futuro Comitato convenzionale rispetto a quello attuale, ampliandone notevolmente l'attività e ponendo dunque un problema importante di reperimento di risorse. L'auspicio è che il Comitato e il suo segretariato possano essere dotati delle risorse necessarie a svolgere a pieno le attività previste,

finalizzate, tra l'altro, a rafforzare la credibilità della Convenzione e l'effettiva implementazione dei suoi principi da parte degli Stati. Del resto, il testo della Convenzione modernizzata viene già utilizzata dal Comitato consultivo come parametro normativo di riferimento nell'elaborazione dei documenti, in particolare linee guida, sulla protezione dei dati in diversi settori.

- Linee guida sui trattamenti di dati nel contesto elettorale. Il 7 giugno 2024 sono state adottate dal Comitato le linee guida sui trattamenti di dati personali nel contesto elettorale contenenti raccomandazioni per i titolari del trattamento affinché registrazione e autenticazione finalizzate all'esercizio del diritto di voto siano svolte nel pieno rispetto della protezione dei dati e della loro confidenzialità. Particolare attenzione è dedicata alle specifiche salvaguardie che devono assistere i trattamenti di categorie speciali di dati (art. 6 della Convenzione 108+), inclusi i dati biometrici, sempre più spesso adoperati in diversi paesi per l'autenticazione degli elettori.

- Clausole contrattuali per il trasferimento dei dati verso paesi terzi. È proseguito il lavoro del Comitato per la stesura di modelli di clausole contrattuali per il trasferimento di dati verso paesi terzi (che non sono Parti cioè della Convenzione 108) di cui i titolari del trattamento potranno avvalersi, in base all'art. 14, par. 2, lett. b), della Convenzione modernizzata per garantire un livello appropriato di protezione. In particolare, il Comitato ha adottato un modello di clausole per il trasferimento di dati tra responsabili del trattamento (*processor to processor*), in linea di continuità con i modelli di clausole già adottati nel 2023 per il trasferimento dei dati tra titolari (*controller to controller)* e da titolare a responsabile (*controller to processor*).

Si è così completato un lavoro particolarmente significativo per l'attuazione dei principi della Convenzione modernizzata.

- Neurotecnologie. Attraverso un *report* realizzato da due esperti scientifici, disponibile *online* sul sito web del Comitato, sono state esaminate le sfide etiche e giuridiche e le opzioni di *policy* in tale ambito. Il rapporto, pur non escludendo per il futuro l'opportunità che le sfide per i diritti fondamentali lanciate dalle neurotecnologie siano affrontate anche attraverso nuovi strumenti giuridici, sottolinea come l'impianto esistente dei diritti fondamentali (si pensi agli artt. 3 e 8 della Convenzione europea dei diritti dell'uomo capaci di racchiudere la tutela dell'integrità e della *privacy* mentale) sia cruciale per proteggere le persone e che, con particolare riferimento alla protezione dei dati, la Convenzione 108+ offre già importanti norme di tutela.

Tra i punti di discussione affrontati dal Comitato, anche in vista dell'elaborazione delle linee guida che seguiranno, si segnalano in particolare se e in quale misura i cd. *neural data* debbano considerarsi dati sensibili ai sensi dell'art. 6 della Convenzione 108+, godendo così della protezione rafforzata offerta da tale norma; quanto il consenso dell'interessato possa costituire l'appropriata base giuridica per il trattamento dei dati degli interessati; dove collocare eventuali divieti rispetto a impieghi delle neurotecnologie che risultino eccessivamente invasivi specialmente se concernenti soggetti vulnerabili quali i minori; la necessità di approfondire l'applicazione dei principi della Convenzione 108+, in particolare in materia di decisioni automatizzate, di correttezza del trattamento e minimizzazione dei dati.

- Linee guida sull'art. 11 della Convenzione 108+. Il Comitato ha proseguito il lavoro di interpretazione dell'art. 11 della Convenzione 108+ dedicato alle eccezioni e limitazioni di alcuni principi della Convenzione stessa in specifici settori quali la sicurezza nazionale e l'accertamento e il perseguimento dei reati.

Le linee guida, una volta completate, rappresenteranno uno strumento interpretativo particolarmente significativo per le Parti che intendano ratificare la 108+ perché forniscono indicazioni, supportate dalla cospicua giurisprudenza della Corte europea

dei diritti dell'uomo, sui requisiti ai quali le normative nazionali devono attenersi nella previsione di eccezioni ai principi della Convenzione – eccezioni che, in via primaria, devono essere previste per legge, proporzionate, necessarie al perseguimento degli specifici interessi elencati dall'art. 11 stesso e rispettose dell'essenza dei diritti fondamentali tutelati dalla Convenzione.

- Premio Rodotà. Anche nel 2024 è stato conferito il Premio alla memoria di Stefano Rodotà, insigne giurista e primo Presidente del Garante italiano. I due vincitori, Konrad Kollnig e Lin Kyi, rispettivamente per la miglior tesi di dottorato (sul potere delle piattaforme nell'economia delle *app*) e miglior saggio (sulle *policy*, spesso poco trasparenti, dei siti web con riferimento al ricorso al legittimo interesse come base giuridica del trattamento), hanno presentato il loro lavoro, interloquito con il Comitato nel corso della plenaria e ricevuto il premio del Consiglio d'Europa.

- CAI - Comitato *ad hoc* sull'IA**.** L'Autorità ha continuato a seguire, attraverso un proprio rappresentante, anche l'attività del Comitato *ad hoc* sull'IA (CAI) che ha portato a termine il lavoro di preparazione della Convenzione quadro in materia di IA, diritti umani, democrazia e Stato di diritto adottata dal Comitato dei Ministri a Vilnius il 5 ottobre 2024 (cfr. cap. 16).

- CDDEM - *Steering Committee on Democracy*. L'Autorità ha partecipato anche alle attività della neo-costituita *Steering Committee on Democracy* (CDDEM), nata a seguito dell'impegno dei Capi di Stato e di Governo del Consiglio d'Europa al loro quarto vertice di Reykjavik nel 2023 per garantire e rafforzare la democrazia.

OCSE – DGP *(Working Party on Policies for Digital Data Governance and Privacy)*

È proseguita l'attività dell'Autorità in ambito OCSE, in particolare attraverso la partecipazione al DGP (*Working Party on Data Governance and Privacy)*, di cui una rappresentante del Garante è membro in qualità di Vice*Chair* dal 2012 (già nel WPSPDE - *Working Party on Security and Privacy in Digital Economy)* ed ha conservato la vicepresidenza per il 2025 (confermata nelle elezioni della plenaria DGP di novembre 2024).

Le due riunioni plenarie del DGP (27 e 28 giugno e 6 e 7 novembre), cui si sono come di consueto aggiunte tre riunioni del *Bureau*, il gruppo ristretto del *Board*, sono state anche per il 2024 caratterizzate da un'altissima partecipazione delle delegazioni dei paesi membri.

-Intelligenza Artificiale. Nel corso del 2024, il Gruppo si è confrontato sui recenti progressi tecnologici dell'IA, in particolare l'ascesa dell'IA generativa, che hanno sollevato molte preoccupazioni per la *governance* dei dati e la *privacy.* L'approccio a questi problemi spesso varia a seconda delle giurisdizioni e dei sistemi legali e ciò ha sollevato nuove domande sull'intersezione tra la *governance* dei dati dell'IA e la *privacy*. In particolare, è emerso che ulteriori sforzi di cooperazione internazionale sono necessari per aumentare la consapevolezza sulla portata delle regole di protezione dei dati nell'IA e per raggiungere una comprensione condivisa e una coerente attuazione. A tal fine si è convenuto sulla necessità di un lavoro in costante sinergia con tutta la comunità dell'OCSE che si occupa di IA.

In proposito, si evidenzia che nel 2024 l'OCSE si è concentrata sul tema dell'IA da più angolature e sotto la spinta di diversi Comitati, tra cui il Comitato per le politiche digitali (DPC) che dispone di un Gruppo di lavoro sulla *governance* dell'IA (AIGO).

La necessità di un lavoro sinergico è emersa anche alla luce degli esiti della riunione del Consiglio ministeriale dell'OCSE del 2024 (MCM) che ha adottato le revisioni dei principi fondamentali dell'OCSE sull'IA. In risposta ai recenti sviluppi delle tecnologie di IA, in particolare all'emergere dell'IA generativa, i principi aggiornati affrontano più direttamente le sfide associate all'IA che coinvolgono la *privacy*, i diritti di proprietà intellettuale, la sicurezza e l'integrità delle informazioni.

21

Partendo da tali premesse, il DGP ha contribuito al lavoro del Gruppo di esperti IA, dati e *privacy* (v. *infra*) che è sfociato nella elaborazione di un "*Report* su AI, dati e *privacy*: sinergie e aree di interesse internazionale" che mira ad identificare le aree prioritarie di necessaria cooperazione, partendo dalla premessa che, nonostante le sfide, gli sviluppi tecnologici e normativi dell'IA permangono compatibili con le norme sulla *privacy* e sulla protezione dei dati personali.

- *Report* analitico sul flusso libero dei dati con fiducia *(data free flow with trust* – DFFT) - L'OCSE ha creato nel 2024 una Comunità di esperti di *data flows* (DFFT *Community*) per sostenere il processo di creazione di fiducia sui dati e sul loro utilizzo oltre confine. Questa nuova Comunità riunisce esperti provenienti da governi, mondo accademico, società civile, imprese e organizzazioni internazionali per fornire supporto tecnico al lavoro orientato alle politiche del Comitato per le politiche digitali (DPC) dell'OCSE e del DGP. La Comunità ha iniziato a lavorare nel 2024 su tre principali progetti: pagamenti transfrontalieri; rafforzamento della trasparenza legale tra le regole; PETs (*Privacy Enhancing Technologies*).

Il progetto relativo ai pagamenti transfrontalieri supporta il lavoro del Comitato per la politica digitale dell'OCSE e del DGP, mappando l'interazione tra la *governance* dei dati e le leggi sulla *privacy* e le normative finanziarie nel contesto dei pagamenti transfrontalieri. L'obiettivo è migliorare la comprensione da parte delle autorità di protezione dei dati del funzionamento e delle sfide di conformità di questo settore. Il progetto relativo al "rafforzamento della trasparenza legale tra le regole" mira a condurre una serie di consultazioni per fornire *input* al Comitato per la politica digitale dell'OCSE e al DGP in merito a potenziali approcci per migliorare i loro sforzi politici nel creare fiducia nei dati e nei flussi di dati. Il Progetto sulle PETs, concentrandosi sui principali casi d'uso delle PETs in contesti transfrontalieri, mira a fornire elementi concreti sulle opportunità e sui limiti delle PETs nel facilitare il DFFT, in particolare analizzando in che misura l'uso delle PETs possa integrare gli strumenti giuridici e organizzativi esistenti per proteggere i diritti e gli interessi delle parti interessate, compresa la *privacy* e la protezione dei dati. Tutto il lavoro della *Community* DFFT è stato pensato anche in coerenza con quanto sul medesimo tema ha affrontato nel 2024 il G7 delle DPA, per il quale v. *supra.*

- Neurotecnologie. Nel 2024 il DGP ha affrontato il tema della neurotecnologia, partendo dall'analisi del contenuto della raccomandazione sull'innovazione responsabile nelle neurotecnologie, adottata dal Consiglio dell'OCSE l'11 dicembre 2019 su proposta del Comitato per la politica scientifica e tecnologica (CSTP). La raccomandazione rappresenta il primo *standard* internazionale di settore e mira a guidare i governi e gli innovatori ad anticipare e affrontare le sfide etiche, legali e sociali sollevate dalle nuove neurotecnologie, promuovendo al contempo la necessaria innovazione. Anche sulla base di contributi conoscitivi forniti da esperti e autorità di protezione dati nel corso dell'anno, il DGP ha deciso di portare avanti un lavoro congiunto con il Gruppo di lavoro sulle biotecnologie, le nanotecnologie e le tecnologie convergenti dell'OCSE (BNCT/CSTP). Dalla discussione è emersa una particolare attenzione alla natura transfrontaliera delle neurotecnologie e alla relativa necessità di politiche che promuovano la cooperazione internazionale sul tema a fronte di una rapida evoluzione tecnologica e di un panorama geopolitico in continuo cambiamento al fine ultimo di sviluppare standard per governare l'innovazione neurotecnologica in linea con i principi condivisi di *data protection*.

- *Privacy* e concorrenza. Nel corso del 2024 è proseguita la discussione sul tema della correlazione tra *privacy* e concorrenza. Il DGP ha preso atto dei principali risultati della tavola rotonda congiunta su dati, *privacy* e concorrenza tenutasi il 13 giugno 2024 durante la settimana della concorrenza dell'OCSE, per la quale il Segretariato del DGP aveva preparato un documento di lavoro congiuntamente con il Segretariato del

Comitato concorrenza. Il Gruppo, partendo dalle diverse esperienze nazionali, ha analizzato l'impatto dei dati dei consumatori sulla concorrenza nei mercati *online*, che dovrebbe teoricamente portare a risultati migliori per i consumatori in termini di livelli più elevati di *privacy* e di controllo dei dati; tuttavia, ciò non sempre si verifica, soprattutto quando i consumatori non gestiscono o non possono gestire attivamente le proprie opzioni in materia di protezione dei dati. È stata condivisa la necessità di proseguire in questo lavoro al fine di valutare come migliorare la cooperazione tra le autorità garanti in materia di concorrenza e quelle garanti della *privacy* e protezione dei dati. Occorre riflettere su un equo bilanciamento tra *privacy* e concorrenza e il DGP è intenzionato a proseguire in tale riflessione anche nel corso del 2025.

- Accesso affidabile dei governi ai dati dei privati. Altro tema permanente nel corso di tutto il 2024 è stato quello della promozione ed attuazione della dichiarazione OCSE sull'accesso affidabile dei governi ai dati detenuti dai privati (*trusted government access to data*) adottata alla ministeriale OCSE di Gran Canaria nel mese di dicembre 2022. La dichiarazione parte dalla constatazione che i flussi transfrontalieri di dati sono parte integrante dell'economia digitale globale e passaggio inevitabile per cogliere appieno i vantaggi della digitalizzazione. Nelle plenarie del 2024 il DGP ha preso atto dei progressi compiuti attraverso la dichiarazione e del fatto che la comunità internazionale per la protezione dei dati ha cominciato ad impegnarsi e fornire *feedback* sull'attuazione della stessa, anche se molto resta da fare per conseguire vantaggi pratici in quanto la dichiarazione non stabilisce ulteriori passi concreti ai fini della sua attuazione. Anche nel contesto della G7 DPA *Roundtable* di Roma (v. *supra*) le autorità dei sette paesi G7 hanno ribadito l'importanza della dichiarazione ed espresso l'impegno alla massima promozione della stessa, avendo in mente i sette principi comuni della dichiarazione che rappresentano una solida e condivisa base globale per un efficace lavoro di attuazione.

