GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione Annuale 2025

Il Collegio del Garante

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

Luigi Montuori, Segretario generale

GPDP
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione annuale 2025

I numeri del Garante 2025

Servizio relazioni con il pubblico

contatti **13.577**

- e-mail **8.432**
- telefonici **4.935**

Notifiche *data breach*

2.415 (di cui 1.901 da soggetti privati)

- violazione riservatezza **70,72%**
- violazione disponibilità **9,98%**

Quesiti **270**

- realtà pubbliche
  - **71** pervenuti
  - **241** trattati
- realtà economiche e produttive
  - **14** pervenuti
  - **49** trattati

I numeri del Garante 2025

Reclami

6.604

reti telematiche e marketing
32,31%

attività economiche e lavoro
26,09%

RISCONTRI A RECLAMI NEL 2025 → **4.288**

Segnalazioni

115.275 (di cui relative al telemarketing automatizzato) **104.433**

RISCONTRI A SEGNALAZIONI NEL 2025 → **145.846**

(di cui relative al telemarketing automatizzato) **138.895**

I numeri del Garante 2025

Provvedimenti del Collegio

807

SU RECLAMO → **253**

SU SEGNALAZIONE /D'UFFICIO → **95**

DATA BREACH → **12**

RATIFICHE *REVENGE PORN* → **267**

Pareri resi dall'Autorità **65**

I numeri del Garante 2025

Misure correttive **506**

Sanzioni pecuniarie → **229**

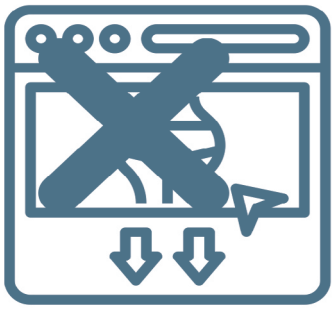
Ammonimenti → **91**

Sanzioni pecuniare pagate

€ 36.760.961

Attività ispettive *in loco*

130



Revenge porn

determinazioni dirigenziali ratificate **514**

I numeri del Garante 2025

Attività internazionale

riunioni **260**

- CEPD → 195
- CoE → 10
- OCSE → 10

Comunicazione esterna

prodotti **183**

- Video spot/*teaser* → 55
- Comunicati stampa → 59

follower social **110.867**

Indice

Indice

Indice

Indice

Indice

Indice

Elenco delle abbreviazioni e degli acronimi più ricorrenti

ANPR	Anagrafe nazionale della popolazione residente
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
ACN	Agenzia per la cybersicurezza nazionale
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
C.d.S.	Consiglio di Stato
CEDU	Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali
CEPD o Comitato	Comitato europeo per la protezione dei dati
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
LSA	*Lead Supervisory Authority*
MEF	Ministero dell'economia e delle finanze
n.	numero
p.	pagina
p.a.	pubblica amministrazione/pubbliche amministrazioni
par.	paragrafo
PDND	Piattaforma digitale nazionale dati per l'interoperabilità
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
SPE	*Support Pool of Experts*
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
VPN	*Virtual Private Network*

GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione annuale
2025

1 Introduzione

1. Attraversare la complessità. Questo potrebbe essere, in estrema sintesi, il tratto caratterizzante l'attività del Garante nel corso del 2025, un anno che ha mostrato quanto pervasivo, rapido e radicale sia il processo di trasformazione in corso a tutti i livelli della società e del vivere sociale innescato dagli sviluppi tecnologici e dai grandi rivolgimenti politici ai quali stiamo assistendo a livello mondiale. La complessità delle interrelazioni e dei rapporti che è cresciuta costantemente negli ultimi anni ha reso infatti necessario, anche nel contesto della protezione dei dati, porre particolare attenzione agli strumenti esistenti (a partire dal RGPD) e alla loro maggiore o minore effettività, in modo da assicurare che lo statuto della persona continui a essere tutelato anche (e, si potrebbe dire, in prima battuta) dalle autorità che, come il Garante, hanno come missione la protezione della persona umana e della sua dignità. Non è un caso che, a quasi dieci anni dalla pubblicazione del RGPD, il Comitato europeo per la protezione dei dati (CEPD) abbia voluto dedicare un momento specifico (durante l'incontro di Helsinki, cfr. cap. 20) alla delineazione di una strategia di maggiore semplificazione e armonizzazione delle regole sulla protezione dei dati e della loro applicazione. Questa linea di tendenza è individuabile sia nelle attività dello stesso CEPD, sia a livello normativo, con le proposte della Commissione europea che hanno riguardato la disciplina della protezione dei dati e le normative in materia di e-

1 Introduction

1. Working your way through complexity. This metaphor may best capture the essence of the Garante's work as we reflect on 2025 – a year that was marked by an incredibly fast, radical and pervasive transformation across all levels of society and community life, driven by technological advancements and the major political upheavals we have watched unfold on the global stage. The ever-increasing complexity of interrelationships and connections in recent years has led to a need, including in the context of data protection, to put extra focus on existing tools (such as the GDPR) and their varying degrees of effectiveness, so that individuals' rights carry on being safeguarded also – if not primarily – by those authorities whose mission is to protect human beings and their dignity, as is the case with the Garante. It is no coincidence that almost ten years after the adoption of the GDPR, the European Data Protection Board (EDPB) decided to hold a specific session (during the Helsinki meeting, see Chapter 20) to outline a strategy for greater simplification and harmonisation of data protection rules and their enforcement. This trend is evident both in the activities of the EDPB itself and at the regulatory level, with the European Commission's proposals concerning data protection regulations and legislation on e-privacy and AI. Artificial intelligence is undoubtedly one of the major factors contributing to this growing complexity. The Report includes several

Privacy e di IA. L'intelligenza artificiale, a tale proposito, rappresenta una delle componenti primarie (e non potrebbe essere altrimenti) di questa complessità crescente. Nella Relazione si troveranno decine di riferimenti ad attività scaturite dalla o mirate alla definizione dei rapporti fra una tecnologia che ormai è parte del nostro quotidiano, ma che non ha ancora espresso tutte le proprie potenzialità, e il mondo della protezione dei dati. Che non può rimanere arroccato nella turris eburnea della normativa, sia essa rappresentata dal RGPD o dalle norme nazionali che, in termini differenziati, riconoscono un diritto specifico di protezione delle informazioni personali, anche nel settore delle attività giudiziarie e di polizia (cfr. cap. 8). Come si è detto, il mondo della protezione dei dati ha scelto ancora una volta, e il Garante lo ha fatto in modo deciso nel 2025, di scendere nell'agone e accettare il confronto a tutto campo. La complessità non è però solo tecnologica, ma è fatta anche dello stratificarsi e addensarsi di cattive prassi che, 30 anni dopo l'adozione della l. n. 675/96, di recepimento nel nostro paese della direttiva 1995/46/CE, il primo strumento comunitario dedicato alla protezione dei dati personali, della quale il RGPD è figlio ed erede, continuano a sussistere e hanno acquisito, in realtà, maggiore pregnanza grazie all'utilizzo di sempre più sofisticati strumenti tecnologici (fra i quali, ancora una volta, i sistemi di IA). Per questo, noterà il lettore, il Garante in centinaia di occasioni, rispondendo a reclami, segnalazioni, quesiti, oppure istruendo d'ufficio procedimenti e accertamenti, ha finito con il ribadire, ricordare, riaffermare principi e indirizzi ampiamente consolidati ma, evidentemente, non abbastanza introiettati da titolari e responsabili di trattamento.

2. Che non si tratti di fenomeno solo nazionale è dimostrato dal focus che il CEPD ha voluto dedicare, come accennato, alla riflessione su semplificazione e applicazione coerente del RGPD, ma anche al tema delle intersezioni tra diverse regolamentazioni in ambito digitale (regolamento sull'IA,

references to activities arising from or aimed at defining the relationship between this technology – which already plays a role in our daily lives but has not yet reached its full potential – and the world of data protection. The latter can no longer sit in the ivory tower of legislation, be it the GDPR or national regulations, which – in their own terms – grant a specific right to the protection of personal data, including in the judicial and police sectors (see Chapter 8). As previously mentioned, the world of data protection has once again decided to take the field and face the challenge on all fronts, just as the Garante did with great determination in 2025. However, it is not only technological complexity that makes this a difficult task; it is also the consolidation of multiple layers of bad practices that persist and have actually become more widespread as a result of increasingly sophisticated technological tools (among which, once again, AI systems) - 30 years after the adoption of Law 675/96 transposing Directive 1995/46/EC into Italian law, which was the first EU instrument dedicated to the protection of personal data from which the GDPR originated. As the reader will note, in countless instances when addressing complaints, reports and inquiries, or when initiating *ex officio* proceedings and investigations, the Garante has consistently reiterated, emphasised and upheld principles and guidelines that despite being well-established, have yet to be adequately digested by data controllers and data processors.

2. The fact that this is not merely a national phenomenon is demonstrated by the emphasis that the EDPB has placed, as mentioned above, on simplification and consistent application of the GDPR, but also on the issue of intersections between different regulations in the digital sphere (the AI Regulation, DMA, DSA, Data Act, Data Governance Act, etc.) during the meeting of the heads of European data protection authorities held in Helsinki in July 2025. This has led to the

DMA, DSA, *Data Act*, *Data Governance Act*, ecc.) durante l'incontro dei vertici delle autorità europee di protezione dati tenutosi a Helsinki nel luglio 2025. Da questo sono scaturiti diversi prodotti e strumenti, anche operativi, che hanno messo al centro una visione di efficacia e collaborazione fra autorità anche estranee al mondo della protezione dei dati (*in primis*, le autorità competenti in materia di concorrenza). Ma il 2025 ha visto un'intensa attività propositiva anche da parte della Commissione europea, la quale ha dapprima presentato una proposta di regolamento, pubblicata il 21 maggio, per emendare alcuni atti legislativi, incluso il RGPD, introducendo misure cosiddette di semplificazione e di attenuazione anche di alcuni obblighi per le piccole e medie imprese (come la tenuta del registro di trattamento prevista dall'art. 30 del RGPD), e successivamente una più ampia proposta di "Digital Omnibus" comprendente modifiche al RGPD, alla direttiva e-Privacy e al complesso di leggi sui dati del pacchetto digitale (DMA, DSA, DGA), con più incisive modifiche anche alla disciplina sulla protezione dei dati. A tutto questo si è accompagnata una proposta di regolamento che punta alla semplificazione dell'attuazione delle norme armonizzate sull'intelligenza artificiale, introducendo alcuni emendamenti al reg. IA che attengono alla protezione dei dati. Sempre nell'ottica di rafforzare la cooperazione fra autorità, in questo caso per quanto concerne i casi transfrontalieri, è stato adottato nel mese di dicembre un regolamento recante norme procedurali aggiuntive per l'applicazione del RGPD; si tratta di un altro elemento significativo per la riorganizzazione e armonizzazione dell'attività delle autorità di protezione dei dati. L'intento lodevole di fare una sorta di "tagliando" della normativa correggendone alcune (supposte) deficienze sconta, tuttavia, un equivoco di fondo che è, a sua volta, spia della complessità di cui prima si parlava. Nel caso del reg. IA, per esempio, si è rilevato dal CEPD (nel parere appositamente reso, cfr. par. 20.1) che occorre mantenere

creation of a number of products and tools, including operational ones, which have been designed to promote a vision of effectiveness and collaboration among authorities, including those beyond the world of data protection (in particular competition authorities). However, 2025 also saw extensive legislative activity on the part of the European Commission, which first submitted a draft regulation, published on 21 May, to amend certain legislative acts (including the GDPR), with measures to simplify and ease certain obligations for SMEs (such as the requirement to maintain a record of processing activities under Article 30 of the GDPR), and subsequently a broader proposal for a 'Digital Omnibus' comprising amendments to the GDPR, the e-Privacy Directive and the body of data laws within the Digital Services Package (DMA, DSA, DGA), with further significant changes to data protection rules. This was followed by a draft regulation aimed at simplifying the implementation of harmonised rules on artificial intelligence, by introducing a set of amendments to the AI Act relating to data protection. Again with a view to strengthening cooperation among authorities, this time in cross-border cases, a regulation laying down additional procedural rules for the application of the GDPR was adopted in December; this is another significant step towards the reorganisation and harmonisation of the activities of data protection authorities. Nevertheless, the admirable intention to perform a 'sanity check' of the legislation by rectifying some of its (alleged) shortcomings is undermined by a deep-rooted misunderstanding that, in turn, reflects the complexity mentioned above. For example, as regards the AI Act, the EDPB pointed out (in its formal opinion on the matter, see section 20.1) that a balance must be struck between simplification and the protection of fundamental rights, whilst ensuring that the safeguards currently provided by the AI Act are not undermined by a failure to take due account of the