OCSE: Gruppo di esperti OCSE su IA, dati e *privacy*

Il 2024 ha visto l'avvio del lavoro del neo-costituito Gruppo di esperti dell'OCSE su IA, dati e *privacy* di cui il Garante è parte (cfr. cap. 16). Il Gruppo di lavoro si caratterizza per riunire in uno stesso forum le diverse *expertise* in materia di *privacy* e *data protection* nonché nel settore dell'IA al fine di effettuare approfondimenti sulle aree di intersezione tra i due ambiti e fornire *output* sulle scelte di *policy* da adottare in chiave prospettica e all'interno della cornice sovranazionale. Il Gruppo in collaborazione con il DGP (v. *supra*) ha elaborato il *Report* su "AI, dati e *privacy*: sinergie e aree di interesse internazionale". Il *Report* fornisce una panoramica delle aree prioritarie in cui i vari gruppi di lavoro e istanze operanti in ambito IA e *privacy* possono collaborare e rafforzare le loro sinergie all'interno dell'OCSE e oltre, e contribuire a sviluppare risorse e strumenti per sistemi di IA affidabili che rispettino la *privacy*, cogliendo opportunità politiche e sfide di rilevanza comune, aree di complementarità e potenziali lacune. Nel medio termine, questi sforzi di cooperazione potrebbero aiutare a valutare se le raccomandazioni sull'IA e sulla *privacy* debbano essere aggiornate per riflettere le sinergie tra i due ambiti. Ciò consentirà ai politici e ai decisori di sfruttare punti comuni, complementarità ed elementi di convergenza nei rispettivi quadri politici o, al contrario, di identificare gli ostacoli allo sviluppo di posizioni comuni o della cooperazione.

21.4. *Le conferenze internazionali ed europee delle autorità di protezione dati e* privacy

Global Privacy Assembly

La *Global Privacy Assembly* (GPA) si è tenuta a Jersey dal 28 ottobre al 1° novembre ed è stata come di consueto articolata in una sessione aperta, che si è particolarmente soffermata sulla protezione dei dati di soggetti vulnerabili in un ambito digitale sempre più accresciuto, e in una sessione chiusa alla partecipazione delle sole autorità di protezione di dati.

21

La GPA ha continuato ad ampliare la propria attività ed ambito di influenza, ed ha proseguito il percorso di stabilizzazione delle sue attività attraverso più stringenti regole procedurali e la creazione di un segretariato permanente. Sono state infatti accolte le richieste di accreditamento alla GPA di diverse autorità che hanno accresciuto il numero complessivo dei Membri, ed è stato riconosciuto lo *status* di osservatori a diverse autorità tra cui la Banca mondiale.

In ossequio alla risoluzione adottata nella 43ª GPA di Città del Messico del 2021, il 2025 ha segnato il primo anno di attività del segretariato permanente, attualmente gestito dall'autorità di protezione dati filippina, completando così un percorso di rafforzamento della Conferenza.

Nella sessione chiusa, oltre a significative risoluzioni, riguardo, rispettivamente, ai flussi transfrontalieri di dati (cd. *Data Free Flow with Trust* di cui il Garante è stato co-*sponsor*), alle neurotecnologie, ai meccanismi di certificazione, nonché al tema della sorveglianza di massa, la Conferenza ha approvato una risoluzione contenente proposte di emendamento alle regole procedurali della GPA, volte, tra l'altro, ad adeguare le procedure dell'*Assembly* al funzionamento del nuovo segretariato e a migliorare e precisare i meccanismi di partecipazione alla GPA.

La GPA si è conclusa con la presentazione, da parte dell'Autorità della Repubblica coreana, della prossima conferenza internazionale che si terrà a Seul, dal 16 al 19 settembre 2025.

Conferenza di primavera *(Spring Conference)*

Si è tenuta a Riga dal 14 al 16 maggio, ospitata dall'autorità lettone, la Conferenza di primavera delle autorità europee di protezione dati, cd. *Spring Conference*.

Tra i temi principali della Conferenza del 2024 si segnalano in particolare l'analisi delle diverse normative UE che concernono l'ambito digitale e della loro interazione con la protezione dati, le sempre nuove sfide per *privacy* e tutela dei dati provenienti dalle tecnologie emergenti, la salvaguardia dei dati sanitari nell'era digitale, nonché la necessità di favorire e promuovere forme di cooperazione efficaci tra le autorità di protezione dei dati, decisori e imprese. La sessione aperta al pubblico della Conferenza è stata quest'anno dedicata al tema della protezione dati nell'ambito della lotta al riciclaggio e al finanziamento del terrorismo.

Nel corso della sessione chiusa è stata adottata una risoluzione che riflette l'impegno delle autorità europee di protezione dei dati affinché sia accresciuta la cooperazione, anche attraverso la creazione di un sito permanente della Conferenza, il rafforzamento del *Case Handling Workshop,* nonché la creazione di una rete operativa di autorità europee con il supporto del Consiglio d'Europa per facilitare la cooperazione.

21.5. *Le domande pregiudiziali davanti alla Corte di giustizia dell'Unione europea*

Si conferma anche per quest'anno l'aumento degli interventi interpretativi della Corte di giustizia dell'UE a seguito di richieste di rinvio pregiudiziale *ex* art. 267 TFUE, in relazione a disposizioni del RGPD e della direttiva polizia e giustizia, nonché con riguardo alla direttiva 2002/58/CE. Con questi interventi, in relazione ai quali il Garante è stato coinvolto dai competenti organismi nazionali, la Corte ha fornito importanti elementi interpretativi in tema, per esempio, di risarcimento del danno non patrimoniale conseguente al trattamento di dati personali, di titolarità e contitolarità dei trattamenti, di esercizio dei poteri delle autorità di controllo.

Al riguardo, va segnalato che nel corso del 2024 è stato operato un trasferimento parziale della competenza pregiudiziale della Corte al Tribunale dell'UE in sei materie specifiche, mentre la materia della protezione dei dati personali è restata di esclusiva competenza della Corte.

Nel prosieguo si segnalano, in particolare, le seguenti sentenze adottate dalla CGUE nel corso del 2024, rappresentando che su ulteriori questioni pregiudiziali sono state presentate nel medesimo anno le conclusioni degli Avvocati generali, delle quali non è possibile dare conto in questa sede:

- sentenza 11 gennaio 2024, causa C-231/22, in materia di titolare del trattamento in caso di pubblicazione dei dati in G.U.;
- sentenza 16 gennaio 2024, causa C-33/22, in materia di ambito di applicazione del RGPD e attività riguardanti la sicurezza nazionale, nonché di competenza dell'autorità di controllo e diritto di reclamo;
- sentenza 25 gennaio 2024, causa C-687/21, in materia di risarcimento del danno non patrimoniale;
- sentenza 30 gennaio 2024, causa C-118/22, in materia di conservazione dei dati di una persona fisica condannata per un reato e cancellazione dei dati (direttiva 2016/680);
- sentenza 7 marzo 2024, causa C-604/22, in materia di dato personale, titolare e contitolare del trattamento;
- sentenza 7 marzo 2024, causa C-740/22, in materia di accesso ai dati relativi alle condanne penali trattati da un tribunale;
- sentenza 14 marzo 2024, causa C-46/23, in materia di poteri delle autorità di controllo in assenza dell'iniziativa dell'interessato;
- sentenza 21 marzo 2024, causa C-61/22, in materia di dati biometrici nelle carte d'identità elettroniche;
- sentenza 11 aprile 2024, causa C-741/21, in materia di risarcimento del danno non patrimoniale;
- sentenza 30 aprile 2024, causa C-178/22, in materia di accesso ai dati di traffico conservati dai fornitori di servizi di comunicazione elettronica (direttiva 2002/58/CE) da parte di un'autorità nazionale competente al fine di perseguire reati gravi, e portata del controllo preventivo del giudice sulle richieste di accesso ai dati;
- sentenza 30 aprile 2024, causa C-470/21, in materia di comunicazioni elettroniche (direttiva 2002/58/CE) e lotta contro le contraffazioni commesse in internet;
- sentenza 30 aprile 2024, causa C-670/22, in materia di servizio di telecomunicazioni cifrate ed utilizzo di prove acquisite in violazione del diritto dell'Unione;
- sentenza 7 maggio 2024, causa C-115/22, in materia di violazione delle disposizioni *antidoping* e pubblicazione *online*;
- ordinanza 27 maggio 2024, causa C-312/23, in materia di diritto, per l'interessato, di ottenere una copia dei dati personali che lo riguardano oggetto del trattamento;
- sentenza 13 giugno 2024, causa C-229/23, in materia di ascolto, captazione e memorizzazione delle conversazioni telefoniche di persone sospettate di aver commesso un reato doloso grave (direttiva 2002/58/CE);
- sentenza 20 giugno 2024, cause riunite C-182/22, e C-189/22 in materia di risarcimento del danno e furto o usurpazione d'identità;
- sentenza 20 giugno 2024, causa C-590/22, in materia di risarcimento del danno non patrimoniale;
- sentenza 11 luglio 2024, causa C-461/22, in materia di titolarità del trattamento da parte dell'amministratore di sostegno e obbligo di fornire l'accesso ai dati;
- sentenza 11 luglio 2024, causa C-757/22, in materia di obblighi di informazione del titolare del trattamento e alla rappresentanza degli interessati da parte di un'associazione di tutela degli interessi dei consumatori;
- sentenza 29 luglio 2024, causa C-623/22, in materia di cooperazione amministrativa nel settore fiscale;
- sentenza 12 settembre 2024, cause riunite C-17/22 e C-18/22, in materia di

necessità del trattamento per finalità contrattuali ovvero per il legittimo interesse del titolare;

- sentenza 26 settembre 2024, causa C-768/21, in materia di compiti dell'autorità di controllo e discrezionalità;
- sentenza 4 ottobre 2024, causa C-200/23, in materia di pubblicazione nel registro del commercio di un contratto di società contenente dati personali, e diritto alla cancellazione e al risarcimento del danno non patrimoniale;
- sentenza 4 ottobre 2024, causa C-507/23, in materia di diritto al risarcimento del danno non patrimoniale;
- sentenza 4 ottobre 2024, causa C-21/23, in materia di commercializzazione di medicinali tramite una piattaforma *online* e nozione di dati relativi alla salute;
- sentenza 4 ottobre 2024, causa C-4/23, in materia di cambiamento del prenome e della identità di genere e dell'obbligo per lo Stato membro d'origine di riconoscere e di annotare tale cambiamento nell'atto di nascita;
- sentenza 4 ottobre 2024, causa C-621/22, in materia di legittimo interesse del titolare del trattamento;
- sentenza 4 ottobre 2024, causa C-446/21, in materia di principi di limitazione delle finalità e di minimizzazione dei dati, nonché di trattamento di categorie particolari di dati personali resi manifestamente pubblici dall'interessato;
- sentenza 4 ottobre 2024, causa C-548/21, in materia di trattamento dei dati personali contenuti in un telefono cellulare da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati (direttiva 2016/680) e controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente;
- sentenza 28 novembre 2024, causa C-80/23, in materia di registrazione da parte della polizia di dati biometrici e genetici (direttiva 2016/680), e interpretazione della sentenza 26 gennaio 2023, C-205/21;
- sentenza 28 novembre 2024, causa C-169/23, in materia di obbligo di informazione del titolare del trattamento in caso di dati generati dallo stesso, e competenza dell'autorità di controllo in caso di reclamo;
- sentenza 19 dicembre 2024, causa C-65/23, in materia di trattamento di dati nell'ambito dei rapporti di lavoro e risarcimento del danno non patrimoniale.

21.6. *I progetti per l'applicazione del RGPD finanziati dall'Unione europea*

Progetto ARC II

È proseguita e si è conclusa nel corso del 2024 l'attività del consorzio composto dal Garante, dall'Autorità croata di protezione dati e dalle Università di Firenze, di Zagabria e di Bruxelles (Vrije), nel Progetto ARC II, dedicato alle PMI.

Dopo aver implementato uno strumento digitale *open source* a cui è stato dato il nome OLIVIA, su misura per le esigenze specifiche delle PMI, si è proseguito nella realizzazione dei seminari (10 in presenza e 10 da remoto) previsti dal progetto.

In particolare, nel primo semestre del 2024 sono stati organizzati cinque seminari da remoto tenuti da personale del Garante e dieci in presenza, tenuti da personale del Garante e dell'Università di Firenze.

Il 9 aprile è stata organizzata una Conferenza internazionale che ha avuto un grande successo di pubblico e ha visto la partecipazione tra i relatori, oltre al Presidente del Garante e al Direttore dell'Autorità croata di protezione dati, di rappresentanti dell'Unione europea, delle figure apicali delle maggiori associazioni e confederazioni di PMI, oltre a docenti universitari e dirigenti del Garante e di altre istituzioni dello Stato.

Inoltre, è proseguita la campagna di sensibilizzazione rivolta alle PMI e al grande pubblico, attraverso *post* pubblicati nei profili *social* del Garante.

Gemellaggio *(Twinning)* con la Bosnia-Erzegovina

Ha avuto inizio l'impegno del Garante nel gemellaggio con la Bosnia-Erzegovina, il cui obiettivo generale è di contribuire all'attuazione della riforma della pubblica amministrazione bosniaca in linea con gli standard dell'Unione europea e internazionali. Il contributo dell'Autorità, all'interno di un consorzio composto anche da CSI Piemonte, HAUS ed EUTALIA, è stato finalizzato a fornire supporto riguardo allo sviluppo dei servizi di *e-government*, conformemente alle disposizioni del RGPD.

In particolare, nell'espletamento delle attività assegnate, il Garante ha predisposto: due *set* di raccomandazioni, rispettivamente sulla trasparenza ed il controllo democratico e per le procedure di lavoro riguardanti l'etica dei dati e l'utilizzo dei dati personali, linee guida per l'uso etico dei dati personali ed un corso di formazione di una settimana *in loco* sulle procedure di lavoro per l'uso etico dei dati personali, basato sulla metodologia di formazione dei formatori.

22 Trattamenti transfrontalieri di dati personali e cooperazione europea

I trattamenti transfrontalieri, ovverosia i trattamenti di dati personali che, secondo la definizione dell'art. 4, n. 23 del RGPD, hanno luogo nell'ambito delle attività di più stabilimenti di un titolare nel SEE, o di un unico stabilimento ma incidendo in modo sostanziale su interessati in più di uno Stato membro, sono molto ricorrenti sia nell'ambito delle attività connesse alla società dell'informazione sia in ambito economico-produttivo.

Il meccanismo dello sportello unico (*one stop shop*) si fonda sui principi di cooperazione (tra autorità di controllo) e di coerenza (tra autorità di controllo e CEPD), i quali congiuntamente danno vita ad un sistema amministrativo pan-europeo, il cui futuro si prospetta ulteriormente rafforzato e consolidato dalla proposta della Commissione europea di un regolamento che stabilisce norme procedurali aggiuntive (COM/2023/348 *final*, del 4 luglio 2023).

La fisiologia di tali trattamenti emerge chiaramente in termini sia quantitativi che qualitativi nell'ambito delle procedure di cooperazione (cd. procedure IMI, dal nome della piattaforma prevista dal reg. (UE) 1024/2012, per la gestione dei meccanismi di cooperazione e coerenza di cui al Capo VII del RGPD, sulla quale vengono scambiate le informazioni tra autorità di controllo) (cfr. tabb. 17-21).

Nell'anno 2024 le procedure di cooperazione nel settore delle reti telematiche sono aumentate di circa il 20% rispetto al 2023. Nell'arco di due anni l'impatto delle procedure di cooperazione, nel solo ambito delle reti telematiche, è dunque cresciuto quasi del 100% rispetto al dato del 2022. Per quanto riguarda l'ambito economico, si sottolinea che le procedure IMI riguardano casistiche eterogenee riferite ad una variegata pluralità di titolari e responsabili del trattamento, considerata la granularità del settore di riferimento. Anche in questo ambito, si conferma nel 2024 la prevalenza delle procedure IMI ai sensi dell'art. 56 del RGPD volte all'identificazione dell'autorità capofila (*Lead Supervisory Authority*) e delle autorità interessate (*Concerned Supervisory Authority*) che rappresentano circa il 72% delle procedure pervenute.

22.1. *Trattamenti transfrontalieri e società dell'informazione*

In questo ambito, in termini generali, si registra un costante aumento sia delle procedure di vera e propria cooperazione (artt. 60 e ss. RGPD), che delle procedure preliminari *ex* art. 56 del RGPD, ovverosia le procedure relative alla fase iniziale di determinazione, su ogni singolo caso, aperto d'ufficio o originato da un reclamo, dei ruoli rispettivamente di autorità capofila e autorità interessata/e. Si rileva altresì un aumento delle procedure di cooperazione nei confronti delle ben note *tech company* stabilite in Irlanda, originate da reclami di interessati che si trovano in Italia, che vengono trasmessi attraverso procedure di assistenza reciproca volontaria (*Voluntary Mutual Assistance Procedure*) all'autorità capofila irlandese. I reclami in argomento vengono spesso trattati e definiti mediante procedure di composizione amichevole (*amicable settlement*), che sono applicate da alcune autorità di controllo sulla scorta della legislazione nazionale

nella cornice normativa di cui all'art. 57, par. 1, lett. f), RGPD nonché alla luce delle linee guida CEPD 6/2022 sull'*amicable settlement* e 2/2022 sull'applicazione dell'art. 60 del RGPD.

Le procedure di cooperazione rappresentano uno strumento imprescindibile che consente all'Autorità di prendere parte alle istruttorie condotte nei confronti dei principali *players* delle piattaforme *online* e dei servizi di *social networking*. In tale contesto vengono, infatti, affrontate le tematiche transnazionali di maggiore attualità e rilevanza nella società dell'informazione, come l'interpretazione e l'applicazione dei principi generali in materia di trattamento dei dati personali, la base giuridica di specifiche attività di trattamento dei dati e l'esercizio dei diritti.

In particolare, nel corso del 2024, attraverso le procedure di cooperazione è stato affrontato a livello europeo l'innovativo e dirompente tema relativo ai trattamenti di dati personali finalizzati all'addestramento di modelli e servizi di IA generativa. In tale ambito, al netto delle numerose istruttorie concluse e di quelle ancora in corso, si segnalano due casi di cooperazione con l'autorità (irlandese) capofila che hanno avuto un preliminare esito positivo. Il primo riferimento è alla vicenda relativa alla decisione di X Corp. di trattare i dati personali degli utenti europei contenuti nei *post* del *social network* X (*ex* Twitter) per l'addestramento dei modelli di IA connessi al Sistema Grok, che si è conclusa nell'agosto 2024 con la decisione – in esito ad un procedimento giudiziario d'urgenza promosso dall'autorità di controllo irlandese innanzi alla *High Court* – della società di sospendere spontaneamente tali trattamenti a data da definire.

Il secondo riferimento è alla questione relativa all'intenzione di Meta di addestrare i suoi modelli di *GenAI* con i dati personali degli utenti dei servizi Facebook e Instagram; in questo caso l'istruttoria si è conclusa nel giugno 2024, dopo una intensa interlocuzione, con la decisione della società di sospendere il progetto.

Nell'ambito della tematica relativa ai trattamenti di dati personali connessi all'IA generativa, si rappresenta ancora la partecipazione del Garante, in veste di co-coordinatore, ai lavori della *Task Force* ChatGPT, istituita dal CEPD dei dati nell'aprile 2023. La *Task Force* è stata creata per agevolare la cooperazione tra autorità di controllo nell'ambito delle istruttorie nazionali avviate nei confronti di OpenAI in relazione al servizio ChatGPT prima dello stabilimento della società statunitense in Irlanda e dunque in una fase di non applicazione del meccanismo dello Sportello unico. I lavori della *Task Force* sono confluiti, nel maggio 2024, in un *report* finale che contiene una serie di valutazioni giuridiche preliminari in merito ai modelli linguistici di grandi dimensioni (LLM *Model*) e, in particolare, al servizio ChatGPT con riferimento alla base giuridica, alla trasparenza, ai principi di correttezza ed esattezza nonché ai diritti degli interessati.

I principi espressi nel *final report* della *TF* ChatGPT sono stati più volte richiamati nella *Opinion* 28/2024 "*On certain data protection aspects related to the processing of personal data in the context of AI models*" adottata in data 17 dicembre 2024 dal CEPD, ai sensi dell'art. 64, par. 2, RGPD (cfr. par. 21.1). In relazione a tale parere, richiesto dall'autorità irlandese al fine di perseguire un'armonizzazione normativa a livello europeo su un tema di particolare rilevanza e di grande impatto sulla società, come quello delle tecnologie in rapida evoluzione, il Garante ha partecipato attivamente alla discussione e alla stesura della *Opinion* assicurando la partecipazione ai lavori dei sottogruppi.

Tra i più rilevanti progetti di decisione esaminati nell'ambito della cooperazione europea, si segnala quello nei confronti di un importante *social network* statunitense, con riferimento a trattamenti di dati personali finalizzati all'analisi comportamentale e alla pubblicità mirata. La procedura di cooperazione ha tratto origine da un reclamo *ex* art. 80 del RGPD, presentato in data 28 maggio 2018 da un'associazione per i diritti civili francese relativamente ad un presunto trattamento illecito di dati personali (base giuridica,

trasparenza e correttezza) per finalità di *behavioural analysis* e *targeted advertising*. L'autorità irlandese (DPC), in cooperazione con le autorità interessate, ha accertato la violazione degli artt. 5, par. 1, lett. a), 6, 13, par. 1, lett. c), 14, par. 1, lett. c), RGPD e ha, pertanto, adottato nei confronti del titolare *de quo* un ammonimento, ai sensi dell'art. 58, par. 2, lett. b), RGPD, un ordine di messa in conformità, ai sensi dell'art. 58, par. 2, lett. d), RGPD ed una sanzione amministrativa pari a euro 310 milioni.

Parimenti rilevante è il progetto di decisione della DPC nei confronti di un altro fornitore di servizi di *social networking*, in tema di misure di sicurezza. La procedura di cooperazione ha tratto origine da una indagine aperta d'ufficio dall'autorità capofila irlandese a seguito della comunicazione informale del titolare in merito ad una erronea e involontaria conservazione in chiaro – ovverosia senza alcun sistema di crittografia – di alcune *password* degli utenti dei servizi. L'autorità irlandese, in cooperazione con le autorità interessate, ha accertato la violazione di una serie di disposizioni in materia di sicurezza del trattamento e violazione di dati personali (artt. 5, par. 1, lett. f), 32, par. 1, 33, par. 1 e 5, RGPD) e ha adottato nei confronti del titolare un ammonimento, ai sensi dell'art. 58, par. 2, lett. b), RGPD ed una sanzione amministrativa pari a euro 91 milioni.

Un altro caso di rilievo ha riguardato la decisione dell'autorità olandese nei confronti di una piattaforma di *streaming* la quale è stata sanzionata per euro 4,75 milioni per le gravi carenze in termini di trasparenza informativa relativamente alla gestione dei dati personali degli abbonati, principalmente a causa dell'insufficiente riscontro ad alcune richieste di accesso ai dati formulate da specifici interessati.

Nel contesto delle procedure di cooperazione è stata confermata la tendenza, in conformità alle linee guida 2/2022 sull'art. 60 del RGPD, della ricerca di un consenso condiviso tra autorità capofila e autorità di controllo interessate nelle fasi pre-decisorie, mediante condivisione dei cd. *investigation report* e l'anticipazione dei progetti di decisione. La cooperazione è stata ulteriormente rafforzata anche dall'attuazione, a seguito del congresso di Vienna dell'aprile 2022, del particolare regime previsto per i casi di importanza strategica (*strategic cases*). Il Garante è stato attivamente coinvolto, in collaborazione con altre autorità di controllo, nella trattazione congiunta di un caso che l'Autorità aveva già delineato come prioritario attesa la tematica trattata (*Internet of Things*).

Nella stessa prospettiva si iscrive, con riferimento alle procedure di coerenza di cui all'art. 65 del RGPD, la definizione bonaria, a seguito di un accordo intercorso con l'autorità francese sulla decisione finale, di una controversia relativa ad un progetto di decisione riveduto e adottato dall'autorità francese nei confronti di importante motore di ricerca francese in relazione al quale il Garante aveva presentato obiezioni pertinenti e motivate.

22.2. *Trattamenti transfrontalieri in ambito economico-produttivo*

Come negli anni passati, la partecipazione al sistema IMI impegna le autorità di protezione dei dati del SEE in misura sempre crescente sia in termini di risorse impegnate che di quantità di lavoro svolto anche in questo ambito.

L'Autorità si è dichiarata "interessata", ai sensi dell'art. 4, n. 22, RGPD, in 96 casi (43%) assumendo invece la posizione di autorità capofila in un numero limitato di casi riguardanti società con stabilimento unico o principale in Italia. In particolare, l'Autorità si è dichiarata "interessata" in tutti quei casi ove 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 avviare le procedure di cooperazione applicabili provvedendo a trasmettere la relativa documentazione alla competente autorità capofila.

Rimane sostanzialmente stabile, rispetto al 2023, il numero delle procedure IMI di consultazione informale previste dall'art. 60, par. 1, RGPD.

Sono invece lievemente aumentate le procedure di cooperazione giunte alla fase decisoria nel settore privato. Rispetto ai progetti di decisione caricati sulla piattaforma IMI dalle competenti autorità capofila si è ritenuto, complessivamente, di condividerli facendo maturare il silenzio-assenso o limitandosi, ove opportuno, a formulare solo commenti o richieste di chiarimenti.

Riguardo ai casi in cui l'Autorità si è dichiarata capofila nel corso del 2024 in relazione a reclami aventi rilevanza transfrontaliera trasmessi da altre autorità europee di protezione dati tramite la piattaforma IMI, sono state avviate istruttorie (con relativi scambi di informazioni con le altre autorità interessate) relativamente a una serie di reclami o segnalazioni nei confronti di società con sede principale in Italia (*e-commerce*, società di noleggio auto, banche, ecc.). In particolare, con tali reclami gli interessati hanno lamentato principalmente il mancato esercizio dei diritti di accesso o cancellazione o la possibile violazione di dati personali.

Nel 2024 sono state adottate le seguenti decisioni finali:

- provv. 8 febbraio 2024, n. 67 (doc. web n. 9993122). Si è concluso il procedimento relativo al reclamo di un cittadino tedesco, nei confronti di una società con sede in Italia, volto a segnalare una possibile violazione dell'art. 32 del RGPD (il titolare gli avrebbe inviato, nella *e-mail* di conferma della registrazione al proprio sito web, la sua *password* in chiaro). Dopo aver approvato un nuovo progetto di decisione riveduto, che non è stato oggetto di alcuna obiezione pertinente e motivata, il Garante, in qualità di autorità capofila, ha adottato la decisione finale *ex* art. 60, par. 7, disponendo la chiusura del procedimento senza l'adozione di misure correttive o sanzionatorie con l'invito, ai sensi dell'art. 57, par. 1, lett. d), ad una costante verifica e aggiornamento degli standard di sicurezza, e ad adottare, in particolare, tecniche di conservazione della *password* che offrono maggiori garanzie di sicurezza del sistema;

- provv. 9 maggio 2024, n. 294 (doc. web n. 10074277). Si è concluso il procedimento relativo al reclamo nei confronti di una società tedesca, proposto da un cittadino italiano che aveva chiesto di accedere ai dati ostativi all'apertura di un conto su *app* di pagamento. Al riguardo, l'autorità di Berlino, capofila nel relativo trattamento transfrontaliero, aveva comunicato la sua valutazione e la proposta di archiviare il caso (ritenendo soddisfacente il riscontro del titolare) ed aveva chiesto al Garante di consultare l'interessato a riguardo. In particolare, si è ritenuto soddisfacente il riscontro fornito all'interessato dalla società, titolare di una piattaforma di pagamenti e investimenti, che dopo aver consultato la banca *partner* (la quale si era occupata di verificare la richiesta di apertura del conto), aveva riportato che a causa delle politiche interne e linee guida dei relativi partner non era oggettivamente in grado di offrire il servizio, confermando inoltre la cancellazione dei dati dell'interessato. Poiché quest'ultimo, consultato, non aveva fatto pervenire obiezioni o osservazioni, il Garante ha aderito alle valutazioni della capofila, disponendo, ai sensi dell'art. 60, par. 8, la chiusura del procedimento, in quanto non era stata ravvisata una violazione delle norme in materia di protezione dei dati da parte della società;

- provv. 17 luglio 2024, n. 441 (doc. web n. 10070252). In questo caso, i reclamanti, due cittadini norvegesi, avevano ricevuto la notifica di sanzioni amministrative per mancato pagamento di pedaggio autostradale, come conseguenza dell'erronea identificazione degli stessi da parte di una società di autonoleggio italiana quali conducenti del veicolo a cui erano state associate le violazioni del codice della strada italiano. La società, dopo aver provveduto ad effettuare le necessarie rettifiche anche presso i carabinieri e la concessionaria dei servizi autostradali che avevano richiesto i dati identificativi dei conducenti

(richiesta lecita in quanto giustificata da obbligo di legge), si era fatta carico dei relativi addebiti ed aveva aggiornato i propri sistemi con soluzioni tecniche allo scopo di ridurre il rischio di simili errori in futuro. Tuttavia, tenendo conto di tutte le circostanze del caso e, in particolare, del fatto che si era trattato di un errore umano occasionale (anche secondo le linee guida CEPD 01/2021 e 09/2022) e che il titolare aveva provveduto a porre fine alla violazione eliminando le possibili conseguenze, il Garante, in qualità di autorità capofila, ha disposto la chiusura del procedimento, sensi dell'art. 60, par. 7, senza l'adozione di misure sanzionatorie *ex* art. 58, par. 2, RGPD (conformemente alle linee guida CEPD 02/2022 sull'applicazione dell'art. 60 del RGPD), invitando ad ogni modo il titolare del trattamento (*ex* art. 57, par. 1, lett. d), RGPD) a verificare costantemente le misure tecniche e organizzative adottate, necessarie ad evitare errori simili in futuro.

Assistenza reciproca

Per quanto riguarda l'assistenza reciproca fra le autorità di controllo, con riferimento all'ambito economico, si conferma l'utilizzo della relativa procedura IMI allo scopo di ottenere informazioni sulle normative nazionali in tema di protezione dei dati o su questioni relative all'applicazione di particolari disposizioni del RGPD.

I temi trattati sono stati molteplici: applicabilità dell'art. 22 del RGPD e più in generale i processi decisionali automatizzati; trattamento dei dati dei membri della comunità religiosa dei Testimoni di Geova; *data retention* con riguardo alle informazioni relative agli acquisti nell'ambito di programmi di fidelizzazione; interpretazione dell'art. 77, par. 2, RGPD; organismi di certificazione; installazione di impianti di videosorveglianza in infrastrutture critiche; licenze nel settore del credito e attività finanziaria; trattamento dei dati biometrici nel settore bancario; trattamento di dati per finalità di *marketing* da parte delle banche; disciplina nazionale relativa a centrale dei rischi e sistemi di informazioni creditizie; trattamento dei dati relativi alla titolarità effettiva di imprese; trattamento dei dati da parte delle società di recupero crediti; servizi di assicurazione e relative registrazioni di chiamate.