in equilibrio semplificazione e salvaguardia dei diritti fondamentali evitando di ridurre le garanzie attualmente offerte dal reg. IA in assenza di un'attenta considerazione della tutela dei diritti delle persone. Lo stesso vale per il Digital Omnibus e le proposte di semplificazione concernenti il RGPD, soprattutto per alcuni emendamenti alla nozione di dato personale, elemento chiave di tutta la disciplina, che verrebbe in qualche modo relativizzato e quindi reso incerto, legato a valutazioni e parametri soggettivi che rischiano di vanificare la certezza giuridica che le proposte intendono invece promuovere. È chiaro che, in sintesi, il processo di semplificazione amministrativa non può comportare una riduzione delle garanzie, cioè non può esimersi dal considerare con attenzione la complessità della gestione del dato personale – e, quindi, non può funzionare in assenza di altri strumenti che accompagnino e assistano i titolari nella realizzazione di una piena *accountability*: si veda, in questo senso, il lavoro svolto dal CEPD e dal Garante sulle linee guida in materia di pseudonimizzazione (linee guida 1/2025, par. 20.1) con l'acquisizione di elementi conoscitivi anche attraverso un incontro ad-hoc con numerosi stakeholder. E proprio l'*accountability*, che, come si sa, è la chiave di volta del sistema protezione dati del RGPD e della direttiva 680/2016, viene di fatto messa in discussione dalla mini-proposta iniziale di abolizione dell'obbligo di tenuta del registro dei trattamenti sopra menzionata per le PMI. Il registro dei trattamenti è lo strumento primario per la valutazione degli asset informativi di ciascun titolare e responsabile di trattamento; per questo associare, meccanicamente, alla dimensione ridotta dell'impresa una dimensione ridotta delle responsabilità significa applicare un approccio meccanicistico che non tiene conto della complessità del reale: in un paese come l'Italia ove (dati EUROSTAT) oltre il 98% delle imprese sono PMI (ossia hanno meno di 250 dipendenti, secondo lo standard europeo), una proposta di questo tipo rischierebbe di minare alla radice l'attuazione

protection of individuals' rights. The same applies to the Digital Omnibus and the simplification proposals concerning the GDPR, particularly with regard to certain amendments to the notion of personal data – a key element of the regulatory framework – which could be made more open to interpretation and thus uncertain, depending on subjective assessments and parameters that risk jeopardising the legal certainty that these proposals seek to promote. In brief, it is clear that the process of administrative simplification cannot entail a reduction in safeguards; in other words, it cannot fail to take due account of the complexity of personal data management and, therefore, cannot operate without other tools to support and assist data controllers in achieving full accountability: see, in this regard, the work carried out by the EDPB and the Garante on the guidelines on pseudonymisation (Guidelines 1/2025, Chapter 20.1), which involved gathering information, including through a dedicated meeting with various stakeholders. And it is precisely accountability – which, as we know, is the cornerstone of the data protection system under the GDPR and Directive 680/2016 – that is effectively challenged by the initial, more limited proposal to withdraw the obligation for SMEs to maintain a record of processing activities, as mentioned above. The record of processing activities is the primary tool for assessing the information assets of each data controller and data processor; this is why the idea that smaller companies have fewer accountability issues mirrors a simplistic approach that fails to take into account the intricacies of the actual situation: in a country such as Italy, where (according to Eurostat data) over 98% of businesses are SMEs (i.e. they have fewer than 250 employees, according to the European standard), a proposal such as this would risk undermining the very foundations of the implementation of the principle of accountability.

3. Returning to the topic of AI, whose

del principio di responsabilizzazione.

3. Tornando al tema IA, della cui importanza ampiamente testimoniano le attività del Garante ricordate in più sezioni della presente Relazione (cfr. in particolare cap. 16, e i rinvii ivi contenuti), il contesto normativo a livello nazionale è stato caratterizzato dall'approvazione della legge 23 settembre 2025, n. 132 "Disposizioni e deleghe al Governo in materia di intelligenza artificiale". Quest'ultima non ha attribuito al Garante o ad altro soggetto dotato di equivalente requisito di indipendenza il ruolo di autorità di vigilanza del mercato previsto dal reg. IA con riguardo, in particolare, ai sistemi di IA ad alto rischio, che sono suscettibili di incidere sui diritti fondamentali delle persone oltre che su interessi di natura generale connessi alla democraticità dell'ordinamento. Unitamente alla mancata previsione di forme di partecipazione delle autorità di tutela dei diritti fondamentali e, tra queste, del Garante, al sistema di *governance* coordinato nazionale, ciò rappresenta un'occasione (sinora) mancata per promuovere e disciplinare forme di cooperazione avanzata fra le diverse autorità in modo da gestire con piena cognizione la complessità dei sistemi in parola. Va detto che il Garante, per parte sua, ha avuto modo di confrontarsi con alcuni impegnativi esercizi che, soprattutto in ambito pubblico, stanno focalizzandosi sulla declinazione di regole e raccomandazioni utili agli operatori – si veda il caso del parere e delle indicazioni rese sulle linee guida per l'introduzione dell'intelligenza artificiale nelle istituzioni scolastiche del Ministero dell'istruzione e del merito; si tratta di un documento di particolare interesse, in quanto rappresenta uno fra i primi documenti di indirizzo da parte di un'amministrazione centrale verso le sue articolazioni periferiche, e si associa alla creazione di una piattaforma digitale per la condivisione di materiali anche didattici (cfr. par. 4.3). Stesso discorso vale per la sanità digitale, uno degli ambiti di più intenso intervento da parte dell'Autorità (cfr. cap. 5): ne sono testimonianza le decine di pareri resi al Ministero della

importance is widely reflected in the activities of the Garante referred to in a number of sections of this Report (see in particular Chapter 16 and the references contained therein), the regulatory framework at national level has been shaped by the adoption of Law No. 132 of 23 September 2025, 'Provisions and Delegations to the Government on Artificial Intelligence'. However, the latter law did not confer on the Garante or any other entity meeting equivalent independence requirements the role of market surveillance authority (MSA) provided for in the AI Act, particularly with regard to high-risk AI systems, which are likely to affect individuals' fundamental rights as well as general interests relating to the democratic nature of the legal system. In addition to not involving fundamental rights protection authorities – such as the Garante – in the coordinated national governance system, this marks a missed opportunity (so far) to promote and regulate advanced cooperation among the various authorities, so as to manage the complexity of the systems under discussion with full awareness. It is worth mentioning that the Garante, for its part, took on some challenging tasks in the public sector in particular, focusing on the rules and recommendations for those working in the field – see, for example, the opinion and guidance provided on the Ministry of Education and Merit's 'Guidelines for the introduction of artificial intelligence in schools' ; this is a document of special interest, as it is one of the first guidance documents issued by a central administration to its local branches, and is linked to the creation of a digital platform for sharing materials, including educational resources (see section 4.3). Another area where the Garante has been actively engaged is digital healthcare (see Chapter 5), as demonstrated by the dozens of opinions issued to the Ministry of Health and to the Regions, as well as by a flurry of fact-finding and procedural activities confirming that 2025 was another year that saw this sector take on great

salute e alle regioni, e molte altre attività istruttorie e procedimentali che hanno confermato trattarsi, anche nel 2025, di un settore di grande rilevanza strategica in cui il Garante ha cercato di accompagnare la transizione digitale del SSN nel rispetto dei diritti fondamentali degli interessati. Significativa l'accelerazione dei progetti previsti dal PNRR, con particolare riferimento alle infrastrutture digitali sanitarie e ai sistemi informativi centrali. Anche in questo settore, il Garante è intervenuto in profondità, per accompagnare l'evoluzione dei sistemi sanitari nella gestione sempre più articolata e complessa delle singole componenti, necessariamente interconnesse (dal Fascicolo sanitario elettronico alla telemedicina). In particolare, in continuità con l'adozione del decalogo in materia di IA (cfr. Relazione 2023, par. 5.2), l'Autorità ha proseguito le interlocuzioni con il Ministero della salute e l'AGENAS (Agenzia nazionale per i servizi sanitari regionali) relative alla realizzazione di una piattaforma informatica di IA a supporto dell'assistenza primaria; per altro verso, nel contesto di un'istruttoria concernente una procedura di gara per la conclusione di un accordo quadro per l'affidamento di servizi applicativi e di supporto in ambito «Sanità digitale - *Data Governance* e *Artificial Intelligence*» per le p.a. del SSN, ha colto l'occasione per ribadire i principi sanciti dal Consiglio di Stato (sez. VI, 13 dicembre 2019, n. 8472) e applicabili al trattamento di dati sulla salute con logiche algoritmiche basate su sistemi di IA: il principio di conoscibilità, per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e di ricevere informazioni significative sulla logica utilizzata; il principio di non esclusività della decisione algoritmica; quello di non discriminazione algoritmica. L'affidamento fideistico alla tecnologia costituisce una scorciatoia e non è ammissibile, non solo in via generale, ma neppure alla luce di quanto prevede il reg. IA: l'intervento umano (sotto forma di supervisione qualificata) è essenziale per prevenire rischi che potrebbero incidere direttamente sulla salute

strategic importance, with the Authority seeking to support the digital transition of the SSN (National Health Service) while respecting the fundamental rights of data subjects. The projects set out in the PNRR (National Recovery and Resilience Plan) have accelerated significantly, particularly with regard to digital healthcare infrastructure and central information systems. In this sector too, the Garante has taken major steps to support the evolution of healthcare systems in the increasingly intricate and complex management of its individual components, which are necessarily interconnected (from electronic health records to telemedicine). More specifically, following on from the adoption of the ten-point code of conduct on AI (see 2023 Report, para.5.2), the Authority has continued its discussions with the Ministry of Health and AGENAS (the National Agency for Regional Health Services) on the development of an AI-based IT platform to support primary care; furthermore, as part of a fact-finding investigation concerning a tender procedure for the conclusion of a framework agreement for the assignment of implementing and support services in the field of 'Digital Health - Data Governance and Artificial Intelligence' for the public administrations of the SSN (National Health Service), it seized the opportunity to reiterate the principles established by the Council of State (Section VI, 13 December 2019, No. 8472) and applicable to the processing of data concerning health using AI-based algorithmic logic: the principle of 'knowability' (or transparency), whereby individuals have the right to be aware of the existence of automated decision-making processes concerning them and to receive meaningful information on the logic used; the principle of non-exclusivity of algorithmic decisions; and the principle of algorithmic non-discrimination. Blind reliance on technology alone is a shortcut and cannot be accepted, not only in general terms, but also in light of the provisions of the AI Act: human inter-

della persona (cfr. art. 14 reg. IA) e deve essere garantito in tutte le fasi del ciclo di vita del sistema di IA, come ricordato dall'Autorità anche attraverso un apposito comunicato stampa.