Da segnalare, inoltre, i riscontri forniti su questioni di natura più propriamente istituzionale. Fra queste ultime, le condizioni previste a livello nazionale per la presentazione delle richieste di accesso ai sensi dell'art. 15 del RGPD e le eventuali limitazioni all'esercizio del diritto, ai sensi dell'art. 23 del RGPD; la natura obbligatoria e vincolante dei pareri, resi dal Garante sui progetti di legge nazionali (art. 36, par. 4, RGPD); le autorità deputate in Italia alla supervisione dei sistemi di IA e, in particolare, il ruolo del Garante a tale riguardo; la normativa nazionale relativa alla accessibilità dei dati contenuti nelle liste elettorali da parte dei partiti politici.

23 Attività di normazione tecnica internazionale e nazionale

Il Garante ha proseguito la collaborazione in tema di elaborazione di norme tecniche internazionali nell'ambito del *Working Group* 5 del sottocomitato SC27, che si occupa della sicurezza delle informazioni all'interno del comitato tecnico JTC1 dell'Organizzazione internazionale per la normazione (ISO). Il gruppo di lavoro segue gli aspetti di sicurezza nella gestione delle identità relativamente alle tecnologie biometriche e alla protezione dei dati personali. Armonizzando la propria posizione con quelle delle altre autorità di protezione dati tramite il CEPD, che ha un collegamento in proposito con ISO, l'Autorità ha seguito lo sviluppo delle seguenti norme tecniche:

- *ISO 27701:2019 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*, revisione a seguito della pubblicazione della ISO 27002:2022;

- ISO 27566 - *Information security, cybersecurity and privacy protection - Age assurance systems - Framework*, che si propone di stabilire principi chiave, che includono anche la *privacy*, per abilitare decisioni di fornitura di beni, servizi o contenuti che dipendano dall'età del soggetto richiedente mediante la definizione di un *framework* di indicatori di confidenza di età o di *range* di età delle persone fisiche nonché, con la parte 2 definire gli approcci tecnici e una guida per l'implementazione dei sistemi e con la parte 3 indicare elementi per il *benchmark*, le misure e il test delle componenti per la *age verification*;

- 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 27560:2023 *revision* che intende estendere il documento 27560:2023 - *Consent Receipt and Record Standard* a tutte le basi giuridiche del trattamento di dati personali;

- ISO TS 27561 - *Privacy operationalisation model and method for engineering (POMME)*, che, sulla base del modello OASIS-PMRM (*Privacy Management Reference Model*), fornisce elementi e supporta le organizzazioni al fine di definire un modello e metodi standardizzati per la *privacy engineering* di sistemi complessi (pubblicato a marzo 2024);

- ISO 29151:2017 - *Code of practice for personally identifiable information protection* – revisione sistematica che tiene conto dell'applicabilità dei controlli individuati nelle organizzazioni (in particolare PMI) che non implementano sistemi di gestione;

- ISO 27018:2019 - *Code of practice for protection of PII in public clouds acting as PII processors* – revisione della norma tecnica (che individua controlli specifici per i *provider* di servizi *cloud* che, trattando dati personali, agiscono in qualità di responsabile del trattamento) per allineamento alla nuova della norma ISO 27002:2022;

- ISO 27562 - *Privacy guidelines for fintech services* che propone una linea guida per la *privacy* per i *fintech services* identificando i modelli di business, i ruoli delle relazioni C2B, B2B, i rischi e i requisiti *privacy* e fornendo specifici controlli *privacy* per tali servizi tenendo conto del contesto (legale) e dei ruoli;

- ISO 27564 - *Privacy models* che intende fornire una linea guida circa l'uso dei modelli nella *privacy engineering*;

- ISO 27568 - *Security and privacy of digital twins* che ha lo scopo di monitorare il progresso dei lavori di standardizzazione sul tema *digital twin* e approfondire le problematiche degli *stakeholders* quali *security* e *privacy*;

- ISO 27573 - *Privacy protection of user avatar and system avatar interactions in the metaverse* che si pone l'obiettivo di descrivere i concetti fondamentali, la definizione e le caratteristiche del metaverso, degli *avatar* (rappresentazione di un utente nell'ambiente digitale, delle sue preferenze, dell'identità, etc..), i diversi tipi di avatar (*realistic, iconic, fantasy*), gli elementi di protezione della *privacy* che intervengono durante le interazioni dei medesimi;

- ISO 27091 - *Cybersecurity and privacy – Artificial intelligence – Privacy protection* che fornisce una guida alle organizzazioni che utilizzano o sviluppano sistemi di IA e modelli di *machine learning* per indirizzare i rischi *privacy* identificando i rischi nel ciclo di vita dei sistemi IA e stabilendo meccanismi per valutare le conseguenze e trattare tali rischi mediante misure di mitigazione.

L'Autorità inoltre, nell'ambito del *Working Group* 5 del comitato tecnico JTC13 del CEN CENELEC che si occupa dello sviluppo di norme tecniche riguardanti *Data Protection, Privacy and Identity Management*, ha contribuito 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 17926 - *Privacy Information Management System per ISO/IEC 27701 - Refinements in European context*, che adatta il *framework* internazionale offerto dalla ISO 27701 nel contesto europeo;

- JT013068 - *Certification scheme as per ISO/IEC 17065 for certification against EN 17926 - Privacy Information Management System per ISOIEC 27701 - Refinements in European context* che intende definire uno schema di certificazione ai sensi dell'art. 42 del RGDP basato sulla norma tecnica EN 17926.

Del pari è proseguita la collaborazione con le diverse commissioni tecniche UNINFO, l'Ente di normazione federato con UNI (Ente nazionale italiano di unificazione).

24 L'attività di comunicazione, informazione e di rapporto con il pubblico

24.1. *La comunicazione del Garante: profili generali*

Anche nell'anno 2024 il Garante ha contribuito alla crescita sociale e culturale del Paese grazie al potenziato impulso impresso al consolidamento del diritto alla protezione dei dati, alla diffusione della cultura della *privacy* presso cittadini, istituzioni, imprese ed associazioni.

Il grande sviluppo delle tecniche di IA che ha caratterizzato il 2024, e che è testimoniato dai provvedimenti adottati e dalle iniziative profuse dal Garante in tale ambito al fine di tutelare i dati personali di tutti gli interessati, in particolare dei minori, ha comportato una importante attività di comunicazione e sensibilizzazione su queste stesse tematiche attraverso molteplici canali di cui si dà conto nei paragrafi successivi.

Il 2024 è stato anche un anno chiave per la regolamentazione dell'IA, avendo visto l'adozione del reg. europeo sull'IA (2024/1689), ed è stata al centro peraltro del G7 guidato dall'Italia e del G7 *Privacy* organizzato dal Garante a Roma dal 9 all'11 ottobre 2024.

Più in generale, l'attività di comunicazione e informazione è stata fondamentale per valorizzare l'operato del Garante, grazie anche alla realizzazione di campagne di comunicazione istituzionale e alla progettazione e realizzazione di strategie innovative.

Le attività di comunicazione istituzionale hanno avuto come oggetto il contrasto ai fenomeni più invasivi della riservatezza delle persone, quali il *telemarketing* aggressivo, il controllo dei lavoratori e i diritti dei *rider* o, per quanto riguarda le tecnologie emergenti, i sistemi di raccolta di dati biometrici e l'uso del riconoscimento facciale. Grande attenzione è stata posta ai vari aspetti del *cybercrime*: dal *ransomware*, al *phishing*; alle *app* pirata che rubano i dati ai *software* per lo spionaggio. Come già in passato, il Garante è anche intervenuto sui rischi legati ad un uso poco consapevole della rete quali il cyberbullismo e il *revenge porn*, il *sexting*, il *deep fake*, l'*hate speech* e lo *sharenting* promuovendo in molte occasioni una vera e propria educazione digitale, capace di rendere tutti consapevoli delle grandi opportunità, ma anche dei rischi che caratterizzano la sfera digitale.

Costante attenzione è stata posta al fenomeno degli accessi abusivi alle banche dati pubbliche e private, che ha visto negli ultimi anni un incremento collegato alla rivendita di informazioni riservate, anche attraverso opachi meccanismi di reperimento dei dati sui quali il Garante ha voluto fare luce; essenziale, al riguardo, è stata l'informazione puntuale fornita dall'Autorità sulle attività e le strategie messe in atto a diversi livelli, anche attraverso un potenziato coordinamento interno ed esterno.

Inoltre, una specifica attività di informazione è stata svolta nei confronti dei *media* a tutela delle vittime di violenza.

La campagna di comunicazione istituzionale condotta dall'Autorità nel 2024 ha riguardato il cd. *sharenting* attraverso l'invito rivolto ai genitori di figli minorenni a una maggiore consapevolezza sui rischi connessi alla pubblicazione su internet delle loro foto.

Le attività di comunicazione strategica

Nella specie in uno *spot,* diffuso sulle reti radio tv della Rai ed anche attraverso i *social media* del Garante, un professore (interpretato dall'attore Luca Angeletti) ha con leggerezza ed ironia sollecitato una classe di genitori, anche attraverso il *claim* finale "La

24

sua *privacy* vale più di un *like*", a considerare che le foto e le informazioni pubblicate sui *social* o condivise nelle *chat* potrebbero essere catturate e riutilizzate per scopi impropri e/o attività illecite o finire addirittura sui siti pedopornografici.

L'Autorità ha preso parte alla Fiera Didacta, il più importante evento dedicato alla scuola che si svolge ogni anno a Firenze (20-22 marzo 2024). In tale occasione l'Autorità ha proposto agli insegnanti delle diverse regioni italiane di costruire un percorso didattico allo scopo di diffondere i princìpi e i valori connessi al diritto alla *privacy* e alla protezione dei dati allo scopo di aiutare i più giovani a sapersi muovere in rete.

È partito dal sud Italia il *Privacy Tour* 2024, ovvero l'iniziativa lanciata dal Garante per coinvolgere, anche in luoghi piuttosto disagiati, soggetti pubblici e privati in percorsi di sensibilizzazione ed approfondimento sui temi della protezione dati ed uso responsabile del web e delle tecnologie. La prima tappa del simbolico *Tour* è stata Messina, nelle giornate dell'11 e 12 aprile 2024. All'iniziativa hanno aderito Ferrovie dello Stato italiane, Fondazione FS italiane, Fondazione Magna Grecia, Fondazione Bonino-Pulejo, Università di Messina, Google, Meta e Società Editrice Sud Gazzetta del Sud-Giornale di Sicilia. L'iniziativa è poi proseguita nel corso dell'anno nelle città di Catania, Cosenza, Lecce, Napoli, L'Aquila, Pescara, Teramo, Camerino, Ancona, Orio al Serio e Chiavenna.

Il 27 maggio presso la Fondazione Parchi Monumentali Bardini e Peyron a Villa Bardini di Firenze si è svolta la terza edizione di "*State of Privacy-Focus* sull'IA", l'evento-dialogo del Garante con i rappresentanti dei principali *stakeholder* pubblici e privati sul futuro della protezione dei dati e sui problemi connessi allo sviluppo delle più recenti tecnologie. L'incontro, organizzato in collaborazione con le Università di Firenze e Roma Tre e la Fondazione CR Firenze, si è aperto con gli interventi di tre importanti *speaker*: Luciano Violante, Presidente Fondazione Leonardo-Civiltà delle Macchine ETS; Francesco Caio, Presidente Caio *Digital Partners* e Professore aggiunto MIP-*Graduate School of Management* Politecnico di Milano; Luigi Rebuffi, Segretario generale ECSO-*European Cyber Security Organisation*.

I lavori sono poi proseguiti nell'ambito di tre tavoli tematici sulle implicazioni dell'IA rispetto a "economia e sostenibilità", "diritti ed etica", "sicurezza e geopolitica", ai quali hanno partecipato esponenti di diversi settori. I tre tavoli sono stati coordinati rispettivamente dai componenti del Garante Agostino Ghiglia e Guido Scorza e dal costituzionalista Andrea Simoncini.

Gli eventi

Nelle giornate del 9, 10 e 11 ottobre 2024 si è svolta a Roma la riunione delle autorità di protezione dati dei paesi G7 organizzata dal Garante italiano, il cui tema è stato "La *privacy* nell'era dei dati". A tale evento hanno partecipato i componenti del Collegio del Garante italiano e le autorità competenti di Canada, Francia, Germania, Giappone, Regno Unito e Stati Uniti d'America, insieme al CEPD e al GEPD.

Nel corso dell'evento sono state affrontate varie tematiche di estrema rilevanza e sono state approvate importanti dichiarazioni, in continuità con la "Dichiarazione sull'IA generativa" adottata dal G7 *Privacy* di Tokyo nel 2023. Con l'invito alla prosecuzione del dialogo, le autorità hanno convenuto sull'importanza di adottare garanzie adeguate per i minori nell'uso dell'IA, nonché di progettare una tecnologia funzionale ad assicurare la loro crescita libera e armonica. Su questo tema, affrontato anche nell'ambito delle tecnologie emergenti, i Garanti hanno ribadito l'esigenza che la progettazione di tali tecnologie, ancor prima dell'uso, sia tale da porle davvero al servizio dell'uomo. Nel corso del dibattito è stata poi sottolineata la necessità di adottare politiche sull'innovazione che comprendano anche un'adeguata educazione digitale, fondamentale per la formazione soprattutto dei minori. Si è, inoltre, concordato sull'opportunità di esprimere ai Governi l'auspicio del riconoscimento di un ruolo adeguato alle autorità di protezione dei dati nel sistema complessivo di *governance* dell'IA. I Garanti, infine, hanno deciso di svolgere

un monitoraggio sugli sviluppi legislativi dell'IA e il ruolo delle autorità *privacy* all'interno delle giurisdizioni coinvolte.

Questo, come altri obiettivi, sono contenuti nell'*Action Plan*, il documento che guarda al futuro del G7 stabilendone i propositi e le aree tematiche che saranno oggetto dei lavori nei prossimi anni. Il G7 *Privacy* 2025 sarà ospitato dall'autorità federale canadese.

24.2. *I prodotti informativi*

Nel corso del 2024 sono stati diffusi 50 comunicati stampa e 15 *Newsletter.*

La *Newsletter* del Garante è una pubblicazione periodica, registrata al Tribunale di Roma, giunta al XXVI anno di diffusione (per un totale di 565 numeri e 1.817 notizie). È inviata in via telematica a redazioni, professionisti, amministrazioni pubbliche, imprese e semplici cittadini che ne fanno esplicita richiesta o si iscrivono *online* sul sito dell'Autorità.

La *Newsletter* è da anni uno strumento conosciuto ed apprezzato che l'Autorità utilizza per illustrare e divulgare i più importanti provvedimenti adottati in vari settori, la sua attività in ambito nazionale, europeo ed internazionale, le molteplici iniziative legate alla protezione dei dati personali e alla tutela dei diritti fondamentali. Tra i numerosi provvedimenti adottati dal Garante viene operata una scelta tra quelli di maggiore interesse pubblico il cui testo viene rielaborato in chiave giornalistica.

Sul sito è sempre possibile consultare l'archivio tematico della pubblicazione che raccoglie, per categorie, i 26 anni di articoli prodotti dalla redazione. *Online* è consultabile anche l'intero archivio dei comunicati stampa.

Tra le attività di divulgazione anche quest'anno il Garante ha pubblicato 12 numeri del GPDPDigest, il magazine *online* del Garante che raccoglie mensilmente i principali interventi e le campagne di comunicazione dell'Autorità, nonché una sintesi delle principali attività di CEPD, GEPD e una rassegna di comunicati della CGUE in tema di protezione dei dati e di educazione digitale.