4. Come non menzionare, sempre in rapporto al mondo IA, le molte interlocuzioni a livello sovranazionale e nazionale rese necessarie dall'espandersi delle applicazioni e degli utilizzi dell'IA generativa soprattutto nel settore delle comunicazioni elettroniche (cfr. cap. 12)? Il Garante non ha esitato, per esempio, ad adottare un provvedimento di limitazione definitiva dei trattamenti nei confronti delle società cinesi titolari di un noto servizio di IA generativa sia su piattaforma web che via app, con riferimento alle attività di trattamento dei dati personali di interessati che si trovano nel territorio italiano, ottenendo un parziale adempimento con rimozione dell'app del servizio dagli app store italiani; per altro verso, le società in questione hanno opposto l'impossibilità tecnica di aderire alla richiesta dell'Autorità di bloccare l'accesso al servizio fornito dall'Italia. Da questa istruttoria sono scaturite istruttorie nei confronti dei medesimi titolari anche a opera delle autorità di controllo di altri paesi UE, e la discussione sugli approcci coordinati nei confronti di titolari privi di stabilimenti nel SEE si è trasferita a livello di una task force specificamente costituita dal CEPD (*Generative AI Enforcement*, GAIE - cfr. par. 12.2). Significativo in questa ottica anche il coinvolgimento del Garante da parte dell'autorità irlandese di protezione dei dati in un intenso lavoro di cooperazione, unitamente alle altre autorità europee, con riguardo all'esame ed allo studio della documentazione fornita da un'altra nota società statunitense, stabilita in Irlanda, che offre un social network ampiamente utilizzato in Europa. Nello specifico, l'iniziativa del titolare riguardava il trattamento dei dati personali degli utenti europei maggiorenni del social network, per addestrare i propri sistemi di IA generativa a partire dal 3 novembre 2025 sulla base del legittimo interesse di cui all'art. 6, par.1, lett. f), RGPD. Vista l'individuazione

vention (in the form of qualified supervision) is essential to prevent risks that could directly affect the health of individuals (see Article 14 of the AI Act) and must be ensured at all stages of the AI system's lifecycle, as the Garante pointed out in a dedicated press release.

4. How can we fail to mention, again in relation to the field of AI, the multiple discussions at national and supranational levels made necessary by the proliferation of applications and uses of generative AI, particularly in the electronic communications sector (see Chapter 12)? In this regard, the Garante had no hesitation in adopting a measure imposing a definitive limitation on processing by Chinese companies operating a well-known generative AI service, both via a web platform and an app, in relation to the processing of personal data of data subjects located in Italy, which was partially complied with through the removal of the service's app from Italian app stores; on a different note, the companies in question claimed that it was technically impossible for them to comply with the Garante's request to block access to the service as provided from Italy. This led to further fact-finding activities against the same controllers by supervisory authorities in other EU countries, and the discussion on coordinated approaches towards controllers without establishments in the EEA was handed over to a task force specifically set up by the EDPB (*Generative AI Enforcement*, GAIE – see paragraph 12.2). Also noteworthy in this regard is the involvement of the Garante by the Irish Data Protection Commission (DPC) in intensive cooperation, alongside other European authorities, to examine and study the documentation provided by another well-known US company, established in Ireland, which operates a social network that is widely used in Europe. Specifically, the controller's initiative was to process the personal data of adult European users of the social network in order to train its own generative AI systems from 3 November 2025 onwards,

di tale base giuridica del trattamento, e in considerazione del conseguente obbligo del titolare di garantire agli utenti un efficace esercizio del diritto di opposizione, l'Autorità ha valutato il corretto funzionamento del sistema di *opt-out* predisposto dal titolare per gli utenti, nonché il modulo di *opt-out* predisposto per utenti e non utenti, secondo un approccio chiaramente orientato alla verifica e validazione in chiave giuridica e di efficacia delle soluzioni tecnologiche concretamente prospettate dal titolare. È stata quindi pubblicata, a ulteriore integrazione, una scheda informativa sul sito web del Garante volta ad informare gli utenti relativamente al trattamento dei loro dati per finalità di addestramento di IA generativa da parte del titolare in questione.

5. Tornando alla metafora dell'attraversare la complessità, bisogna ricordare in questa sede la consultazione pubblica volta a valutare la liceità del consenso per trattamenti di profilazione da parte di diversi titolari, *in primis* dagli editori di giornali, attraverso l'adozione del cosiddetto modello *pay or ok* (anche denominato *pay or consent* o *consent paywall*). Tale modello impone agli utenti, per accedere ai contenuti, ai servizi o alle funzionalità offerte online, di scegliere se sottoscrivere un abbonamento a pagamento oppure acconsentire al trattamento dei propri dati personali, attraverso cookie e strumenti di tracciamento, ai fini di profilazione commerciale. In mancanza di una delle due opzioni, l'accesso ai siti è bloccato. La natura controversa di questa modalità di business, quanto alla dubbia possibilità di considerare libero il consenso eventualmente prestato dall'utente (se ne parla nel parere 8/2024 del CEPD sul consenso valido nel contesto dei modelli consenso o pagamento attuati dalle piattaforme online di grandi dimensioni – cfr. Relazione 2024) è stata analizzata attraverso un approccio non meramente sanzionatorio da parte dell'Autorità, che pure sarebbe stato possibile, ma certo anche miope, al fine di non compromettere l'attuale modello di mercato degli editori e degli altri titolari coinvolti senza offrire una valida alternativa in grado

on the basis of the legitimate interest referred to in Article 6(1)(f) of the GDPR. With this legal basis for processing being identified, and in view of the data controller's consequent obligation to ensure that users can effectively exercise their right to object, the Authority assessed the proper functioning of the opt-out system set up by the data controller for users, as well as the opt-out form provided for both users and non-users, by adopting an approach clearly focused on verifying and validating – from a legal perspective and in terms of effectiveness – the technological solutions put forward by the data controller. This was supplemented by the publication of an information sheet on the Garante's website, designed to inform users about the processing of their data for the purposes of training generative AI by the data controller in question.

5. Echoing the metaphor of working one's way through complexity, it is worth recalling the public consultation aimed at assessing the lawfulness of consent for profiling by a variety of controllers, primarily newspaper publishers, through the adoption of the so-called 'pay or ok' model (also known as 'pay or consent' or 'consent paywall'). This model requires users who wish to access content, services or features available online to either subscribe to a paid service or consent to the processing of their personal data, via cookies and tracking tools, for the purposes of commercial profiling. If neither option is selected, website access is not enabled. The contentious nature of this business model, due to the questionable legitimacy of considering user consent provided in this context to be freely given (as discussed in EDPB Opinion 8/2024 on valid consent in the context of 'consent-or-pay' models implemented by large online platforms – see Report 2024) has been analysed by the Authority. The approach taken was not merely to impose sanctions – which could have been done, but would certainly have been narrow-minded – so as not to jeopardise the current market model of

di bilanciare adeguatamente le diverse componenti secondo un'ottica olistica: le esigenze economiche dei settori interessati, la libera circolazione dell'informazione e il diritto fondamentale alla protezione dei dati personali. Sono così stati raccolti, attraverso una consultazione pubblica, contributi utili a individuare soluzioni tecniche e operative – come modelli alternativi di accesso ai contenuti – in grado di garantire agli utenti il rispetto dei principi di libertà, specificità e consapevolezza del consenso. È interessante notare come la maggior parte dei contributi ricevuti contenesse una posizione critica, evidenziando come tale modello si fondi sullo squilibrio di potere tra piattaforme e utenti in assenza di una reale terza opzione, in contrasto con i principi del RGPD e con i diritti e le libertà fondamentali degli interessati.

6. Lo stratificarsi di cattive prassi, potenziate dal ricorso ai nuovi ausili tecnologici compresi i sistemi di IA, rappresenta l'altro elemento che spiega la complessità crescente dello scenario in cui si muove l'Autorità. In questo senso, l'attenzione posta dalle attività ispettive del Garante (supportate ormai da anni proficuamente dal Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza) su alcuni temi specifici getta una luce significativa sulla persistenza di approcci patologici da parte di titolari pubblici e privati, in un contesto sempre più articolato. Violazioni di dati personali, trattamento di dati dei lavoratori (incluso il ricorso alla videosorveglianza) e telemarketing sono stati gli ambiti primari delle attività ispettive nel 2025, e non si tratta certo di una novità (cfr. par. 18.2). Al contempo, ciò segnala la necessità di mantenere la presa e l'attenzione su condotte che, come nel caso delle violazioni di dati personali, hanno assunto una dimensione assai più raffinata tanto da necessitare la costituzione di una specifica task force interna che opera ormai da più di un anno, con ispezioni *in loco*, per svolgere gli accertamenti sul fenomeno dell'illecita acquisizione di informazioni provenienti dalle grandi banche di dati pubbliche (anagrafe

publishers and other data controllers involved without offering a viable alternative solution to adequately balance the various factors from a comprehensive perspective: the economic needs of the sectors involved, the free flow of information, and the fundamental right to the protection of personal data. A public consultation was held to gather input useful for identifying technical and operational solutions – such as alternative models for accessing content – capable of ensuring that user consent is freely given, specific and informed. It is striking that most of the input expressed concerns that this model is based on a power imbalance between platforms and users, with no genuine third option available, which runs counter to the principles of the GDPR and the fundamental rights and freedoms of data subjects.

6. The proliferation and consolidation of bad practices, exacerbated by the use of new technological tools including AI systems, are key factors explaining the growing complexity of the environment in which the Garante conducts its work. In this regard, the focus of the Garante's inspection activities (which have been effectively supported for years by the Special Unit for Privacy Protection and Technological Fraud of the Guardia di Finanza) on certain specific issues casts significant light on how public and private data controllers continue to adopt inadequate approaches in an increasingly complex environment. Personal data breaches, processing of workers' data (including the use of video surveillance), and telemarketing were the primary areas targeted by inspections in 2025, but this is certainly nothing new (see para. 18.2). At the same time, this highlights how important it is to keep a close eye on practices that, as in the case of personal data breaches, have become so sophisticated that they made it necessary to set up a special internal task force – which has now been operating for over a year, conducting on-site inspections – to investigate the unlawful acquisition of information from large

tributaria, banche dati dell'INPS, delle forze di polizia) (cfr. par. 4.9.1). Questa attività ha consentito di acquisire una mole consistente di informazioni e documenti e di individuare carenze dal punto di vista delle misure di sicurezza e, appunto, prassi non adeguate da parte degli operatori. Attraverso complesse attività istruttorie e impegnativi accertamenti ispettivi, l'Autorità ha esaminato le principali applicazioni in uso e i sistemi di cooperazione applicativa, con particolare riguardo alle procedure di gestione delle utenze e delle abilitazioni, ai sistemi di autenticazione informatica e di tracciamento delle operazioni eseguite, alle procedure di controllo per verificare la liceità delle operazioni eseguite, nonché alla gestione delle violazioni dei dati personali, anche con riferimento a quelle determinate da accessi abusivi.

7. Non diversa la situazione riferita all'impiego scorretto di tecniche di videosorveglianza nel trattamento dei dati di lavoratori, sempre più spesso associate a dispositivi informatici capaci di "seguire" o "monitorare" il lavoratore nelle varie fasi della sua prestazione lavorativa o a strumenti per raccogliere ed incrociare informazioni sulle opinioni, lo stato di salute o i rapporti interpersonali dei dipendenti. Si tratta di un ambito di intervento di grande delicatezza, tradizionalmente fra i principali fulcri dell'attività del Garante, e che si sta da poco confrontando anche con le sfide degli strumenti che utilizzano le potenzialità dell'intelligenza artificiale. Si può parlare, dall'osservatorio dell'Autorità, di una vera e propria recrudescenza di un fenomeno che interessa in particolare gli esercizi commerciali di piccole dimensioni, ove vengono utilizzati sistemi di ripresa in grado di monitorare costantemente tutti gli spazi interni da remoto mediante app installate sui telefoni cellulari del titolare – con ciò realizzando un sistema preordinato al controllo a distanza dell'attività del lavoratore in violazione dell'art. 4 della l. n. 300/1970 e tale da incidere sulla libertà e sulla dignità delle persone (cfr. par. 15.2).

8. Molteplici provvedimenti adottati dal-

public databases (tax registry, national social security institution databases, police databases) (see para. 4.9.1). This activity provided a substantial amount of information and documents as well as revealed gaps in security measures and, as mentioned, inadequate practices on the part of practitioners. Through complex fact-finding activities and rigorous inspections, the Authority examined the main applications in use and the application cooperation systems, with particular regard to user and authorisation management procedures, IT authentication and operation tracking systems, control procedures to verify the lawfulness of operations performed, as well as the management of personal data breaches, including those resulting from unauthorised access.