24.3. *Il sito istituzionale, i prodotti multimediali e le pubblicazioni*

Nel 2024 sono stati incrementati il numero e la varietà dei prodotti di comunicazione digitale destinati alla diffusione tramite il sito web e i canali *social media* e di messaggistica del Garante. Particolare attenzione è stata rivolta all'aspetto creativo e qualitativo, con la ricerca e lo sviluppo di nuovi *format* e stili allineati alle più recenti e avanzate tendenze della comunicazione digitale. Quasi tutti i *format* e i contenuti sono stati ideati e sviluppati *in house* con le risorse interne.

Tra i temi principali si possono ricordare la sensibilizzazione sull'importanza della protezione dei dati, l'educazione digitale, l'informazione sui rischi e sulle buone pratiche nel campo della cybersicurezza, dell'IA, della conoscenza dei diritti e dei principali adempimenti connessi alla normativa in materia di protezione dati.

Nell'anno di riferimento la produzione di video è sensibilmente aumentata, sia per andare incontro ai nuovi *trend* del consumo digitale, sia per valorizzare le potenzialità dei canali *social*, in particolare di Instagram e di YouTube. Sono stati in particolare realizzati 52 video tutti *in house* (con 2 sole eccezioni) tra cui interviste, *teaser*, *tutorial*, video informativi e promozionali, montaggi e rielaborazione di eventi.

Il Garante è stato anche impegnato nello sviluppo di campagne informative integrate e multicanale che hanno portato alla creazione di nuove sezioni tematiche del sito web

del Garante, di *vademecum* e di contenuti *social*, tra cui in particolare, la scheda sui modelli di progettazione ingannevoli (*Dark Pattern*), su *"dating online"*, scuola, *sharenting* e su "*app* e dispositivi *fitness tracker*".

Sono stati pubblicati 2.500 contenuti sul sito web del Garante e circa 2.240 sui profili *social media* dell'Autorità su LinkedIn, YouTube, Telegram, Instagram e X. Importante anche la crescita del numero di *follower* totali dei profili *social media* e di messaggistica che ha raggiunto il numero complessivo di 102.529 (+11,2% rispetto al 2023). Sul sito web dell'Autorità sono state create *ex novo* o significativamente aggiornate 31 pagine tematiche.

Sul fronte editoriale si segnala, in particolare, l'ideazione, la progettazione grafica e l'impaginazione del volume "La protezione dei dati personali - Normativa essenziale" in edizione aggiornata.

Tutte le questioni sulle quali il Garante è intervenuto hanno ricevuto costante attenzione dai *media*. 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 temi legati alla *privacy* sono state 6.102, quelle relative all'attività del Garante 4.829. Gli articoli aventi per oggetto interviste, interventi e dichiarazioni dei componenti del Collegio del Garante sono state 62 su stampa e web, mentre 60 su radio e TV. Infine, 1.516 sono stati gli articoli relativi ai comunicati stampa e 703 quelli relativi agli argomenti trattati nelle *Newsletter*.

24.4. *Le manifestazioni e i convegni*

A partire dal 2007, il 28 gennaio di ogni anno, viene celebrata in tutta Europa la Giornata europea per la protezione dei dati personali, promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le autorità europee per la *privacy* e finalizzata a sensibilizzare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali.

Il Garante ha dedicato la giornata europea 2024 alle forme di violenza *online*. Il Convegno, intitolato "Violenza della rete, violenza nella rete", si è svolto in presenza ed in diretta *streaming* presso la Sala del Refettorio di Palazzo San Macuto della Camera dei deputati. L'obiettivo dell'evento è stato quello di approfondire i pericoli legati all'utilizzo della rete che troppo spesso è "il teatro" dove si manifestano le forme di violenza più svariate contro la persona e la sua dignità. Molte persone intessono con le nuove tecnologie un rapporto quasi osmotico, al punto da voler riprodurre in rete la propria vita, anche al prezzo di quella degli altri. Si rischia così di confondere la vita con la sua rappresentazione, la persona con l'*avatar*, il corpo con la sua immagine, fino a ridurre anche la percezione della "violenza". Ai lavori, ai quali hanno preso parte i componenti del Collegio, hanno partecipato Giuliano Amato, Presidente emerito della Corte costituzionale, Donatella Stasio, giornalista, Vittorio Lingiardi, psichiatra e psicanalista, ordinario dell'Università La Sapienza di Roma; Giovanni Melillo, Procuratore nazionale antimafia e antiterrorismo; Marco Tarquinio, giornalista, già direttore di Avvenire; Maria Prodi, docente di filosofia e dirigente scolastica.

Regolamentazione e sfide future dell'IA sono stati i temi trattati dal Collegio del Garante nel corso della sessione italiana del "*Privacy Symposium*", la conferenza internazionale che annualmente organizza l'omonima manifestazione. All'evento, ospitato dalla Camera di commercio di Roma presso il Tempio di Adriano, hanno preso parte rappresentanti del Consiglio d'Europa, del Parlamento europeo e delle principali autorità di protezione dati europee ed extra-europee. Durante la giornata sono stati messi a fuoco alcuni tra gli aspetti più dirimenti dell'IA, dai rischi alle opportunità di

una tecnologia così rivoluzionaria, fino alle priorità della cooperazione internazionale.

Ad aprile, presso la Fondazione Konrad Adenauer sul lago di Como, il Garante italiano ha incontrato il Commissario federale per la protezione dei dati e la libertà di informazione tedesco, Ulrich Kelber. L'evento è stata l'occasione per un proficuo scambio di opinioni su temi attuali e di reciproco interesse tra rappresentanti ed esperti delle due Autorità, tra i quali *age verification* per i più piccoli e IA. Nel corso del *meeting* sono state trattate anche le questioni riguardanti il modello "*Pay-or-ok*", ossia il servizio che condiziona l"accesso ai contenuti *online* alla sottoscrizione di un abbonamento o in alternativa alla prestazione del consenso all"uso dei propri dati ai fini di profilazione.

Il 3 luglio, presso la Sala della Regina della Camera dei deputati, alla presenza di deputati e senatori, di ministri, rappresentanti delle istituzioni, delle imprese e delle associazioni di categoria si è svolta la cerimonia di presentazione della Relazione sull'attività svolta dal Garante nell'anno 2023. Sono stati illustrati i diversi e delicati fronti sui quali l'Autorità è stata impegnata nel far rispettare i diritti fondamentali delle persone e i principi alla base della legislazione in materia di *privacy*. Come di consueto, la cerimonia è stata trasmessa 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.

24.5. *L'attività internazionale*

L'Autorità ha svolto una rilevante attività unitamente al gruppo di comunicatori istituito presso il CEPD per realizzare attività coordinate di comunicazione, con la condivisione, tra l'altro, di comunicati stampa e la gestione comune dei casi con valenza transnazionale.

Il Garante ha contribuito direttamente a numerose attività di comunicazione e sensibilizzazione, quali, tra le altre: produzione delle *news* per la sezione italiana del sito CEPD in materia di attività di *enforcement*; collaborazione con gruppi di lavoro specifici del CEPD impegnati in azioni di coordinamento e raccolta di elementi informativi; contributo all'avvio del progetto di comunicazione del CEPD dedicato alle piccole e medie imprese; collaborazione all'aggiornamento delle statistiche CEPD; collaborazione allo sviluppo di nuove linee guida condivise per le attività di comunicazione sui casi transfrontalieri.

Da segnalare, infine, le attività di comunicazione relative al Progetto ARC II (cfr. cap. 21.6).

24.6. *L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi*

Nel corso del 2024, l'Autorità ha continuato a curare, attraverso il Servizio per le relazioni con il pubblico, l'informazione sulle disposizioni in materia di diritto alla protezione dei dati personali e sulle relative modalità di tutela, anche mediante un servizio di ascolto telefonico e la posta elettronica, riscontrando, quotidianamente, quesiti di varia natura provenienti da enti pubblici e privati e da cittadini, spesso di rilevante complessità e delicatezza. Quanto al ricevimento del pubblico presso la sede, in un'ottica di semplificazione e al fine di facilitare l'utente, è stata introdotta la possibilità di fornire l'assistenza necessaria tramite collegamento da remoto o appuntamento telefonico, riservando il ricevimento in presenza ai soli casi più delicati.

24

Il Servizio per le relazioni con il pubblico ha continuato a rappresentare un punto essenziale di contatto dei cittadini con l'Autorità e, contestualmente, ha svolto anche una funzione di filtro curando, laddove possibile, il diretto riscontro delle richieste pervenute, anche sulla base delle indicazioni e della documentazione fornita dai Dipartimenti e Servizi. Nel periodo in esame, numerose sono state le richieste pervenute con riguardo a una pluralità di tematiche da parte non solo di cittadini interessati, ma anche da avvocati e consulenti, giornalisti, funzionari di enti pubblici, RPD, studenti/ricercatori, in particolare nei settori sanitario, lavorativo e scolastico. L'interesse degli utenti rispetto a tali temi è dimostrato dai dati numerici relativi ai contatti con il Servizio, che ammontano in totale a circa 16.045, di cui 10.682 *e-mail*, circa 5.200 via telefono, 133 fascicoli e 30 visitatori (cfr. parte IV, tab. 15).

Oltre all'assistenza giuridica all'utenza, il Servizio ha operato quale *front office* per le richieste inerenti ai servizi telematici attivi sul sito istituzionale (in particolare, il servizio di comunicazione dei dati di contatto dell'RPD, il servizio telematico dedicato al *data breach*, le segnalazioni di comunicazioni indesiderate e quelle per prevenire il fenomeno del *revenge porn*), procedendo al riscontro diretto delle richieste in costante coordinamento con l'Ufficio.

In conformità ai principi di semplificazione e trasparenza amministrativa, nel 2024 il Servizio ha altresì curato un ulteriore aggiornamento delle note-tipo di riscontro sulle tematiche ricorrenti, nonché la predisposizione di nuove note dedicate a specifici temi giuridici (tra le altre sull'accesso ai dati di traffico telefonico e telematico, sul trattamento dei dati in caso di dimissione ospedaliera cd. SDO, sulle ricette mediche dematerializzate, sulle *app* mediche, sulle specifiche tutele in caso di pazienti positivi all'HIV, sul fotosegnalamento, sulle *app* per la timbratura sui luoghi di lavoro, sulle richieste di categorie particolari di dati in ambito lavorativo, sull'utilizzo dei cellulari a scuola, sull'accesso ai dati bancari con particolare riguardo alla dichiarazione di consistenza) utilizzando un linguaggio chiaro e sintetico, pur mantenendo i riferimenti normativi specifici atti a consentire all'utente le tutele necessarie.

Per far fronte al numero crescente di richieste provenienti da utenti stranieri, anche alla luce della dimensione sempre più europea ed internazionale dell'Autorità, è stata avviata un'attività di predisposizione di note di riscontro standard in lingua inglese in relazione alle tematiche più ricorrenti.

In linea con l'attenzione dell'Autorità rivolta all'IA e altre nuove tecnologie, è stata predisposta una scheda semplificata, utilizzabile anche come nota-tipo, dedicata a queste tematiche, anche in un'ottica di implementazione di una comunicazione più efficace, senza tralasciare le indicazioni specifiche e normative utili all'utenza.

Si è dato pronto riscontro a molteplici richieste su fascicoli assegnati ad altre unità organizzative (oltre 1.000 *e-mail*). Tra le tematiche di carattere generale esaminate direttamente, si segnalano, in primo luogo, quelle concernenti le forme di tutela (circa 1.300 *e-mail* ricevute) e gli adempimenti previsti dal RGPD (oltre 2.300 *e-mail* hanno riguardato la designazione del RPD e la relativa procedura *online* realizzata dal Garante per la comunicazione dei dati di contatto dello stesso).

Altre questioni oggetto di interesse hanno riguardato i trattamenti in ambito pubblico e privato di dati personali nei seguenti settori: lavoro (oltre 230 *e-mail*); videosorveglianza (circa 400 *e-mail*); sanità e ricerca scientifica (oltre 300 *e-mail*); scuola (circa 180 *e-mail*); tecnologie digitali (oltre 450 *e-mail*), nonché in ambito giornalistico, con riferimento alle richieste di deindicizzazione dei dati personali dai motori di ricerca (oltre 100 *e-mail*).

III

L'UFFICIO DEL GARANTE

25 Attività di studio e documentazione

Attività di studio, documentazione e supporto giuridico

L'attività di studio e ricerca ha mirato principalmente a garantire l'aggiornamento costante e puntuale del personale dell'Autorità su questioni tecnico-giuridiche di interesse, nonché a fornire supporto su questioni specifiche volta per volta poste all'attenzione dell'Autorità.

Oltre che attraverso un "Osservatorio", ad uso interno, avente cadenza mensile e comprendente sezioni di giurisprudenza e dottrina, nazionale e internazionale, in materia di protezione dati, tale aggiornamento è stato garantito attraverso il monitoraggio di contributi dottrinali e di altro genere in rapporto a specifiche tematiche sulle quali l'Autorità ha operato con particolare intensità nel corso del 2024, tenendo conto anche delle fattispecie più frequentemente esaminate; fra queste, menzioniamo in primo luogo le applicazioni connesse all'intelligenza artificiale, nelle sue molteplici connotazioni, alla luce del dibattito in corso in sede unionale e nazionale. L'attenzione si è concentrata, inoltre, sulle tematiche del diritto di accesso, nelle sue molteplici declinazioni, e sulle implicazioni della normativa in materia di *whistleblowing*.

Approfondimenti sono stati realizzati con riguardo a domande di rinvio pregiudiziale rivolte alla Corte Ue che hanno investito la materia della protezione dei dati e rispetto alle quali l'Autorità, attraverso la sinergia di tutte le articolazioni interne interessate, ha potuto fornire contributi qualificati nelle sedi competenti.

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 sull'attività svolta nel 2023. La Relazione contiene informazioni puntuali con riguardo all'attività provvedimentale, sanzionatoria e comunicativa del Garante, nonché all'ambito europeo ed internazionale, e offre un quadro sintetico, ma esaustivo, dei numeri relativi a tale attività.

In conformità a quanto previsto dall'art. 22, d.l. n. 90/2014 convertito in l. 11 agosto 2014, n. 114, la Relazione annuale del Garante è stata altresì trasmessa alla Corte dei conti.

26 La gestione amministrativa e dei sistemi informatici

26.1. *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 e ad una prudente programmazione delle spese, nel rispetto delle specifiche disposizioni normative 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. La fonte pressoché unica del finanziamento del Garante è rappresentata dal contributo posto a carico del bilancio dello Stato, in aggiunta al quale sono previsti solo marginali importi a titolo di rimborsi. La somma erariale è stata quantificata dalla l. 30 dicembre 2023, n. 213 recante bilancio di previsione dello Stato per l'anno finanziario 2024 ed il bilancio pluriennale per il triennio 2024-2026 che ha previsto uno stanziamento di euro 45.301.252 per il 2024, di euro 45.611.775 per il 2025 e di euro 45.931.360 per il 2026.

Il contributo statale a consuntivo 2024 è pari a euro 50.301.252 imputabili ai maggiori trasferimenti erariali disposti dal legislatore riferibili a rifinanziamenti e riprogrammazioni delle dotazioni finanziarie.

Ulteriori somme sono da ascrivere a titolo di entrate proprie del Garante per complessivi euro 143.519 riferibili in parte a rimborsi per trasferte effettuate dal personale nell'ambito degli organismi europei.