7. Nor is the situation any different when it comes to the improper use of video surveillance techniques in the processing of employee data, which is increasingly associated with IT devices capable of 'tracking' or 'monitoring' employees throughout their workday, or with tools designed to collect and cross-check information on employees' opinions, health status, or personal relationships. This is a highly sensitive area of intervention that has long been one of the core activities of the Garante and is currently undergoing a transformation driven by the emergence of new tools leveraging the potential of artificial intelligence. From the perspective of the Garante, this can be described as the upsurge of a phenomenon that mainly concerns small-scale retail businesses, where CCTV systems are used to constantly monitor all internal areas remotely via apps installed on the controller's mobile phones – thereby creating a system designed for the remote monitoring of the worker's activities, in infringement of Section 4 of Law No. 300/1970, which has an impact on the freedom and dignity of individuals (see paragraph 15.2).

8. Furthermore, several decisions adopted by the Garante addressed data processing in the public and private workplace, in-

l'Autorità hanno riguardato, del resto, il trattamento dei dati nel contesto lavorativo pubblico e privato, anche relativamente alla fase successiva alla cessazione del rapporto di lavoro, in particolare caratterizzati dall'aumentato utilizzo di strumenti tecnologici con una crescente pervasività del controllo del datore di lavoro sull'attività del lavoratore, e conseguentemente un'accresciuta esigenza di garantire l'effettività della tutela del diritto alla protezione dei dati personali individuando soluzioni equilibrate e rispettose del quadro normativo complessivo. È in molti di questi casi (cfr. par. 13.1, e par. 13.3) che il Garante, dinanzi all'impiego disinvolto di sistemi di geolocalizzazione del lavoratore o per la valutazione della guida di conducenti di mezzi di trasporto affidati a lavoratori, o alla luce delle attività di profilazione condotte su social network anche precedentemente e successivamente all'instaurazione del rapporto di lavoro, è tornato a ribadire e riaffermare concetti e princìpi che dovrebbero essere patrimonio comune anche al di là dell'area della protezione dei dati (lo Statuto dei lavoratori, nelle sue varie declinazioni, risale al 1970). Il Garante ha così dovuto ribadire, ricordare o riaffermare che i dati personali pubblicati sui social network o, più in generale, disponibili in rete, non possono essere utilizzati a ogni fine, solo perché accessibili a un numero più o meno esteso di persone, essendo messi a disposizione dagli interessati per finalità di comunicazione interpersonale o di libera manifestazione del pensiero; che l'esigenza di ridurre il rischio di usi impropri della navigazione in Internet, da parte dei dipendenti, non giustifica ogni forma di interferenza nella vita privata, richiedendo invece la predisposizione di misure tecniche e organizzative idonee a prevenire *ab ovo* che le eventuali informazioni relative alla sfera extralavorativa vengano raccolte dal datore di lavoro; che la corrispondenza e "ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione "in presenza"

cluding after the termination of the employment relationship. Such decisions involved, in particular, the increased use of technological tools with a growing pervasiveness of the employer's control over the employee's activities, and consequently a greater need to ensure the effective protection of the personal data protection right through the identification of balanced solutions that respect the overarching regulatory framework. It is in many of these instances (see paragraphs 13.1 and 13.3) that the Garante, in consideration of the careless use of systems for geolocating workers or for assessing the performance of transport drivers employed by the organisation, or in light of profiling activities carried out on social networks both before and after the establishment of the employment relationship, has reiterated and reaffirmed concepts and principles that should be commonly shared even beyond the realm of data protection (the 'Workers' Statute', in its various versions, dates back to 1970). Likewise, the Garante was called upon to reiterate, remind or reaffirm that personal data published on social networks or, broadly speaking, available online, cannot be used for any purpose simply because they are accessible to a more or less extensive number of people, such data being made available by the data subjects for the purposes of personal communication or the free expression of thought; that the need to reduce the risk of improper use of the Internet by employees does not justify any form of interference in private life, but rather requires the implementation of appropriate technical and organisational measures to prevent, from the outset, any non-work-related information from being collected by the employer; that correspondence and 'any communication of human thought (ideas, intentions, feelings, data, news) between two or more specific individuals, taking place in a manner other than a conversation "in person", also encompasses, given the current state of available technology, the exchange of elec-

1

ricomprende, allo stato delle tecnologie disponibili, anche lo scambio di messaggi elettronici fra dipendenti quali e-mail, WhatsApp, SMS "e simili" (secondo quanto statuito dalla Corte costituzionale nella sentenza n. 170/2023); che attività di monitoraggio del lavoratore a distanza non sono necessariamente vietate ma devono essere previamente autorizzate dall'Ispettorato del lavoro territorialmente competente, ai sensi dell'art. 4, l. n. 300/1970, e prevedere l'adozione di soluzioni tecnologiche tali da impedire il trattamento di dati ulteriori e non pertinenti rispetto alle finalità organizzative e produttive. Non vi sono, insomma, scorciatoie facili in questo e in tutti gli altri ambiti che investono la protezione delle persone e occorre passare dalla ricerca di soluzioni ponderate e attente.

9. Sempre in tema di videosorveglianza, e della necessità di confrontarsi con un fenomeno certamente non nuovo (le linee guida in materia di videosorveglianza del Garante risalgono al 2010), ma che ha assunto negli ultimi anni dimensioni preoccupanti, si deve ricordare l'ampia gamma di problematiche legate all'utilizzo di sistemi di videosorveglianza tra privati. Le ragioni dell'incremento registrato dall'Autorità nel numero di segnalazioni relative a questa tipologia di trattamenti sono molteplici e chiamano in causa, ancora una volta, fattori di ordine infrastrutturale e anche sociologico: si sono ridotti i costi di acquisto degli apparati di ripresa, che hanno acquisito al contempo nuove funzionalità e spesso consentono di accedere alle immagini da remoto; dall'altro lato, il ricorso alla videosorveglianza è la spia di un malessere sociale e dei rapporti interpersonali, tanto che spesso la questione videosorveglianza risulta essere solo la parte emergente di un mondo di conflitti e litigiosità in tutte le dimensioni del vivere sociale. Rispetto a queste problematiche, la risposta non può collocarsi nella sola dimensione dell'*enforcement*; piuttosto, il Garante ha scelto un approccio graduato, muovendo dall'ampia gamma di compiti assegnati alle autorità di controllo dall'art. 57 del RGPD, e quindi ricercando

tronic messages between employees such as emails, WhatsApp, SMS and the like' (in accordance with the ruling of the Constitutional Court in judgment No. 170/2023); that remote monitoring of employees is not strictly prohibited but must be authorised in advance by the competent local Labour Inspectorate, pursuant to Article 4 of Law No. 300/1970, and must provide for the adoption of technological solutions designed to prevent the processing of additional data that is not relevant to organisational and productive purposes. In short, there are no easy shortcuts in this or any other area concerning the protection of individuals; we must instead seek well-considered and carefully thought-out solutions.

9. Staying on the topic of video surveillance and the need to address a phenomenon that is by no means new (the guidelines on video surveillance issued by the Garante date back to 2010), but which has reached alarming proportions in recent years, we should bear in mind the wide range of issues associated with the use of video surveillance systems by private individuals. The reasons underlying the increase observed by the Authority in the number of reports concerning this type of processing are manifold and, once again, bring into play both infrastructural and sociological factors: the purchase costs of recording equipment have dropped, while new features have been added and remote access to images is now possible in many cases; the use of video surveillance may be a symptom of social unease and strained interpersonal relationships, to the extent that such phenomenon often appears to be merely the tip of the iceberg in a world of conflict and strife across all aspects of social life. These issues cannot be addressed merely through enforcement, which is why the Garante has adopted a multi-tiered approach, building on the wide range of tasks assigned to supervisory authorities under Article 57 of the GDPR, and thus seeking to delve deeper into the issues underlying the reports and gathering

un approfondimento delle questioni alla base delle segnalazioni e acquisendo informazioni utili alla valutazione della singola fattispecie (non essendo ipotizzabile condurre accertamenti in loco in tutti i casi), e procedendo poi, ove necessario, all'esercizio di poteri sanzionatori (cfr. par. 15.3).

10. Questo stesso approccio graduato, articolato, non meccanicistico né acritico, ha contraddistinto la gestione di un'altra delle tematiche da sempre ricorrenti nel lavoro del Garante, ossia il telemarketing e il marketing aggressivo in generale (cfr. par. 11.1). Anche in questo ambito, costante è stato l'incremento del numero di segnalazioni e reclami ricevuti, e il Garante ha scelto di operare lungo tre diverse direttrici: la cooperazione con le altre autorità di regolazione (in particolare AGCOM), le associazioni di consumatori e l'Organismo di monitoraggio del codice di condotta per le attività di telemarketing e *teleselling*; un impegno costante nel fornire, fin dalle fasi istruttorie, riscontri, chiarimenti e indicazioni operative alle numerosissime segnalazioni e lamentele presentate dagli interessati (nell'ordine delle migliaia); un approfondimento istruttorio a partire dall'esame delle segnalazioni e dei reclami anche mediante iniziative ispettive, che hanno condotto all'adozione di provvedimenti correttivi e sanzionatori, talora con importanti risvolti interpretativi. È il caso qui di sottolineare che, nella quasi totalità delle istruttorie, l'attività condotta ha evidenziato, come per gli anni precedenti, la carente assimilazione degli obblighi di *accountability* gravanti sul titolare del trattamento. E quindi, di nuovo, il Garante si è trovato a dover ribadire principi e indicazioni che si immaginerebbero consolidati: la necessità di un adeguato controllo lungo l'intera filiera del trattamento; di predisporre idonee misure tecniche e organizzative; di utilizzare liste di contatto acquisite da soggetti terzi rispettose dei presupposti normativi, con particolare riferimento alla correttezza dell'informativa resa agli interessati e alla validità dei consensi da questi prestati. Tuttavia, accanto alle metodologie tradizionali caratterizzanti il telemarketing sel-

information useful for the case-by-case assessment (as conducting on-site inspections for every case is not feasible), and then proceeding, where necessary, to exercise its powers to impose sanctions (see para. 15.3).

10. This same multi-tiered, structured approach – far from being mechanistic or uncritical – has also been applied to another recurring issue in the Garante's work: telemarketing and aggressive marketing in general (see section 11.1). The number of reports and complaints received has increased steadily in this area too, and the Garante has pursued three distinct lines of action: cooperation with other regulatory authorities (in particular AGCOM), consumer associations, and the Monitoring Body for the Code of conduct on telemarketing and telesales activities; a constant commitment to providing – as early as the fact-finding activity – feedback, clarifications and operational guidance in response to the vast number of reports and complaints submitted by data subjects (amounting to thousands); an in-depth fact-finding activity beginning with the examination of reports and complaints – including through inspections – which led to the adoption of corrective measures and sanctions, which in some cases had significant interpretative implications. It is worth noting in this context that the vast majority of investigations carried out revealed – as in previous years – failure on the part of data controllers to comply with their accountability obligations. Hence, the Authority once again was compelled to reiterate principles and guidelines that should be assumed to be well established: the need for appropriate oversight throughout the entire data processing chain; the need to implement suitable technical and organisational measures; and the need to use contact lists acquired from third parties that comply with regulatory requirements, particularly with regard to the accuracy of the information provided to data subjects and the validity of their consent.

vaggio, il Garante si confronta con sempre maggiore frequenza con tecniche più aggiornate di *digital advertising*, cosicché le informazioni anagrafiche vengono acquisite mediante moduli presenti su siti web di comparazione o portali riguardanti concorsi a premi e social network, che utilizzano informative generiche e poco trasparenti non idonee a verificare l'identità del soggetto che fornisce i dati e l'esattezza delle informazioni acquisite. Tutto questo conferisce una parvenza di liceità a pratiche di fatto illecite e ha richiesto all'Autorità l'individuazione di strategie, ancora una volta, più raffinate e articolate anche attraverso la cooperazione delle associazioni di categoria e degli operatori di telemarketing e *teleselling* che hanno aderito all'apposito codice di condotta (cfr. Relazione 2024). Nello stesso solco si inseriscono le risposte fornite dal Garante in casi di furto d'identità e frodi informatiche (cfr. par. 14.2), basate su comportamenti fraudolenti sempre più sofisticati e complessi sul piano tecnologico; qui il Garante ha ricordato di aver reso disponibile, sul proprio sito, una scheda informativa per sensibilizzare gli utenti rispetto ad alcuni accorgimenti e cautele da adottare al fine di evitare di rimanere vittime di queste condotte illecite.

11. Per attraversare la complessità confrontandosi con le sue varie declinazioni in modo efficace, occorrono preparazione e formazione adeguate. In questo senso, l'Autorità ha proseguito l'attività di mappatura, aggiornamento e formalizzazione di alcuni processi rilevanti per la gestione della sicurezza, e ha rafforzato nel corso del 2025 la propria postura di sicurezza (cfr. cap. 26) in termini di capacità di rilevazione e risposta agli incidenti cyber, tanto dal punto di vista tecnico quanto da quello organizzativo, con la progettazione di un modello operativo di governo della gestione degli incidenti. Allo stesso tempo, ha puntato ad aumentare la consapevolezza in ambito cyber, attraverso l'erogazione di sessioni di formazione a favore di tutto il personale dell'Autorità. Le attività di formazione hanno riguardato, per tornare a un tema

However, in addition to dealing with the traditional practices that characterise unsolicited telemarketing, the Garante is increasingly confronted with more up-to-date digital advertising techniques, such that personal data is acquired via forms on comparison websites or portals related to prize competitions and social networks, which use generic and opaque privacy notices that are unsuitable for verifying the identity of the data subject and the accuracy of the information obtained. All of this makes unlawful practices appear legitimate and has required the Authority to identify more refined and articulated strategies once again, including through cooperation with trade associations and telemarketing and telesales operators who have agreed to comply with the relevant Code of Conduct (see Annual Report 2024). Along the same lines are the responses provided by the Garante in cases of identity theft and cyber fraud (see paragraph 14.2), which involve increasingly sophisticated and technologically complex fraudulent behaviour; in this regard, the Garante reminded users that an information sheet is available on its website to raise awareness about certain precautions and measures to take so as to be protected against such unlawful practices.

11. Suitable preparation and training are essential to work one's way through such complexity and effectively address the wide variety of forms it can take. In this regard, the Authority continued to be engaged in the mapping, updating and standardisation of specific processes for security management, and in 2025 strengthened its security capabilities (see Chapter 26) by enhancing its capacity to detect and respond to cyber incidents, both from a technical and an organisational perspective, with the development of an operational incident management governance model. At the same time, it has focused on raising awareness about cyber issues by delivering training sessions for all its staff. Another key training activity

chiave, anche le tecniche di IA e le loro applicazioni, grazie alla convenzione rinnovata con il consorzio interuniversitario italiano (CINI) che ha messo a disposizione del Garante qualificati docenti al fine di svolgere una serie di lezioni su queste tematiche. Per altro verso, è proseguita la formazione erogata a seguito dell'entrata in vigore del codice dei contratti pubblici (d.lgs. n. 36/2023), per i responsabili unici di progetto (RUP) e per il personale assegnato alle attività contrattuali, ai fini della qualificazione della stazione appaltante presso l'ANAC. Si deve rilevare, infatti, che l'emanazione del cosiddetto decreto correttivo al codice dei contratti pubblici (d.lgs. n. 209/2024) ha reso necessario (cfr. cap. 25) proseguire nell'aggiornamento dei processi lavorativi alle nuove procedure, anche alla luce delle ulteriori competenze tecnico-giuridiche richieste dalle numerose modifiche apportate dal decreto correttivo. Tutto questo ha imposto all'Autorità, ancora una volta, un serrato sforzo volto a mantenere autonomia organizzativa anche in materia di appalti pubblici, come si conviene ad una autorità indipendente.

12. Il quadro che l'attività svolta nel 2025 ci consegna è, dunque, quello di un'Autorità seriamente e fattivamente impegnata a confrontarsi con la complessità derivante dall'interazione fra il nuovo che avanza e lo stratificarsi di cattive abitudini dure a morire. Bisogna dire, del resto, che attraversare la complessità è in qualche modo un tratto connaturato all'Autorità per la protezione dei dati personali, se già nella "Prefazione" alla sua seconda relazione di attività, quella dedicata al lavoro svolto nel 1998, cioè nel primo anno di compiuta attività dopo la sua istituzione, si legge che "questa seconda relazione coglie il Garante in un momento di passaggio difficile da un avvio avventuroso a una stabilità non ancora raggiunta". Un passaggio difficile è senza dubbio quello che il Garante (e non solo) sta vivendo in questa fase storica, e tenere fede al proprio statuto costitutivo, al proprio DNA si potrebbe dire, è probabilmente l'unica delle opzioni possibili.

focused on AI techniques and their applications, made possible by a renewed agreement with CINI (the Italian Inter-University Consortium), which provided the Garante with highly qualified lecturers to deliver on these topics. At the same time, training for sole project managers (RUP) and staff assigned to contractual activities continued following the entry into force of the Public Contracts Code (Legislative Decree No. 36/2023), with a view to qualifying as contracting authority before ANAC. It is worth noting that the issuance of the so-called corrective decree to the Public Contracts Code (Legislative Decree No. 209/2024) made it necessary (see Chapter 25) to further upgrade working processes in light of the new procedures, particularly given the additional technical and legal expertise required by the numerous amendments introduced by the corrective decree. This has once again required the Authority to put in a great deal of effort to maintain organisational autonomy in the area of public procurement as well, as is appropriate for an independent authority.

12. The work carried out in 2025 paints a picture of an Authority that is seriously and actively committed to working its way through the complexity arising from the clash between the new advances and the consolidation of hard-to-break bad habits. It is worth remarking that working through such complexity is in some way an inherent characteristic of an authority for the protection of personal data. This was already evident in the 'Preface' to its second activity report on the work carried out in 1998 – its first full year of activity following its establishment – in which it is stated that 'this second report finds the Garante in a difficult transition from an adventurous start to a stability not yet achieved'. A difficult transition is undoubtedly what the Garante (along with others) is experiencing at this historic juncture, and keeping faith with its founding charter – what might be called its DNA – is probably the only viable option.

I

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

2 Principali novità normative in materia di protezione dei dati personali

Nel 2025 sono stati approvati numerosi provvedimenti normativi rilevanti in termini di protezione dei dati personali. Si analizzano di seguito gli atti normativi maggiormente incidenti sulla materia.

2.1. *Le leggi*

Semplificazione imprese

La l. 2 dicembre 2025, n. 182, recante disposizioni per la semplificazione e la digitalizzazione dei procedimenti in materia di attività economiche e di servizi a favore dei cittadini e delle imprese, è intervenuta direttamente sul Codice, novellandolo.

In particolare, l'art. 72, comma 1, lett. g), ha disposto l'abrogazione dei commi 2, 4 e 6 dell'art. 2-o*cties* del Codice. Le disposizioni abrogate prevedevano che, in assenza di disposizioni di legge o di regolamento, i trattamenti dei dati di cui all'art. 10 del RGPD e le garanzie appropriate per i diritti e le libertà degli interessati fossero individuati con decreto del Ministro della giustizia, da adottarsi previo parere del Garante. Il medesimo decreto, inoltre, avrebbe dovuto: individuare le garanzie appropriate per gli interessati, ove non già indicate dalle disposizioni di settore; autorizzare il trattamento dei dati di cui all'art. 10 del RGPD, effettuato in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con le prefetture-UTG, individuando le tipologie dei dati trattati, gli interessati, le operazioni di trattamento eseguibili, anche in relazione all'aggiornamento e alla conservazione, con previsione delle garanzie per i diritti e le libertà degli interessati.

L'art. 72, comma 2, della medesima legge dispone, altresì, l'abrogazione del comma 2 dell'art. 5, d.lgs. n. 51/2018 e apporta, di riflesso, le conseguenti modifiche di coordinamento agli artt. 14, comma 2, alinea, 21, comma 1 e 49, comma 3. Per i trattamenti o le categorie di trattamenti non occasionali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali, è stato dunque eliminato il riferimento all'individuazione, tramite decreto del Presidente della Repubblica, dei termini (ove non già stabiliti da disposizioni di legge o di regolamento) e delle modalità di conservazione dei dati, dei soggetti legittimati ad accedervi, delle condizioni di accesso, delle modalità di consultazione, nonché dei modi e delle condizioni per l'esercizio dei diritti previsti dagli artt. 9, 10, 11 e 13 del medesimo decreto legislativo.

Legge di bilancio 2026

La l. 30 dicembre 2025, n. 199, recante il bilancio di previsione dello Stato per l'anno finanziario 2026 e bilancio pluriennale per il triennio 2026-2028, prevede al suo art. 1, numerose disposizioni di interesse in materia di protezione dei dati personali, tra le quali si segnalano, in particolare:

- il comma 111, che reca le misure di contrasto agli inadempimenti in materia di imposta sul valore aggiunto, introducendo l'art. 54-*bis*.1 al d.P.R. n. 633/1972, che permette all'Agenzia delle entrate di procedere, in caso di omissione di dichiarazione annuale IVA, alla liquidazione dell'imposta anche avvalendosi di procedure automatizzate, basandosi su fatture elettroniche emesse e ricevute, corrispettivi telematici ed elementi

desumibili dalle comunicazioni dei dati delle liquidazioni periodiche;

- il comma 117, di novella dell'art. 1, comma 5-*bis*, d.lgs. n. 127/2015, che estende il patrimonio informativo a disposizione dell'agente della riscossione e autorizza l'Agenzia delle entrate a condividere con quest'ultimo i dati relativi alla somma dei corrispettivi delle fatture emesse da debitori iscritti a ruolo e dai loro coobbligati nei confronti di uno stesso soggetto nei sei mesi precedenti, per le attività di analisi mirate all'avvio di procedure esecutive presso terzi;

- il comma 256, che estende ai componenti degli organi di vertice delle autorità amministrative indipendenti le misure relative ai benefici di natura assistenziale e sociale (ivi incluse quelle in materia di previdenza complementare e di welfare integrativo) previste per il personale dipendente, sulla base di una delibera adottata a tal fine dai singoli collegi o organi di vertice comunque denominati;

- il comma 373, che reca disposizioni in tema di adeguamento della piattaforma informatica dell'INPS per il potenziamento dell'assistenza a tutela della salute psicologica e psicoterapeutica, al fine di garantire un efficace aggiornamento delle modalità di gestione, erogazione e monitoraggio del contributo di cui all'art. 1-*quater*, comma 3, d.l. n. 228/2021 convertito, con modificazioni, dalla l. 25 febbraio 2022, n. 15 (cd. bonus psicologo);

- i commi da 381 a 384, che contengono disposizioni in materia di dematerializzazione della ricetta per l'erogazione dei prodotti per soggetti affetti da celiachia, introducendo la generazione di un buono dematerializzato a carico del SSN tramite il Sistema tessera sanitaria. In tale quadro viene demandato a un decreto del Ministro della salute, previo parere del Garante, l'individuazione dei criteri standard per la definizione e l'attuazione tramite il Sistema tessera sanitaria del sistema centralizzato di generazione del buono dematerializzato; delle modalità di assegnazione del budget mensile; delle modalità di utilizzo del buono dematerializzato presso i negozi convenzionati e, infine della tracciabilità dell'importo del budget residuo;

- il comma 405, che stanzia appositi fondi al fine di assicurare la continuità assistenziale nell'ambito dell'Unione europea, mediante la realizzazione di infrastrutture che prevedono servizi di scambio transfrontaliero e consentono la traduzione e lo scambio delle ricette elettroniche, del profilo sanitario sintetico, dei documenti clinici originali, dei referti di laboratorio, delle schede di dimissione ospedaliera e dei referti di diagnostica per immagini, tramite il Sistema tessera sanitaria;

- il comma 410, che stanzia appositi fondi per il potenziamento e l'efficientamento dei servizi di telemedicina, in particolare mediante l'implementazione di procedure finalizzate a dotare i professionisti sanitari di dispositivi medici idonei a garantire l'adeguato monitoraggio dei pazienti, nonché a favorire l'implementazione omogenea dei percorsi di telemedicina;