Va sottolineato, inoltre, 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

Sotto il profilo più strettamente contabile, il risultato finanziario dell'esercizio ha fatto registrare un avanzo di amministrazione di euro 9,4 milioni, 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 selettive per l'immissione in servizio del nuovo personale, a seguito di apposita modifica della pianta organica, hanno richiesto tempi 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 2024, al netto delle partite di giro pari a euro 12,7 milioni, le entrate acquisite dall'Autorità, comprensive dei trasferimenti a carico del bilancio dello Stato, sono state di complessivi euro 50,4 milioni a fronte delle quali sono stati registrati impegni di spesa per euro 41 milioni. Rispetto al precedente esercizio finanziario, l'incremento delle entrate complessive registrato nel 2024 è stato

di euro 3 milioni, con una variazione di circa il 6,4%. Con riferimento alla spesa, invece, gli oneri registrati nell'anno, pari a euro 41 milioni risultano in aumento di euro 2,8 milioni rispetto al 2023, con uno scostamento di circa il 7,4%. La spesa complessiva è da imputare in massima parte alla gestione corrente, nella misura di euro 40,9 milioni, 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 2024 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 parte IV, tab. 25, 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.

La complessiva gestione è stata assoggettata ai controlli dell'organo interno preposto alla verifica della regolarità amministrativo-contabile, che non ha rilevato irregolarità. Il rendiconto della gestione è stato trasmesso alla Corte dei conti, nel rispetto di puntuali disposizioni legislative, per le verifiche di competenza.

26.2. *L'attività contrattuale e le procedure di affidamento*

In materia di contrattualistica pubblica, nel 2024 sono state consolidate le nuove procedure e le relative competenze tecnico-giuridiche conseguenti alle profonde innovazioni determinate dall'introduzione del nuovo codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36) e dall'avvio dell'Ecosistema nazionale di approvvigionamento digitale previsto all'art. 22 dello stesso. Tale novità, che ha segnato una profonda trasformazione nel panorama dell'*e-procurement* e degli appalti, ha comportato considerevoli mutamenti nell'operatività delle stazioni appaltanti pubbliche, con particolare riferimento all'obbligatorietà dell'utilizzo delle piattaforme telematiche e alla loro interconnessione con la Banca dati nazionale dei contratti pubblici, nonché al regime della trasparenza e pubblicità degli atti di gara. Tali rilevanti modifiche non hanno tuttavia colto impreparato l'Ufficio del Garante, già inserito dall'ANAC nell'elenco delle stazioni appaltanti qualificate ad operare in appalti di servizi e forniture per importi fino a 5 milioni di euro. Già dotata di una piattaforma certificata di negoziazione, l'Autorità ha potuto difatti svolgere la propria attività contrattuale affiancandola all'altra piattaforma in uso, ovvero quella predisposta da CONSIP sul portale Acquistinretepa.it. Occorre purtroppo sottolineare come quest'ultima, nella fase di prima applicazione del predetto Ecosistema e in particolare durante il primo semestre 2024, abbia presentato notevoli disfunzioni che, seppure gradualmente risolte con riparazioni incrementali, hanno reso più complessa la transizione degli utilizzatori finali verso le nuove modalità operative, determinando in definitiva un notevole ampliamento delle attività di natura tecnico-amministrativa da parte dell'Autorità. Nonostante la descritta cornice operativa, circa tre quarti del numero di

contratti sottoscritti è stato negoziato all'interno della piattaforma CONSIP, per un valore economico pressoché pari all'80% del valore totale dei contratti stipulati. Nel rispetto dei principi fondamentali del codice dei contratti pubblici (*in primis* quelli di risultato, fiducia e concorrenza) l'Autorità, ove possibile, ha anche continuato a sollecitare il mercato con celeri procedure comparative, salvo i casi in cui si è ritenuto preferibile procedere con maggiore speditezza o nell'ambito di modesti importi contrattuali.

Il processo di adeguamento alla nuova disciplina del codice dei contratti si è concretizzato, sotto il profilo della regolamentazione interna, attraverso l'adozione, da parte del Collegio, di due importanti deliberazioni: la prima concernente il nuovo regolamento in materia di nomina e funzionamento delle commissioni giudicatrici e dei seggi di gara previsti dal codice dei contratti pubblici (provv. 20 giugno 2024, n. 370, doc. web n. 10132592) e la seconda relativa alla disciplina dei contratti di appalto del Garante aventi importo inferiore alle soglie europee (provv. 27 novembre 2024, n. 836, doc. web n. 10101560). Tale apparato regolatorio ha adeguato i meccanismi di funzionamento degli organi incaricati delle valutazioni amministrative e tecniche delle offerte nell'ambito di procedure comparative, nonché disciplinato alcuni profili relativi ai contratti sotto soglia secondo le previsioni del codice degli appalti (rotazione degli affidamenti, controlli a campione ecc.); è stata altresì soppressa la figura dell'Ufficiale rogante presso l'Autorità, divenuta sostanzialmente obsoleta.

Programmazione

In materia di programmazione delle richieste di acquisto di beni e servizi, sono stati apportati i necessari adeguamenti organizzativi connessi sia alla mutata frequenza di programmazione – passata da biennale a triennale – sia al nuovo limite minimo di importo, pari a euro 140.000,00.

Procedure di affidamento

Analizzando, nello specifico, l'attività strettamente contrattuale, la procedura di maggior rilievo sotto il profilo dell'impegno profuso è stata rappresentata da una gara aperta, in ambito comunitario, finalizzata all'affidamento del servizio di assistenza in materia di amministrazione digitale e protocollo informatico, per la quale è stata ricevuta una sola offerta, successivamente esclusa a seguito delle verifiche effettuate; la nuova gara relativa a tale servizio è stata pertanto pubblicata nel mese di dicembre 2024. Degni di nota, sia in termini di impegno economico che di coinvolgimento dell'Ufficio, sono stati poi i contratti riguardanti i servizi di pulizie ed ausiliariato, i servizi di manutenzione di impianti e la locazione della sede, tutti tra loro interconnessi per evidenti ragioni organizzative e logistiche. In particolare, l'Ufficio ha avviato un articolato processo di comparazione, tenendo conto degli strumenti di acquisto disponibili: la Convenzione CONSIP "*Facility management* 4", l'Accordo quadro CONSIP "grandi immobili", nonché la proroga del vigente contratto, nei termini già previsti in sede di gara effettuata sul sistema dinamico della p.a. di CONSIP.

Molto rilevante sotto il profilo non solo economico, ma anche organizzativo, è stato il contratto relativo alla migrazione di infrastrutture e servizi telematici presso il neocostituito Polo strategico nazionale (PSN), stipulato a gennaio 2024 in adesione alla Convenzione quadro sottoscritta dalla Presidenza del Consiglio dei ministri e parzialmente finanziato attraverso fondi comunitari; la migrazione in esame, di strategica rilevanza per l'Autorità, ha determinato un'importante revisione dei servizi e delle forniture in ambito ICT ad essa connesse ed una conseguente, articolata attività contrattuale (contratti di assistenza sistemistica, acquisti di licenze informatiche, sviluppo sito web istituzionale, ecc.).

Il 2024 è stato l'anno di presidenza italiana del G7, nel cui ambito l'Autorità si è impegnata nell'organizzazione del cd. G7 *Privacy* (cfr. 21.3); la specificità dell'oggetto e la necessità di acquisire la collaborazione di un operatore economico competente e

affidabile hanno indotto il Garante ad avvalersi del pratico strumento della trattativa diretta sul MEPA di CONSIP, invitando ad offrire l'impresa aggiudicataria di uno dei lotti dello specifico Accordo quadro messo a disposizione da CONSIP stessa per la gestione degli eventi connessi al G7.

L'anno in esame è stato, inoltre, contraddistinto dal notevole aumento di personale avvenuto all'interno dei limiti stabiliti dalla pianta organica: le procedure di selezione e le fasi concorsuali hanno richiesto ampi sforzi organizzativi anche in materia di contratti, al fine di acquisire i servizi necessari per tali adempimenti (sedi, dispositivi di supporto, servizi connessi). Sempre in materia di risorse umane, altra procedura di approvvigionamento di rilevanza quantitativamente significativa ha riguardato l'adesione alla convenzione CONSIP concernente il servizio sostitutivo di mensa mediante buoni pasto.

È infine proseguito il consueto supporto offerto all'attività informativa e di comunicazione istituzionale del Garante, mediante la stipula di diversi contratti, tra i quali si menziona quello avente ad oggetto la realizzazione di uno *spot* televisivo e di uno *spot* radiofonico sullo *sharenting* e l'educazione digitale degli adulti.

La sede del Garante e i contratti connessi

L'Autorità, in considerazione della necessità di rimodulare la logistica della propria sede in funzione del previsto incremento di personale, ha proseguito le attività volte ad individuare soluzioni soddisfacenti rispetto ai requisiti attesi e alle proprie disponibilità economiche.

Preso atto della indisponibilità sul mercato di idonee soluzioni allocative, sia in termini di acquisto che di locazione di un immobile, l'Autorità ha espletato gli adempimenti finalizzati al rinnovo dell'esistente contratto di locazione, in particolare ai fini della corretta applicazione delle disposizioni in materia di locazione di immobili della p.a. (art. 16-*sexies*, comma 1, lett. a), d.l. 21 ottobre 2021, n. 146, convertito con modificazioni dalla l. 17 dicembre 2021, n. 215).

Per quanto riguarda la manutenzione e l'efficientamento logistico dell'immobile attualmente in uso, sono stati effettuati interventi di ottimizzazione degli spazi, sempre nel rispetto degli standard di sicurezza previsti dal d.lgs. n. 81/2008 e successive modifiche. A fronte delle esigenze rappresentate dalla società proprietaria, è stata assicurata la necessaria assistenza per consentire l'attività di manutenzione e gestione dell'immobile anche in relazione ad interventi urgenti. Si è proceduto agli aggiornamenti dell'inventariazione ed alla valutazione dello stato dei beni mobili presenti all'interno dei locali ed è stata portata a termine la realizzazione di un magazzino dedicato alla custodia dei beni librari.

26.3. *L'organizzazione dell'Ufficio*

Nell'anno di riferimento è proseguito il processo di attuazione del piano strategico dell'Autorità per il pieno raggiungimento degli obiettivi programmati, secondo una duplice linea di azione mirata, dal lato interno, a rafforzare l'organico e reingegnerizzare i processi lavorativi e, dal lato esterno, a valorizzare forme di collaborazione con *stakeholders* istituzionali e sociali che operano nei rispettivi ambiti di competenza su tematiche attinenti anche alla protezione dei dati personali.

Il rafforzamento dell'Autorità

È proseguito il processo di completamento della dotazione organica ai fini dell'attuazione del piano strategico dell'Autorità per il pieno raggiungimento degli obiettivi demandati sul piano nazionale e internazionale. Il rafforzamento dell'organico è stato realizzato con l'assunzione in ruolo di 37 unità delle varie aree professionali (dirigenti, direttivi, operativi ed esecutivi), a seguito dell'espletamento delle relative procedure di concorso pubblico (cfr. parte IV, tabb. 23-24).

Lavoro agile

Sulla base dell'esperienza maturata negli anni precedenti, l'Autorità ha ridefinito l'istituto del lavoro agile come modalità regolata, strutturale e flessibile di svolgimento della prestazione lavorativa, a conclusione di un percorso condiviso con le organizzazioni sindacali che ha portato alla stipula nel corso del 2024 di un accordo che ha regolamentato, a regime, le modalità di svolgimento del lavoro agile, in coerenza con la disciplina di riferimento, comprese le disposizioni normative a tutela dei lavoratori fragili.

Si è reso successivamente necessario procedere alla stipula dei contratti individuali per tutto il personale aderente e ai numerosi adempimenti conseguenti, nell'ottica di assicurare coerenza con le programmazioni delle attività dell'Ufficio a tutti i livelli.

Nel corso dell'anno si è provveduto a monitorare le modalità applicative del lavoro agile, al fine di individuare eventuali correttivi finalizzati ad assicurare il raggiungimento di sempre più elevati standard di efficienza lavorativa, anche mediante l'adozione di misure organizzative di bilanciamento con le esigenze di tutela della salute dei lavoratori maggiormente esposti.

La percentuale del personale che ha aderito all'istituto del lavoro agile è stata molto elevata, a conferma della adeguatezza di tale modalità di lavoro come metodologia organizzativa in grado di conciliare le necessità d'istituto con le esigenze personali dei lavoratori.

Relazioni sindacali

Con riferimento alle trattative volte alla definizione a regime della disciplina del lavoro agile, la relativa attività dell'Ufficio si è conclusa nel mese di febbraio con la stipula dell'accordo. Sono state inoltre affrontate, di concerto con le organizzazioni sindacali, varie questioni negoziali, riguardanti in particolare le procedure concorsuali per l'assunzione di personale, l'individuazione di maggiori spazi per gli uffici del Garante, il *welfare* aziendale e le questioni previdenziali.

Sicurezza sul lavoro

In tema di sicurezza e salute dei lavoratori, sono proseguite le attività di gestione dei profili di sicurezza individuali, soprattutto con riferimento all'esecuzione del piano di visite mediche per monitorare lo stato di salute psicofisica dei lavoratori, secondo le modalità stabilite dal d.lgs. n. 81/2008, anche in rapporto alle istanze di estensione del lavoro agile in favore dei lavoratori maggiormente esposti per ragioni di salute. L'Autorità ha ulteriormente incrementato il numero delle unità componenti le squadre di primo soccorso e di antincendio, al fine di assicurare le migliori condizioni di sicurezza all'interno della propria sede.

E' stata altresì rafforzata, anche a livello contrattuale, la collaborazione del Responsabile del servizio di prevenzione e protezione e del medico competente, con l'obiettivo di assicurare la migliore gestione degli spazi in considerazione delle nuove assunzioni.

A seguito del predetto reclutamento del personale effettuato alla fine del 2024, sono state avviate le procedure previste dal citato d.lgs. n. 81/2008 per la formazione obbligatoria anche con l'intento di formare sin da subito ulteriori dipendenti per le squadre antincendio e primo soccorso.

Formazione del personale

Il Garante ha attuato soluzioni formative innovative per la crescita delle competenze individuali e di gruppo, coerentemente con le esigenze manifestate dai rispettivi Servizi e Dipartimenti. Allo scopo, è stato prorogato il rapporto collaborativo con la Scuola nazionale dell'amministrazione (SNA), il cui catalogo è costantemente aggiornato anche grazie al lavoro svolto dal Club dei Formatori della medesima Scuola, un progetto al quale prendono parte anche i referenti dell'Autorità al fine di migliorare il grado di coerenza della programmazione didattica della SNA con le effettive esigenze formative delle amministrazioni e dello stesso Garante. Contestualmente, l'Autorità ha aderito ai corsi compresi nell'iniziativa, gestita dall'INPS, denominata Valore PA.

L'Autorità ha inoltre favorito l'utilizzo da parte del personale della Piattaforma SYLLABUS in adesione alle indicazioni fornite con la direttiva del Ministro per la p.a. del 23 marzo 2023 in materia di formazione, relativa alla crescita delle competenze funzionali alla transizione digitale, ecologica e amministrativa promosse dal PNRR.

Per la formazione obbligatoria relativa alla normativa di settore, si segnala in particolare quella erogata a seguito dell'entrata in vigore del codice dei contratti pubblici (d.lgs. n. 36/2023), per i responsabili unici di progetto e per il personale assegnato alle attività contrattuali, anche tramite sessioni formative erogate a distanza da una società specializzata nel settore (rilevanti per la qualificazione della stazione appaltante presso l'ANAC).

L'impatto economico di bilancio degli indicati strumenti formativi è stato estremamente limitato, grazie un'offerta formativa molto varia, con particolare riguardo alla citata Piattaforma SYLLABUS.