- i commi da 706 a 708, che definiscono il livello essenziale delle prestazioni (LEP) per l'assistenza all'autonomia e alla comunicazione degli alunni con disabilità. In particolare, si individua il contenuto del LEP (numero di ore di assistenza all'autonomia e alla comunicazione personale e l'impiego di personale in possesso di specifico profilo professionale) e si stabilisce che entro il 31 dicembre 2027 debba essere alimentato un registro nazionale per la ricognizione del fabbisogno territoriale aggregato delle ore prestate e degli utenti assistiti. Si demanda la definizione dei criteri tecnici, delle modalità per l'accesso, della condivisione e utilizzo dei dati contenuti nel registro, ad un decreto dell'autorità politica delegata in materia di disabilità, di concerto con il Ministro dell'istruzione e del merito, con il Ministro dell'economia e delle finanze e l'autorità politica delegata per gli affari regionali e le autonomie;

- i commi 723 e 724, che recano disposizioni in materia di revisione e di razionalizzazione

della spesa, prevedendo il primo che l'INPS accerti, su richiesta del datore di lavoro, la permanenza dei requisiti sanitari per i quali sono riconosciuti i permessi di cui alla l. n. 104/1992, ai dipendenti delle p.a. di cui all'art. 1, comma 2, d.lgs. n. 165/2001. Per lo svolgimento di tali verifiche, l'INPS può avvalersi, tramite specifiche convenzioni, delle risorse umane e strumentali delle aziende sanitarie locali, delle aziende ospedaliere, degli istituti di ricovero e cura a carattere scientifico pubblici, delle aziende ospedaliere universitarie integrate con il SSN (art. 19, comma 2, lett. c), d.lgs. n. 118/2011), nonché dei medici della sanità militare. Le modalità di attuazione del predetto comma 723 sono rimesse a un decreto del Ministro del lavoro e delle politiche sociali, sentito l'INPS. Il comma 724, invece, al fine di potenziare il sistema dei controlli sulla fruizione dei permessi di cui all'art. 33 della l. n. 104/1992, dei congedi straordinari e parentali spettanti ai lavoratori, introduce l'obbligo in capo alle p.a. di inserire le informazioni relative all'evento fruito e al relativo dante causa nelle denunce mensili di cui all'art. 44, comma 9, d.l. n. 269/2003, convertito, con modificazioni, dalla l. n. 326/2003;

- i commi da 867 a 869, che autorizzano – al fine di potenziare il coordinamento tra il Ministero della salute, amministrazioni regionali e province autonome – il finanziamento della raccolta dei dati relativi alle misure di contenzione meccanica presso le strutture sanitarie afferenti ai dipartimenti di salute mentale, prevedendo anche l'istituzione di una apposita banca dati. Tali informazioni sono raccolte dalla direzione di ciascun dipartimento di salute mentale e censite nel registro di raccolta regionale che alimenta il flusso di dati del Sistema informativo per il monitoraggio e la tutela della salute mentale curato dai competenti uffici del Ministero della salute (comma 868). Il comma 869, infine, demanda ad un decreto del Ministro della salute la definizione delle modalità di attuazione dei due precedenti commi.

Intelligenza artificiale

La l. 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale, introduce diverse disposizioni rilevanti per la protezione dei dati oltre alle deleghe di adeguamento al reg. (UE) 2024/1689 (cd. AI Act). L'art. 3, in particolare, reca i princìpi di carattere generale, disponendo tra l'altro che la ricerca, la sperimentazione, lo sviluppo, l'adozione, l'applicazione e l'utilizzo di sistemi e modelli di IA per finalità generali debbano avvenire nel rispetto dei diritti fondamentali e delle libertà costituzionali, del diritto dell'Unione europea e dei principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, nonché su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza.

L'art. 4 enuncia i principi in materia di "informazione e riservatezza dei dati personali", imponendo, da un lato, l'utilizzo dei sistemi di IA senza pregiudizio per la libertà e il pluralismo dei mezzi di comunicazione, la libertà di espressione e l'obiettività, completezza, imparzialità e lealtà dell'informazione e, dall'altro, garantendo la liceità, correttezza e trasparenza del trattamento, nonché la sua compatibilità con le finalità della raccolta e con vincolo di conformità al diritto unionale. È richiesto che le informazioni e le comunicazioni da rendere agli interessati in ordine al trattamento dei loro dati personali siano chiare e comprensibili, al fine di garantire la conoscibilità dei rischi connessi all'utilizzo dei sistemi di IA e il diritto di opporsi ai trattamenti autorizzati. La disposizione reca infine la disciplina per l'accesso alle tecnologie di IA e il conseguente trattamento dei dati personali relativi a infraquattordicenni, richiedendo il consenso di chi esercita la responsabilità genitoriale nel rispetto di quanto stabilito dal RGPD e dal Codice. Il minore ultraquattordicenne può esprimere il consenso al trattamento dei propri dati personali purché le informazioni e comunicazioni di cui sopra siano facilmente accessibili e comprensibili.

L'art. 7 individua gli scopi, i diritti (in particolare d'informazione), le condizioni e i

limiti connessi all'impiego, in ambito sanitario e di disabilità, dei sistemi di IA, disponendo che il loro utilizzo contribuisce al miglioramento del sistema sanitario, alla prevenzione, alla diagnosi e alla cura delle malattie, nel rispetto dei diritti, delle libertà e degli interessi della persona, anche in materia di protezione dei dati personali; la disposizione vieta di selezionare e condizionare l'accesso alle prestazioni sanitarie secondo criteri discriminatori e riconosce agli interessati il diritto di essere informati in ordine all'impiego delle tecnologie di IA.

Particolare interesse assume l'art. 8 che qualifica come di rilevante interesse pubblico i trattamenti di dati personali effettuati per finalità di ricerca e sperimentazione scientifica in ambito sanitario. La norma legittima, inoltre, l'utilizzo secondario dei dati personali e particolari privi degli elementi identificativi diretti, salvi i casi nei quali la conoscenza dell'identità degli interessati sia inevitabile o necessaria per finalità di tutela della loro salute (comma 2). Per specifiche finalità (segnatamente, per quelle di cui all'art. 2-*sexies*, comma 2, lett. v), del Codice) o negli ambiti di cui al comma 1, viene altresì consentito, previa informativa all'interessato, il trattamento per finalità di anonimizzazione, pseudonimizzazione o sintetizzazione dei dati personali e particolari, come pure il trattamento finalizzato allo studio e alla ricerca sui gesti atletici, sui movimenti e sulle prestazioni nell'attività sportiva in tutte le sue forme, nel rispetto dei princìpi generali e dei diritti di sfruttamento economico relativi alle attività agonistiche (comma 3). È previsto che l'AGENAS, previo parere del Garante, possa adottare e aggiornare linee guida per le procedure di anonimizzazione dei dati personali e per la creazione dei dati sintetici (comma 4), mentre allo stesso Garante è demandata la possibilità, previa comunicazione dei trattamenti di cui ai commi 1 e 2 che contenga tutte le informazioni di cui agli artt. 24, 25, 32 e 35 del RGPD e dei soggetti eventualmente designati ai sensi dell'art. 28 del medesimo RGPD, di disporre provvedimenti di blocco, in assenza dei quali è possibile avviare il trattamento (comma 5). Il comma 6, infine, fa espressamente salvi i poteri ispettivi, interdittivi e sanzionatori del Garante.

L'art. 9 rinvia a un decreto del Ministro della salute, sentito anche il Garante, la disciplina del trattamento dei dati con il massimo delle modalità semplificate consentite dal RGPD per finalità di ricerca e sperimentazione, anche tramite sistemi di IA e *machine learning*, inclusi la costituzione e l'utilizzo di spazi speciali di sperimentazione a fini di ricerca, anche mediante l'uso secondario dei dati personali.

In ambito lavorativo, la legge prevede all'art. 11 che l'impiego dell'IA non debba mai violare la riservatezza dei dati personali dei lavoratori, stabilendo che il datore di lavoro è obbligato a informare il dipendente sull'utilizzo di tali sistemi e all'art. 14 che le p.a. debbano assicurare agli interessati la conoscibilità del funzionamento dell'IA e la tracciabilità del suo utilizzo.

L'art. 20 designa quali autorità nazionali per l'IA l'AgID e l'ACN (comma 1), attribuendo alla prima la responsabilità di promuovere l'innovazione e lo sviluppo dell'IA, di definire le procedure e di esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di IA (lett. a) e alla seconda la responsabilità per la vigilanza (ivi incluse le attività ispettive e sanzionatorie) dei sistemi di IA, nonché della promozione e dello sviluppo dell'IA relativamente ai profili di cybersicurezza (lett. b)). Entrambe le autorità assicurano il coordinamento e la collaborazione con le altre p.a. e le autorità indipendenti, nonché ogni opportuno raccordo tra loro per l'esercizio delle rispettive funzioni, anche tramite il comitato di coordinamento istituito presso la Presidenza del Consiglio dei ministri (comma 3). La legge conferma esplicitamente che restano fermi i compiti e i poteri del Garante, il quale deve essere altresì consultato per

l'adozione dei decreti legislativi di adeguamento alla normativa europea sull'IA, ai sensi della delega legislativa prevista all'art. 24.

La legge reca anche disposizioni in materia di sicurezza nazionale, difesa e giustizia, prevedendo esenzioni e limiti per l'uso (comunque rispettoso dei diritti fondamentali) dell'IA a fini di sicurezza nazionale, difesa e prevenzione di reati e delega il Governo a disciplinare l'uso dell'IA nelle indagini preliminari, garantendo il rispetto del diritto di difesa e della privacy dei terzi.

È stata, infine, introdotta all'art. 26 una nuova fattispecie di reato (art. 612-*quater* c.p.) che punisce con la reclusione da uno a cinque anni chi diffonde, senza consenso, immagini, video o voci falsificati o alterati (deepfake) idonei a trarre in inganno sulla loro genuinità e a causare un danno ingiusto.

Intercettazioni

La l. 31 marzo 2025, n. 47, recante modifiche alla disciplina in materia di durata delle operazioni di intercettazione integra, in particolare, il comma 3 dell'art. 267 c.p.p., prevedendo che le intercettazioni non possano avere una durata complessiva superiore a 45 giorni, salvo che l'assoluta indispensabilità delle operazioni per una durata superiore sia giustificata dall'emergere di elementi specifici e concreti (comma 1).

Viene, altresì, novellato l'art. 13 del d.l. n. 152/1991, convertito con modificazioni dalla l. n. 203/1991, precisando che il limite generale di durata complessiva delle operazioni di intercettazione introdotto non si applica alle attività d'indagine relative a delitti di criminalità organizzata o di minaccia con il mezzo del telefono, di cui viene fatta salva la disciplina speciale recata dal medesimo art. 13 (comma 2).

2.2. *I decreti legislativi*

E-evidence

Il d.lgs. 30 dicembre 2025, n. 215, recante individuazione delle autorità competenti di cui all'art. 31 del reg. (UE) 2023/1543 del Parlamento europeo e del Consiglio, del 12 luglio 2023, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali, nonché delle procedure per l'emissione, ricezione, esecuzione e riesame degli ordini europei di produzione e di conservazione, introduce disposizioni di particolare interesse per la protezione dei dati personali.

Il provvedimento, sul cui schema il Garante ha reso parere il 25 settembre 2025 (cfr. par. 3.1.2), individua, infatti, le autorità competenti per l'emissione, la convalida e la trasmissione degli ordini europei di produzione e conservazione e delle relative notifiche; le autorità giudiziarie competenti per la ricezione, a fini di notifica ed esecuzione, degli ordini europei di produzione e conservazione e dei relativi certificati, nonché le autorità giudiziarie competenti per il riesame delle obiezioni motivate dei destinatari degli ordini europei di produzione, disciplinandone altresì le relative procedure, comprese quelle d'urgenza e di esecuzione.

Per quanto di interesse, l'art. 9 reca disposizioni di coordinamento con l'art. 132 del Codice, novellandolo. In particolare, introduce ai commi 3 e 3-*bis* il riferimento all'agevolazione delle ricerche di un latitante, al cui fine potrà essere autorizzata da parte del giudice (o del pubblico ministero per i casi d'urgenza) l'acquisizione dei dati relativi al traffico telefonico presso il fornitore.

Si introducono, inoltre, tre commi aggiuntivi (3-*bis*.1, 3-*bis*.2 e 3-*bis*.3), il primo dei quali prevede che il pubblico ministero possa ordinare ai fornitori e agli operatori di servizi telefonici, informatici o telematici la conservazione e la protezione, per un periodo non superiore a novanta giorni, dei dati relativi al traffico telefonico e telematico, esclusi comunque i contenuti delle comunicazioni, nonché dei dati relativi alle chiamate

senza risposta. Il provvedimento, prorogabile per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi telefonici, informatici o telematici, ovvero di terzi.

Viene inoltre esclusa, dal regime di applicabilità della disciplina di cui ai commi 3 e 3-*bis*, l'acquisizione dei dati relativi agli abbonati – di cui viene fornita apposita definizione (comma 3-*bis*.2) –, precisando che alla stessa provvede il pubblico ministero o la polizia giudiziaria, su delega o di propria iniziativa, ai sensi dell'art. 348 c.p.p. (comma 3-*bis*.3).

La disposizione novella inoltre il comma 4-*ter* dell'art. 132 del Codice, estendendo l'oggetto della conservazione anche ai dati relativi al traffico telefonico e ai dati relativi alle chiamate senza risposta. Il comma 4-*ter* viene, inoltre, novellato così da legittimare gli ufficiali di polizia giudiziaria all'emissione dell'ordine di conservazione per fini attinenti all'accertamento e repressione di specifici reati.

Viene aggiunto, infine, l'art. 263-*bis* al codice di rito penale, per disciplinare l'ordine di conservazione "domestico" emesso dal pubblico ministero per i dati nella disponibilità dei fornitori. L'acquisizione avverrà, poi, secondo la disciplina processuale vigente. Si è inoltre legittimata la polizia giudiziaria a disporre in via di urgenza la conservazione dei dati con provvedimento soggetto a convalida da parte del pubblico ministero.

Il d.lgs. 30 dicembre 2025, n. 216 recante attuazione della direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali, sul cui schema il Garante ha reso parere il 6 novembre 2025 (cfr. par. 3.1.2), si inserisce nel processo di implementazione dell'*e-evidence package* (di cui alla direttiva stessa e al reg. (UE) 2023/1543 su descritto) nel quadro dell'esercizio della delega legislativa conferita al Governo dall'art. 7 della l. 13 giugno 2025, n. 91 (legge di delegazione europea 2024), per conformare l'ordinamento interno alla disciplina dettata dalla direttiva (UE) 2023/1544.

In particolare, il decreto legislativo al suo art. 3, comma 2, in attuazione dell'art. 3, par. 1, della direttiva, impone ai prestatori di servizi rivolti all'Unione la designazione di stabilimenti o la nomina di rappresentanti legali per consentire la ricezione, ottemperanza ed esecuzione dei provvedimenti di acquisizione delle prove elettroniche, con l'eccezione dei prestatori di servizi stabiliti in Italia e che offrono servizi esclusivamente sul territorio nazionale.

L'art. 4 declina gli obblighi dei prestatori di servizi di designazione e nomina, rispettivamente, degli stabilimenti designati e dei rappresentanti legali, diversificandoli a seconda che abbiano personalità giuridica e siano stabiliti in Italia (comma 1), abbiano personalità giuridica ma non siano stabiliti nell'Unione pur offrendo servizi in Italia (comma 2), oppure siano stabiliti in Stati membri che non partecipano agli strumenti indicati nell'art. 3, comma 1 e offrano servizi in Italia (comma 3).

Coerentemente con gli artt. 4 e 5 della direttiva, inoltre, l'art. 6 reca disposizioni in materia di notifica, all'autorità centrale (ovvero a quella del diverso Stato membro in cui lo stabilimento designato è stabilito o il rappresentante legale risiede), dei dati di contatto dello stabilimento o del rappresentante legale dei prestatori di servizi stabiliti o che offrono servizi in Italia, nonché sulle lingue in cui è possibile rivolgersi allo stabilimento designato o al rappresentante legale. L'art. 8, infine, designa il Ministero dell'interno quale autorità centrale ai fini dell'attribuzione dei relativi compiti di vigilanza e controllo sul rispetto delle norme, nonché per l'esercizio dei poteri sanzionatori.

2.3. *I decreti-legge*

Milleproroghe

La l. 21 febbraio 2025, n. 15, ha convertito, con modificazioni, il d.l. 27 dicembre 2024, n. 202, recante disposizioni urgenti in materia di termini normativi (cd. milleproroghe).

Il testo del provvedimento, come risultante dalle modifiche apportate in sede di conversione, risulta composto da 22 articoli e reca importanti disposizioni in materia di termini normativi, tra cui si segnalano:

- l'art. 10, comma 7, che proroga al 31 dicembre 2025 il termine a partire dal quale dovranno essere utilizzate le cosidette infrastrutture digitali interdistrettuali per compiere le operazioni di intercettazione nei procedimenti penali;
- l'art. 18, comma 2, che nel novellare l'art. 4, comma 2-*bis*, d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, dalla l. 31 luglio 2005, n. 15, proroga al 30 giugno 2025 il termine entro il quale il Presidente del Consiglio dei ministri può delegare i direttori delle agenzie d'informazione per la sicurezza interna e esterna (AISI e AISE) o altro personale delegato a svolgere colloqui investigativi con i detenuti, ai fini di prevenzione del terrorismo internazionale;
- l'art. 19-*quater*, comma 1, che estende ad alcuni territori la sperimentazione delle disposizioni relative alla valutazione di base e alla valutazione multidimensionale per l'elaborazione e attuazione del progetto di vita individuale personalizzato e partecipato per le persone con disabilità, stabilendo tra l'altro che il diritto di richiedere l'elaborazione del progetto di vita sia riconosciuto anche in favore di coloro che sono in possesso di una certificazione *ex lege* 5 febbraio 1992, n. 104, rilasciata prima del 1° gennaio 2027, senza effettuare la valutazione di base.

Sicurezza sul lavoro

La l. 29 dicembre 2025, n. 198, ha convertito, con modificazioni, il d.l. 31 ottobre 2025, n. 159, che introduce misure urgenti per la tutela della salute e della sicurezza sui luoghi di lavoro e in materia di protezione civile.

Una delle prime disposizioni di interesse del decreto è l'art. 3, comma 2, che prevede il rafforzamento dello strumento della tessera di riconoscimento, prevista dall'art. 18, comma 1, lett. u), d.lgs. n. 81/2008, nonché dall'art. 5 della l. n. 136/2010. In particolare, in esso si stabilisce che le imprese che operano nei cantieri edili in regime di appalto e subappalto (pubblico o privato) e in altri ambiti ad alto rischio (individuati con decreto ministeriale) debbano fornire ai dipendenti una tessera di riconoscimento, già prevista dal d.lgs. n. 81/2008 e dalla l. n. 136/2010, dotata di un codice univoco anticontraffazione e utilizzabile come badge identificativo del lavoratore. La tessera, resa disponibile anche in modalità digitale tramite strumenti interoperabili con la piattaforma SIISL (Sistema informativo per l'inclusione sociale e lavorativa), è prodotta automaticamente e precompilata, con possibilità di integrazione da parte del datore di lavoro, per i lavoratori assunti sulla base delle offerte di lavoro pubblicate mediante la medesima piattaforma.

L'art. 14 reca disposizioni volte a favorire l'occupazione e la sicurezza nei luoghi di lavoro attraverso il SIISL, nonché la trasparenza nel mercato del lavoro e le pari opportunità tra i lavoratori. Al riguardo, si prevede, al comma 1, che a decorrere dal 1° aprile 2026 i datori di lavoro debbano pubblicare le posizioni lavorative disponibili sul SIISL per ottenere i benefici contributivi, comunque denominati e finanziati con risorse pubbliche. Il comma 2 stabilisce che le comunicazioni obbligatorie di cui all'art. 9-*bis*, d.l. n. 510/1996, convertito, con modificazioni, dalla l. n. 608/1996, possano essere effettuate anche tramite il sistema SIISL, mentre il comma 3 stabilisce che il SIISL renda conoscibili gli esiti delle verifiche dei dati autocertificati dagli utenti iscritti, rendendoli disponibili ai datori di lavoro che li assumono, anche al fine di rafforzare le

garanzie di affidabilità e sicurezza nella gestione del rapporto di lavoro.

Il comma 4, infine, prevede che le agenzie per il lavoro siano tenute alla pubblicazione sul SIISL di tutte le posizioni di lavoro che gestiscono e, nel rispetto della normativa sul trattamento dei dati personali, possono accedere alla piattaforma per individuare i candidati idonei rispetto alle posizioni lavorative pubblicate.

L'art. 17, infine, novella l'art. 41, d.lgs. n. 81/2008, stabilendo che la sorveglianza sanitaria comprende anche la visita medica finalizzata alla verifica della circostanza per cui il lavoratore non si trovi sotto l'effetto di alcol o sostanze stupefacenti o psicotrope, per le attività lavorative ad elevato rischio infortuni.

Sicurezza pubblica

La l. 9 giugno 2025, n. 80, ha convertito con modificazioni, il d.l. 11 aprile 2025, n. 48, recante disposizioni urgenti in materia di sicurezza pubblica, di tutela del personale in servizio, nonché di vittime dell'usura e di ordinamento penitenziario.

Il decreto mediante l'art. 2, novella l'art. 17 del d.l. n. 113/2018 disponendo che a fini di prevenzione del terrorismo e delle attività illecite, sia effettuata la comunicazione, da parte degli esercenti dell'autonoleggio, dei dati identificativi del soggetto richiedente il servizio (per il loro inserimento e raffronto nel Centro elaborazione dati) e dei dati identificativi del veicolo (targa, telaio, passaggi di proprietà e subnoleggio). È previsto, inoltre, che il Centro elaborazione dati proceda al raffronto automatico dei dati comunicati con quelli conservati al suo interno, anche con riguardo alle segnalazioni inserite dalle forze di polizia in merito ai reati di cui all'art. 51, comma 3-*bis*, c.p.p.

L'art. 3 introduce modifiche al codice delle leggi antimafia e delle misure di prevenzione, inserendo, nel novero dei soggetti sottoposti a verifica antimafia, le imprese aderenti al cd. contratto di rete e prevedendo l'esclusione, salvo eccezioni, di alcuni divieti e decadenze ex art. 67, comma 1, d.lgs. n. 159/2011 nei confronti delle imprese individuali, laddove si accerti che per effetto dell'applicazione di tali disposizioni verrebbero a mancare i mezzi di sostentamento al titolare dell'impresa e alla sua famiglia.

L'art. 6 novella l'art. 13 del d.l. n. 8/1991, convertito, con modificazioni, dalla l. n. 82/1991, introducendo alcune disposizioni in materia di protezione di collaboratori e testimoni di giustizia, in particolare per quanto concerne il rilascio delle identità di copertura al fine di elevarne ulteriormente il livello di protezione. Si consente l'utilizzo di documenti di copertura da parte dei collaboratori e dei loro familiari sottoposti alla misura cautelare degli arresti domiciliari o che fruiscano della detenzione domiciliare, nonché la creazione di identità fiscali di copertura, anche di tipo societario, da parte del Servizio centrale di protezione, qualora ciò si renda necessario per il compimento di particolari atti o per lo svolgimento di specifiche attività di natura riservata e al fine di garantire la sicurezza, la riservatezza e il reinserimento sociale delle persone sottoposte a speciale programma di protezione, nonché la funzionalità, la riservatezza e la sicurezza delle speciali misure di protezione. A tal fine, è previsto che il Servizio centrale di protezione si avvalga della collaborazione delle autorità e degli altri soggetti competenti. La disposizione, inoltre, vieta alle autorità e agli altri soggetti interessati di rifiutarsi di predisporre i documenti e di procedere alle registrazioni, istituendo infine un registro riservato attestante i tempi, le procedure e i motivi dell'autorizzazione al rilascio del documento e ogni altra documentazione relativa alla creazione di identità fiscali di copertura, anche di tipo societario.