Tali plurime iniziative si sono affiancate all'ordinaria attività di aggiornamento interno effettuata dal Servizio studi e documentazione mediante la predisposizione di *dossier* di documentazione tematici e degli Osservatori *privacy* (pubblicazioni a cadenza mensile) concernenti la raccolta ragionata della normativa e della giurisprudenza eurounitaria e nazionale, nonché mediante ulteriori approfondimenti funzionali a fornire ai dipendenti periodici aggiornamenti in materia di protezione dei dati personali e *privacy* (cfr. par. 25).

Il ricorso ai suddetti percorsi formativi non ha comportato significativi oneri finanziari a carico del bilancio dell'Autorità, permettendo di conseguire un notevole risparmio di spesa a fronte di un incremento quantitativo e qualitativo dell'offerta formativa a beneficio del personale del Garante. Ciò ha anche portato, dopo un attento percorso di sperimentazione e *scouting* tecnologico, all'acquisizione di una soluzione digitale d'avanguardia volta a far convergere su un'unica piattaforma di *e-learning* una pluralità di contenuti didattici interni ed esterni, fruibili dal personale come eventi in diretta o in modalità differita e *on demand.*

Servizio controllo di gestione

Il controllo di gestione presso l'Autorità continua ad incentrarsi sull'analisi periodica degli affari assegnati alle diverse unità organizzative mediante il sistema di protocollazione "Archiflow" e sulla conseguente produzione anche 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**.**

Responsabile della protezione dei dati (RPD)

Dopo l'avvicendamento avvenuto all'inizio del 2024, il nuovo RPD dell'Autorità ha dato corso a una serie di iniziative principalmente mirate a potenziare e razionalizzare le *policy* di protezione dei dati già in essere, anche con il contributo dell'Ufficio. In particolare, è stato riconfigurato e aggiornato il registro dei trattamenti *ex* art. 30 RGPD, del quale una prima versione è stata sottoposta al vaglio dell'Autorità; si è proceduto a una verifica delle misure di sicurezza applicabili, tecniche e organizzative, alla luce dei passi compiuti dall'Autorità in vista della migrazione sopra ricordata verso il PSN. Sono stati curati, come di consueto, i rapporti con i responsabili di trattamento designati volta per volta dall'Autorità in relazione a specifici affidamenti, anche attraverso una serie di interlocuzioni talora di rilevante complessità; è stato messo a punto un "modello" di atto di designazione al quale si è fatto riferimento in tutti i casi esaminati, integrandovi alcune clausole (con particolare riguardo all'eventuale ricorso a sub-responsabili del trattamento) a partire dal modello di atto di designazione approvato dalla Commissione europea con la sua decisione esecutiva 2021/915. Sono state avviate alcune iniziative finalizzate a garantire la formazione del personale su questioni anche basilari in materia di protezione dei dati personali, soprattutto tenendo conto delle assunzioni di personale avvenute nel corso dell'anno di riferimento.

26

Infine, sono proseguiti i proficui incontri organizzati dalla Rete degli RPD delle autorità indipendenti, ospitati in due occasioni presso la sede del Garante, nei quali sono state affrontate, con l'apporto anche del RPD dell'Autorità, questioni di interesse comune e, in particolare, alcune problematiche connesse alla comunicazione e diffusione di dati personali fra soggetti pubblici.

26.4. *"Amministrazione trasparente" e adempimenti relativi alla disciplina anticorruzione*

La disciplina in materia di trasparenza amministrativa e, conseguentemente, le misure (generali e specifiche) finalizzate alla prevenzione di fenomeni suscettibili di essere ricondotti entro l'ampia accezione del termine "corruzione" continuano a trovare attuazione presso il Garante. In particolare, al fine di assicurare il puntuale assolvimento degli obblighi di trasparenza (e agevolare i flussi informativi interni volti anche ad alimentare la sezione "Amministrazione trasparente" del sito web istituzionale), come già segnalato nella precedente Relazione (par. 25.4), l'Autorità ha innovato il processo interno di pubblicazione di dati e documenti previsto dal d.lgs. n. 33/2013 mediante il supporto professionale fornito da una *software house* specializzata in soluzioni SaaS per la p.a. avvalendosi di un applicativo ceduto con la formula del riuso *ex* artt. 68-69 del CAD (nella fattispecie il PAT - Portale amministrazione trasparente di AgID). Oltre ad assicurare in chiave prospettica la tempestiva pubblicazione in un'unica sede delle informazioni rilevanti a far data dalla sua istituzione, nel corso dell'anno sono altresì migrate verso il PAT larga parte delle informazioni contenute nella (preesistente) sezione "Amministrazione trasparente" del sito istituzionale.

Sempre con riguardo ai profili di trasparenza amministrativa, sulla scorta dell'Atto del Presidente ANAC 1° giugno 2024 – che ha integrato e sostituito la delibera ANAC 23 aprile 2024, n. 213 – è stata pubblicata la griglia di rilevazione resa disponibile mediante l'applicativo web realizzato dall'ANAC, la cui redazione, in assenza di OIV o di strutture equivalenti presso l'Autorità, è stata curata dal RPCT che ha altresì provveduto, seppure per circoscritti profili, a rinnovare tale monitoraggio, rendendone pubblici gli esiti, entro il termine fissato da ANAC nel gennaio 2025. Del pari, un quadro sintetico degli aspetti salienti dell'attività svolta nel periodo di riferimento può desumersi dalla relazione annuale del RPCT riferita al 2024, anch'essa oggetto di pubblicazione nel nuovo PAT.

Considerato che, in qualità di autorità amministrativa indipendente, il Garante non è tenuto all'adozione del Piano integrato di attività e organizzazione (PIAO), sono state intraprese le attività prodromiche all'aggiornamento del Piano triennale di prevenzione della corruzione e della trasparenza (PTPCT 2025-2027), che hanno visto il coinvolgimento del personale dirigenziale mediante la compilazione di apposite schede di rilevazione predisposte dal RPCT (del quale, non diversamente da altre figure dirigenziali, si è assicurata la rotazione nell'incarico in forza della delibera del Garante 12 dicembre 2024, n. 793, doc. web n. 10093600). Tale attività, già svolta nell'anno precedente, ha consentito di verificare l'attualità della mappatura dei processi in essere presso l'Autorità e dei relativi rischi; come in passato, tale attività ha altresì consentito di prendere in considerazione alcuni processi in precedenza non analiticamente individuati. A valle di tale complessiva attività, con deliberazione del Garante 30 gennaio 2025, n. 32, è stato adottato il PTPCT 2025-2027.

Con riguardo alla disciplina in materia di accesso civico introdotta con il d.lgs. n. 33/2013 è stato dato tempestivo riscontro a tutte le istanze pervenute all'Autorità nel

2024 (in numero di 17). Ha formato altresì oggetto di tempestivo riscontro (nel 2025) l'unica istanza di riesame pervenuta all'Autorità; infine, non si sono registrate nel corso dell'anno istanze di accesso civico relative a dati soggetti a pubblicazione obbligatoria (*ex* art. 5, comma 1, d.lgs. n. 33/2013).

26.5. *Il settore informatico-tecnologico e la transizione digitale*

Nel corso del 2024 sono stati portati a compimento diversi significativi progetti in ambito IT, tra cui due iniziative, entrambe assistite da finanziamenti del PNRR, che hanno consentito all'Autorità di effettuare un notevole avanzamento verso la *cloudificazione* dei propri servizi e il potenziamento della propria postura di sicurezza.

In particolare, è stata completata nel corso del 2024 la migrazione dei sistemi informatici a supporto del sistema informativo verso l'infrastruttura del PSN, attività che ha previsto complesse fasi di progettazione, di implementazione e di collaudo.

Sono compresi tra i servizi erogati tramite PSN sia quelli relativi alla piattaforma web a supporto del sito istituzionale, che si avvalgono di un'infrastruttura IaaS (*Infrastructure as a Service*) attivata nel primo semestre 2024, sia quelli consistenti nella realizzazione e messa a disposizione di un'infrastruttura ibrida *Housing/Hosting*, federata con l'attuale componente *on premise* e dotata di caratteristiche di resilienza, affidabilità, prestazioni e sicurezza idonee alle sfide della trasformazione digitale, in adesione alla Convenzione della Presidenza del Consiglio dei ministri - Dipartimento per la trasformazione digitale del 24/08/2022, stipulata ai sensi degli artt. 164, 165, 179, 180, comma 3 e 183, comma 15, d.lgs. 18 aprile 2016, n. 50, avente ad oggetto l'affidamento in concessione della realizzazione e gestione di una nuova infrastruttura informatica al servizio della p.a. denominata "Polo strategico nazionale".

Dal novembre 2024 i servizi all'utenza interna e al pubblico, laddove non erogati in forma SaaS tramite infrastrutture *cloud* di qualificati fornitori, sono realizzati tramite un'infrastruttura cloud privata operante nell'ambito del PSN.

Sono stati quindi rivisti i piani di *backup* e *recovery* dei dati, al fine di assicurare la loro maggiore resilienza, nonché l'architettura dei sistemi di protezione perimetrale, potenziati per presidiare la superficie di attacco e affrontare minacce informatiche in continua evoluzione.

Accanto all'attività sull'infrastruttura, che ha consentito anche di dismettere diversi apparati *on premise*, contribuendo alla riduzione significativa dei consumi elettrici dell'Autorità, è stata dedicata particolare attenzione agli aspetti procedurali e organizzativi della cybersicurezza, anche grazie al supporto dell'Agenzia per la cybersicurezza nazionale (ACN), sempre sotto l'egida del PNRR (cfr. avviso pubblico n. 7/2023 per l'erogazione di interventi di potenziamento e miglioramento delle capacità *cyber* degli organi costituzionali e di rilevanza costituzionale, dei ministeri, delle agenzie fiscali, degli enti di regolazione dell'attività economica, delle autorità amministrative indipendenti e degli enti a struttura associativa a valere sul PNRR, Missione 1 – Componente 1 – Investimento 1.5 "*Cybersecurity*").

Il lavoro svolto in quest'ambito nel 2024 ha riguardato l'attuazione, da parte della citata Agenzia, di una campagna di valutazione della postura di sicurezza *cyber* del Garante, preliminare passaggio essenziale per la corretta pianificazione e messa in esercizio delle necessarie misure volte all'innalzamento dei livelli di *cyber* resilienza. Il livello corrente di maturità delle funzioni di sicurezza è stato valutato previa declinazione tanto sulle funzioni del cd. *Framework* nazionale per la *cybersecurity* e la *data protection* – ossia, *Identify, Protect, Detect, Respond, Recover* – quanto sulle più

26

classiche dimensioni proprie della sicurezza delle informazioni quali la definizione di ruoli e responsabilità, la gestione del rischio, la gestione degli incidenti, la gestione degli accessi, la sicurezza delle applicazioni e la formazione del personale. Ancora, nel corso del 2024, e sempre con riferimento all'intervento di cui al citato avviso pubblico n. 7/2023, è stato dato inizio ad un percorso di mappatura, aggiornamento e formalizzazione di alcuni processi rilevanti per la gestione della sicurezza. Tale iniziativa si inserirà poi, durante il 2025, in un più ampio intervento di ridefinizione dei processi per la gestione della sicurezza e della pertinente documentazione, di maturazione degli strumenti tecnologici a supporto e di acquisizione di competenze specifiche per il personale.

Per quanto riguarda gli sviluppi applicativi, sono state implementate *ex novo* oppure reingegnerizzate diverse applicazioni per la gestione interna dei processi di *backoffice* di alcuni procedimenti, tra cui la trattazione dei casi di violazione dei dati (*data breach*) notificati al Garante; la trattazione dei casi di *revenge porn*; le segnalazioni di telefonate indesiderate.

È stata completata l'analisi informatica dei processi relativi alla presentazione di istanze come i reclami e le segnalazioni. Altri interventi hanno riguardato i flussi di rendicontazione delle missioni e il flusso autorizzativo delle richieste di acquisto.

Altre attività meritevoli di menzione comprendono la messa in linea della piattaforma PAT (Portale amministrazione trasparente); lo sviluppo e l'attivazione del portale *web* a supporto del G7 *Privacy*; la messa in esercizio della piattaforma di *e-learning* "GPDP *Academy*" basata sul sistema *open-source* Moodle; lo sviluppo e la diffusione d'uso della piattaforma di virtualizzazione dei *desktop computer* basata su Horizon; l'attivazione di un link *P-t-P* a 10 Gbps, con caratteristiche di alta disponibilità e bassa latenza, per il collegamento della sede di piazza Venezia con l'infrastruttura *datacenter* del PSN.

IV

I DATI STATISTICI

Tabella 1.
Sintesi delle principali attività dell'Autorità

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	835
Risposte ad atti di sindacato ispettivo e di controllo	2
Audizioni del Presidente del Garante o memorie scritte trasmesse al Parlamento	11
Pareri su norme di rango primario statale, delle regioni e delle autonomie *ex* art. 36, par. 4, RGPD	12
Pareri su atti regolamentari e amministrativi *ex* art. 36, par. 4, RGPD	61
Pareri ai sensi dell'art. 36, par. 1, RGPD (valutazione d'impatto sulla protezione dati)	1
Pareri ai sensi dell'art. 110 del Codice per la realizzazione di un progetto di ricerca medica, biomedica e epidemiologica nonché *ex* art. 36 del RGPD	9
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	20
Altri pareri (art. 58, par, 3, RGPD)	1
Approvazione regole deontologiche	1
Provvedimenti collegiali a seguito di reclamo	91
Provvedimenti collegiali a seguito di reclamo con contestuale ordinanza-ingiunzione	123
Provvedimenti collegiali a seguito di segnalazione nonché a seguito di accertamenti d'ufficio	32
Provvedimenti collegiali a seguito di segnalazione nonché a seguito di accertamenti d'ufficio con contestuale ordinanza-ingiunzione	50
Provvedimenti collegiali a seguito di notifica di violazione di dati	17
Provvedimenti collegiali a seguito di notifica di violazione di dati con contestuale ordinanza-ingiunzione	21
Misure correttive e sanzionatorie (art. 58, par. 2, RGPD)	468
Ricorsi giurisdizionali trattati *ex* art. 152, d.lgs. n. 196/2003	74
Opposizioni (trattate) a provvedimenti del Garante	85
Pagamenti derivanti dall'attività sanzionatoria (euro)	24.430.856
Comunicazioni di notizia di reato all'Autorità giudiziaria	16
Delibere dirigenziali in materia di *revenge porn* (adottate ai sensi dell'art. 33-*bis*, reg. Garante n. 1/2019) e ratificate dal Collegio	625
Provvedimenti di approvazione di codici di condotta	4
Violazioni di dati personali notificate	2.204
Accertamenti e controlli effettuati *in loco* (artt. 157-158, d.lgs. n. 196/2003)	130
Riscontri a reclami	4.090
Riscontri a segnalazioni	93.877
Riscontri a quesiti (art. 11, reg. Garante n. 1/2019)	501
Contatti Servizio relazioni con il pubblico	16.045
Reclami transfrontalieri e procedure di cooperazione ("sportello" unico - *ex* art. 60 del RGPD)	704
Procedure di coerenza (*ex* artt. 65-66 del RGPD)	0
Riunioni del Comitato europeo per la protezione dei dati personali	12
Partecipazione a sottogruppi di lavoro del Comitato europeo per la protezione dei dati personali	180
Riunioni e ispezioni autorità comuni di controllo/organismi di supervisione (EUROPOL, SIS II, Dogane, EURODAC, VIS)	21
Riunioni presso il CoE e l'OCSE	27
Conferenze internazionali	24
Altre conferenze e incontri	16
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 1, d.lgs. n. 33/2013	0
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 2, d.lgs. n. 33/2013	17
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

Tabella 2.
Pareri *ex* art. 36, par. 4, RGPD su norme di rango primario statale, delle regioni e delle autonomie

Pareri *ex* art. 36, par. 4, RGPD su norme di rango primario statale, delle regioni e delle autonomie	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	1
Diritti fondamentali	3
Fisco	4
Interesse pubblico	1
Lavoro	1
Sanità	1
Trasporti	1
Totale	**12**

Tabella 3.
Pareri *ex* art. 36, par. 4, RGPD su atti regolamentari e amministrativi resi al Governo

Pareri *ex* art. 36, par. 4, RGPD su atti regolamentari e amministrativi resi al Governo	
Temi	**Riscontri resi nell'anno***
Ambiente	1
Digitalizzazione p.a.	4
Diritti fondamentali	3
Fisco	4
Funzioni di interesse pubblico	7
Giustizia	5
Imprese	1
Istruzione	3
Lavoro	8
PA/ Autorità indipendenti	1
Sanità	10
Totale	**47**

Tabella 4.
Pareri *ex* art. 36, par. 4, RGPD su atti regolamentari e amministrativi resi ad altre istituzioni

Pareri *ex* art. 36, par. 4, RGPD su atti regolamentari e amministrativi resi ad altre istituzioni	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	2
Diritti fondamentali	3
Fisco	4
Funzioni di interesse pubblico	4
Statistica	1
Totale	**14**

(*) inerenti anche ad affari pervenuti anteriormente al 2024

Pareri *ex* art. 36, par. 1, RGPD (valutazione d'impatto sulla protezione dati)	
Temi	**Riscontri resi nell'anno***
Funzioni di interesse pubblico	1
Totale	**1**

Tabella 5.
Pareri *ex* art. 36, par. 1, RGPD (valutazione d'impatto sulla protezione dati)

(*) inerenti anche ad affari pervenuti anteriormente al 2024

Misure correttive e sanzionatorie	
Avvertimenti a titolare/responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare il RGPD (art. 58, par. 2, lett. a))	5
Ammonimenti a titolare/responsabile del trattamento per violazioni RGPD (art. 58, par. 2, lett. b))	93
Ingiunzioni a titolare/responsabile del trattamento a soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal RGPD (art. 58, par. 2, lett. c))	28
Ingiunzioni a titolare/responsabile del trattamento di conformare i trattamenti alle disposizioni del RGPD (art. 58, par. 2, lett. d))	59
Ingiunzioni a titolare del trattamento di comunicare all'interessato una violazione dei dati personali (art. 58, par. 2, lett. e), RGPD)	19
Imposizioni di limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento (art. 58, par. 2, lett. f), RGPD)	39
Ordine di rettifica/cancellazione di dati personali o limitazione del trattamento *ex* artt. 16, 17 e 18 e altre misure previste dall'art. 58, par. 2, lett. g), RGPD	29
Sanzioni amministrative pecuniarie *ex* art. 83 (art. 58, par. 2, lett. i), RGPD)	196
Totale	**468**

Tabella 6.
Misure correttive e sanzionatorie (art. 58, par. 2, RGPD)

Pagamenti derivanti dall'attività sanzionatoria	
Pagamenti spontanei dei contravventori	23.153.233,08
Riscossione coattiva	1.277.623,37
Totale	**24.430.856,45**

Tabella 7.
Pagamenti derivanti dall'attività sanzionatoria

Comunicazioni di notizia di reato all'Autorità giudiziaria	
Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter*, c.p.)	6
Falsità (artt. 476 e 482, c.p. e 168, d.lgs. n. 196/2003)	2
False comunicazioni al Garante (168, d.lgs. n. 196/2003)	1
Violazioni in materia di controlli a distanza dei lavoratori (art. 171, d.lgs. n. 196/2003)	7
Totale	**16**

Tabella 8.
Comunicazioni di notizia di reato all'Autorità giudiziaria

Tabella 9.
Violazioni di dati personali notificate (per tipologia di titolare del trattamento)

Violazioni di dati personali notificate per tipologia del titolare	
Soggetti pubblici	498
Soggetti privati	1.706
Totale	**2.204**

Tabella 10.
Notifiche di violazioni di dati personali ricevute (per tipologia di notifica)

*relative anche a violazioni notificate negli anni precedenti

Notifiche di violazioni di dati personali ricevute per tipologia di notifica	
Completa	736
Preliminare	1.468
Integrativa*	2.257
Totale	**4.461**

Grafico 11.
Notifiche di violazioni di dati ricevute (per natura della violazione)

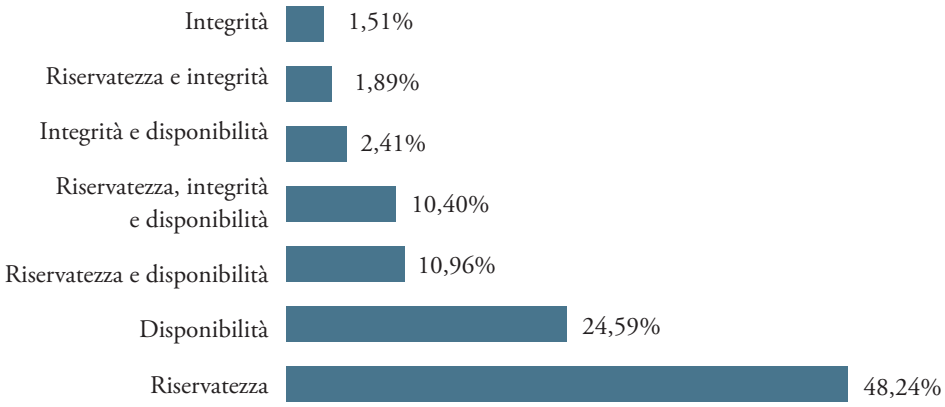

Tabella 12.
Reclami

Reclami			
	Pervenuti nell'anno	Riscontri resi nell'anno (*)	Riscontri resi nell'anno con provvedimento collegiale**
Attività ispettive	1	3	0
Affari di giustizia e di sicurezza	120	71	0
Affari legali e di giustizia	4	26	4
Libertà di manifestazione del pensiero e cyberbullismo	334	462	40
Realtà economiche e produttive	1.383	1.226	64
Realtà pubbliche	459	489	58
Reti telematiche e *marketing*	1.548	1.220	30
Sanità e ricerca	107	110	18
Tecnologie digitali e sicurezza informatica	35	45	0
Altre UU.OO.	39	224	0
Totale	**4.030**	**3.876**	**214**

(*) inerenti anche ad affari pervenuti anteriormente al 2024 e conclusi ai sensi dell'art. 11, reg. Garante 1/2019

(**) inerenti anche ad affari pervenuti anteriormente al 2024

Segnalazioni			
	Pervenuti nell'anno	Riscontri resi nell'anno (*)	Riscontri resi nell'anno con provvedimento collegiale**
Attività ispettive	2	24	0
Affari di giustizia e di sicurezza	106	89	1
Affari legali e di giustizia	5	45	1
Libertà di manifestazione del pensiero e cyberbullismo	1.161	1.483***	6
Realtà economiche e produttive	2.015	1.925	19
Realtà pubbliche	853	1.279	21
Reti telematiche e *marketing*	90.504	88.538****	29
Sanità e ricerca	220	281	5
Tecnologie digitali e sicurezza informatica	12	12	0
Altre UU.OO.	70	119	0
Totale	**94.948**	**93.795**	**82**

Tabella 13.
Segnalazioni

(*) inerenti anche ad affari pervenuti anteriormente al 2024 e conclusi ai sensi dell'art. 19, reg. Garante 1/2019

(**) inerenti anche ad affari pervenuti anteriormente al 2024

(***) di cui 625 in materia *revenge porn*

(****) di cui 87.229 *telemarketing* automatizzato

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
Affari di giustizia e sicurezza	16	22
Affari legali e giustizia	1	9
Intelligenza artificiale	1	0
Libertà di manifestazione del pensiero e cyberbullismo	5	17
Realtà economiche e produttive	115	86
Realtà pubbliche	110	201
Reti telematiche e *marketing*	28	14
Sanità e ricerca	43	50
Tecnologie digitali e sicurezza informatica	1	0
Altre UU.OO.	66	102
Totale	**386**	**501**

Tabella 14.
Quesiti

(*) inerenti anche ad affari pervenuti anteriormente al 2024

Servizio relazioni con il pubblico	
E-mail esaminate	10.682
Contatti telefonici	5.200
Persone in visita al SRP	30
Trattazione pratiche relative a fascicoli	133
Totale	**16.045**

Tabella 15.
Servizio relazioni con il pubblico

Grafico 16.
Oggetto delle *e-mail* esaminate dal Servizio relazioni con il pubblico

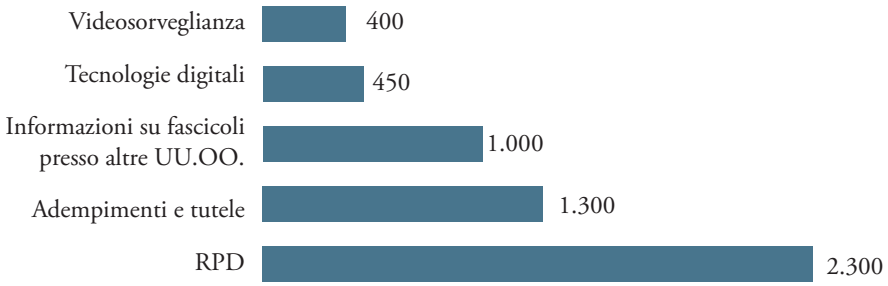

Tabella 17.
Reclami transfrontalieri e procedure di cooperazione ("sportello unico" – *ex* art. 60 del RGPD)

Reclami transfrontalieri e procedure di cooperazione ("sportello unico" – *ex* art. 60 del RGPD)						
	Gestite in qualità di LSA (autorità capofila) (art. 56, comma 1)			Gestite in qualità di CSA (autorità interessata)		
	Totale casi	Procedimenti avviati direttamente dal Garante	Procedimenti inoltrati al Garante da altre autorità di controllo	**Totale casi**	Casi nei quali il reclamo è stato presentato al Garante	Casi riconosciuti come di impatto locale *ex* art. 56, par. 2, RGPD
Numero di reclami transfrontalieri	**13**	7	6	**691**	8	2

Tabella 18.
Assistenza reciproca e operazioni congiunte

Assistenza reciproca e operazioni congiunte			
	Richieste inviate	Richieste ricevute	Partecipazione a
Numero di richieste di assistenza reciproca volontaria (VMN)	52	260	1
Numero di richieste formali di assistenza reciproca *ex* art. 61	6	22	4
Numero di operazioni congiunte *ex* art. 62	0	0	0

Tabella 19.
Pareri richiesti al CEPD (*ex* art. 64, par. 2, RGPD)

Pareri richiesti al CEPD (*ex* art. 64, par. 2, RGPD)	
Numero di richieste di parere formulate dal Garante al CEPD	0

Risoluzione di controversie fra autorità (*ex* art. 65 del RGPD)							
	Numero di casi nei quali sono state formulate RRO al Garante da altre autorità		Numero di casi nei quali il Garante ha formulato RRO ad altre autorità		Numero di casi nei quali è intervenuto il CEPD		
	Totale	Numero di casi nei quali si è raggiunta una posizione consensuale	**Totale**	Numero di casi nei quali si è raggiunta una posizione consensuale	**Totale**	Numero di procedure avviate dal Garante in qualità di LSA	Numero di procedure avviate da altre autorità in cui il Garante era CSA
Numero di casi con RRO (obiezioni pertinenti e motivate)	0	0	1	1	0	0	0

Tabella 20. Risoluzione di controversie fra autorità (*ex* art. 65 del RGPD)

Procedure d'urgenza (*ex* art. 66 del RGPD)		
In qualità di CSA (numero di procedure avviate dal Garante in quanto CSA *ex* art. 66)		0
Procedure *ex* art. 66, comma 1	0	
Procedure *ex* art. 66, comma 2	0	
Procedure *ex* art. 66, comma 3	0	

Tabella 21. Procedure d'urgenza (*ex* art. 66 del RGPD)

Attività di comunicazione dell'Autorità	
Comunicati stampa	50
Newsletter	15
Prodotti editoriali	2
Campagne informative	4
Video *spot* e *teaser* informativi	52
Infografiche e pagine tematiche	42

Tabella 22. Attività di comunicazione dell'Autorità

Tabella 23.
Personale in servizio

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	19	1	2	18
Funzionari	116	7	2	121
Operativi	45	1	0	46
Esecutivi	2	0	0	2
Totale	**182**	**10**	**4**	**188**
Personale a contratto (art. 156, commi 4 e 5 del Codice)				14

(*) Situazione alla data del 31/12/2024

Tabella 24.
Aumento del personale di ruolo

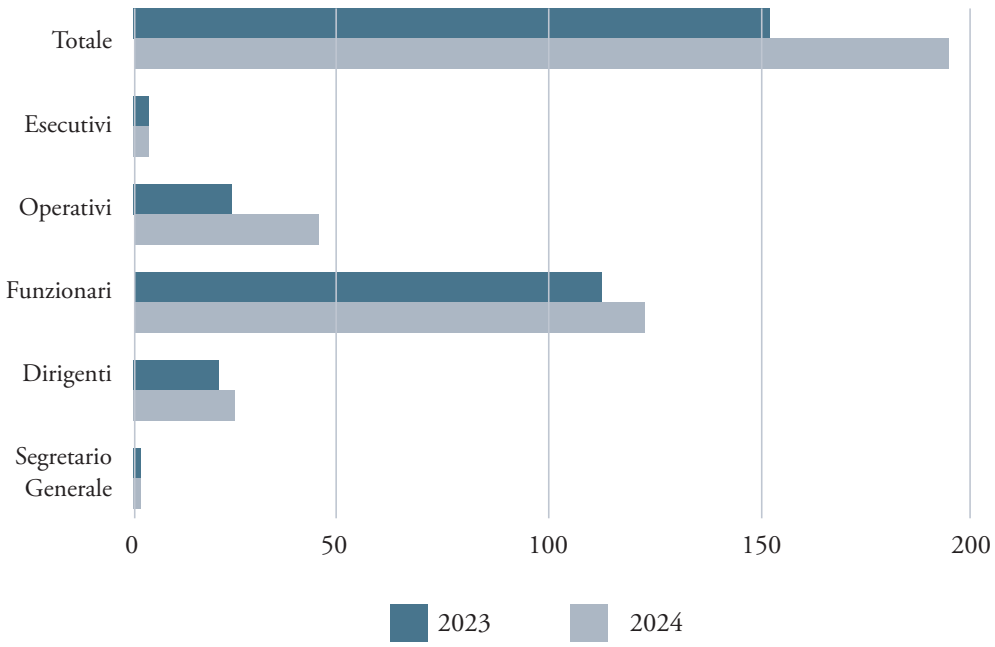

Tabella 25.
Gestione finanziaria

Gestione finanziaria				
Entrate accertate	**Anno 2024**	**Anno 2023**	**Variazione**	
			€	**%**
Entrate correnti	50.301.252	47.367.934	2.933.318	6,19
Altre entrate, trasferimenti e rimborsi	143.519	23.347	120.172	514,72
Totale entrate euro	**50.444.771**	**47.391.281**	**3.053.490**	**6,44**
Spese impegnate				
Spese di funzionamento	40.579.190	37.630.314	2.948.876	7,84
Spese in c/capitale	129.464	210.566	-81.102	-38,52
Trasferimenti ad amministrazioni	337.175	362.908	-25.733	-7,09
Totale spese euro	**41.045.829**	**38.203.788**	**2.842.042**	**7,44**