L'art. 21 consente alle forze di polizia di utilizzare dispositivi di videosorveglianza indossabili nei servizi di mantenimento dell'ordine pubblico, di controllo del territorio, di vigilanza di siti sensibili, nonché in ambito ferroviario e a bordo dei treni. Si prevede inoltre la possibilità di utilizzo dei dispositivi di videosorveglianza nei luoghi e negli ambienti in cui vengono trattenute persone sottoposte a restrizione della libertà personale.

L'art. 30 integra il comma 3 dell'art. 19 della legge-quadro sulle missioni internazionali

(l. n. 145/2016), che contiene disposizioni in materia penale applicabili al personale che partecipa a tali missioni. In particolare, estende la non punibilità di detto personale anche all'uso di apparecchiature, dispositivi, programmi, apparati, strumenti informatici o altri mezzi idonei a commettere i delitti di violazione del domicilio, della corrispondenza e delle comunicazioni, di illegittime interferenze nella vita privata, nonché di violazione dei segreti.

L'art. 31 reca disposizioni per il potenziamento dell'attività di informazione per la sicurezza, stabilizzando, tra l'altro, la previsione relativa alla possibilità di condurre colloqui con detenuti e internati per finalità di acquisizione informativa per la prevenzione di delitti con finalità terroristica di matrice internazionale e prevedendo la possibilità, per AISI e AISE, di richiedere al Nucleo speciale di polizia valutaria della Guardia di finanza e alla Direzione investigativa antimafia le informazioni e le analisi finanziarie connesse alle esigenze di contrasto del terrorismo.

L'art. 32 modifica l'art. 30 del codice delle comunicazioni elettroniche (d.lgs. n. 259/2003), prevedendo la sanzione amministrativa accessoria della chiusura dell'esercizio o dell'attività da 5 a 30 giorni per i casi nei quali le imprese autorizzate a vendere schede SIM non osservino gli obblighi di identificazione dei clienti. Inoltre, con riferimento alla conclusione di contratti il cui oggetto sia un servizio per la telefonia mobile, viene previsto che al cliente, se cittadino di paese non appartenente all'Unione europea, sia richiesta copia del titolo di soggiorno di cui è in possesso ovvero del passaporto o del documento di viaggio equipollente o di un documento di riconoscimento in corso di validità (per il caso in cui il cliente lo abbia smarrito o gli sia stato sottratto, è necessario fornire copia della denuncia di smarrimento o furto).

L'art. 33 introduce nella l. n. 108/1996, che detta disposizioni in materia di usura, il nuovo art. 14-*bis*, che istituisce un albo di esperti da affiancare agli operatori economici vittime di usura ai fini del loro reinserimento nel circuito economico legale, stabilendo altresì le norme fondamentali che disciplinano i compiti, le incompatibilità e decadenze, la durata dell'incarico e il compenso loro spettante. La richiesta di iscrizione all'albo deve essere corredata da un'autocertificazione che attesti l'assenza di cause di divieto, sospensione o decadenza di cui all'art. 67 del codice antimafia. L'esperto, inoltre, è tenuto alla riservatezza sui fatti e sui documenti di cui ha conoscenza in ragione delle sue funzioni.

3 I rapporti con il Parlamento e le altre istituzioni

3.1. *L'attività consultiva del Garante*

La consultazione del Garante sugli atti normativi (di rango primario e non), resa obbligatoria dal RGPD (artt. 36, par. 4, e 57, par. 1, lett. c), cons. n. 96) e dalla direttiva UE 2016/680 (art. 28, par. 2, e art. 24, comma 2, d.lgs. n. 51/2018), contribuisce, in linea generale, all'individuazione di un più corretto bilanciamento tra i diritti nell'ambito delle norme che prevedono trattamenti di dati personali, e comporta un impegno considerevole per l'Autorità in termini sia quantitativi sia qualitativi.

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

Il coinvolgimento del Garante nell'ambito del procedimento legislativo o, comunque, dell'esercizio delle funzioni conoscitiva, di indirizzo e controllo delle Camere è risultato, nel 2025, alquanto significativo.

Numerosi sono stati 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, peraltro, frequente il ricorso allo strumento dell'audizione parlamentare, che offre anche la possibilità di un dialogo diretto tra le Commissioni e il Garante, mediante il dibattito successivo alla relazione.

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

a) memoria trasmessa alla II Commissione giustizia della Camera, nell'ambito dell'esame congiunto dei d.d.l. AC 632 e AC 2328, in materia di pubblicazione delle pronunce favorevoli agli indagati/imputati e di tutela della buona fama e riservatezza in Internet - 27 novembre 2025 (doc. web n. 10198976);

b) audizione dinanzi alla 8ª Commissione del Senato nell'ambito dell'esame del d.d.l. AS 1136, recante disposizioni sulla tutela dei minori nella dimensione digitale - 7 ottobre 2025 (doc. web n. 10176218);

c) audizione dinanzi alla 9ª Commissione del Senato nell'ambito dell'esame del d.d.l. AS 1578, recante legge annuale per il mercato e la concorrenza per il 2025 - 11 settembre 2025 (doc. web n. 10166076);

d) memoria trasmessa alla 9ª Commissione del Senato nell'ambito dell'esame congiunto dei d.d.l. AS 1484-AS 37 e AS 565, recanti la legge annuale sulle piccole e medie imprese - 30 luglio 2025 (doc. web n. 10160213);

e) audizione dinanzi alla III Commissione della Camera nell'ambito dell'esame del d.d.l. AC 2369, recante disposizioni per la revisione dei servizi per i cittadini e le imprese all'estero - 8 luglio 2025 (doc. web n. 10148096);

f) audizione dinanzi alla Commissioni IX e X riunite della Camera, nell'ambito

dell'esame del d.d.l. AC 2316 recante disposizioni e deleghe al Governo in materia di intelligenza artificiale - 7 maggio 2025 (doc. web n. 10129226);

g) audizione dinanzi alle Commissioni riunite IX e X della Camera nell'ambito dell'esame delle proposte di legge C. 579 De Luca, C. 1316 Longi, C. 2040 Iaria, C. 2045 Barabotti, C. 2062 Ghirra e C. 2081 Pastorella, recanti modifiche alla l. 11 gennaio 2018, n. 5, e altre disposizioni in materia di organizzazione e funzionamento dei call center, di formazione del personale, di tutela dell'occupazione e di protezione dei consumatori - 5 febbraio 2025 (doc. web n. 10099791).

Non sono mancate richieste di contributi anche nell'ambito dell'esercizio delle funzioni conoscitiva, di indirizzo e controllo delle Camere o, anche, di esame del rispetto del principio di sussidiarietà degli atti europei, che dimostrano una diffusa sensibilità rispetto alla protezione dei dati personali e alle sue istanze.

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

a) memoria trasmessa alla XIV Commissione della Camera nell'ambito dell'esame delle proposte di regolamento del Parlamento europeo e del Consiglio (COM(2025) 501) e di direttiva del Parlamento europeo e del Consiglio (COM(2025) 502), componenti il quarto pacchetto di semplificazione (cd. Omnibus IV), presentato dalla Commissione europea nell'ambito del programma REFIT - 24 luglio 2025 (doc. web n. 10153209);

b) audizione dinanzi alla Commissione straordinaria per la tutela e la promozione dei diritti umani del Senato nell'ambito dell'indagine conoscitiva sui livelli e i meccanismi di tutela dei diritti umani in Italia e nella realtà internazionale - 8 luglio 2025 (doc. web n. 10148337);

c) audizione dinanzi alla Commissione parlamentare di vigilanza sull'Anagrafe tributaria della Camera, nell'ambito dell'indagine conoscitiva sulla sicurezza delle banche dati dell'Anagrafe tributaria e sulla tutela della riservatezza dei dati dei contribuenti - 22 ottobre 2025 (https://webtv.camera.it/evento/29281);

d) audizione dinanzi alla Commissione parlamentare per la semplificazione della Camera nell'ambito dell'indagine conoscitiva in materia di semplificazione e digitalizzazione delle procedure amministrative nei rapporti tra cittadino e pubblica amministrazione - 16 gennaio 2025 (doc. web n. 10092941).

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 rispetto alla iniziativa legislativa del Governo ovvero agli atti aventi forza di legge, incidenti sulla materia di interesse.

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

a) parere 6 novembre 2025, n. 659, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo recante modifiche e integrazioni al d.lgs. n. 231/2007, per il recepimento dell'art. 74 della direttiva (UE) 2024/1640, relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (doc. web n. 10195739). Lo schema di decreto interviene, in particolare, sulle disposizioni in materia di accesso alle informazioni sulla titolarità effettiva di imprese dotate di personalità giuridica e persone giuridiche private, adeguando il quadro normativo al diritto unionale e legittimando l'accesso alla sezione autonoma del registro – comprensiva delle informazioni e dei dati dei titolari effettivi delle imprese dotate di personalità giuridica e delle persone giuridiche private – oltre alle autorità e ai soggetti obbligati, soltanto ai soggetti privati (compresi quelli portatori di interessi diffusi) titolari di un interesse giuridico rilevante e differenziato. Considerato lo scopo del provvedimento e l'assenza di profili di criticità in termini di

protezione dati, il Garante ha reso parere favorevole, non ritenendo sussistenti i presupposti per la formulazione di rilievi;

b) parere 6 novembre 2025, n. 658, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo di attuazione alla direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali (doc. web n. 10195794). Lo schema di provvedimento è volto a rendere più efficace l'attività di contrasto in ambito penale nello spazio di libertà, sicurezza e giustizia dell'Unione, concorrendo a garantire che l'acquisizione transfrontaliera delle prove elettroniche da parte delle autorità di contrasto e giudiziarie dei singoli Stati membri si inscriva in un contesto di norme armonizzate. A tal fine, si sancisce, in capo ai soggetti che offrono servizi nell'Unione, l'obbligo di rispondere direttamente alle richieste provenienti dalle autorità di un altro Stato membro, previa emissione di un ordine di produzione o conservazione delle prove elettroniche. In assenza di criticità del provvedimento dal punto di vista della protezione dei dati personali, il Garante ha reso parere favorevole;

c) parere 23 ottobre 2025, n. 614, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2023/2668 del Parlamento europeo e del Consiglio del 22 novembre 2023, che modifica la direttiva 2009/148/CE sulla protezione dei lavoratori contro i rischi connessi con un'esposizione all'amianto durante il lavoro (doc. web n. 10197110). Lo schema di decreto legislativo, volto a recepire la direttiva sulla protezione dei lavoratori contro i rischi connessi con un'esposizione all'amianto durante il lavoro (attraverso l'introduzione di limiti più stringenti, metodologie di analisi avanzate e misure preventive rafforzate), estende l'ambito di applicazione delle tutele a tutte le attività lavorative potenzialmente esposte al rischio-amianto, prevedendo misure più rigorose in materia di riduzione dell'esposizione, di sorveglianza sanitaria e di valutazione del rischio. In assenza di criticità del provvedimento dal punto di vista della protezione dei dati personali, anche in ragione della congruità del termine di conservazione della documentazione rispetto ai tempi di sviluppo delle patologie asbesto-correlate, il Garante ha espresso parere favorevole,

d) parere 25 settembre 2025, n. 569, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo recante individuazione delle autorità competenti di cui all'art. 31 del reg. (UE) 2023/1543 del Parlamento europeo e del Consiglio, del 12 luglio 2023, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali, nonché delle procedure per l'emissione, ricezione, esecuzione e riesame degli ordini europei di produzione e di conservazione (doc. web n. 10184519). Lo schema di decreto intende conformare l'ordinamento interno al regolamento (UE) 2023/1543 (cd. e-evidence), relativo all'acquisizione e alla gestione delle prove elettroniche nell'ambito dei procedimenti penali, adeguando i mezzi di prova e di ricerca della prova alla nuova realtà digitale e favorendo una più efficace cooperazione, a livello nazionale e transnazionale, tra le autorità di contrasto alla criminalità informatica e giudiziarie. L'art. 9, che modifica l'art. 132 del Codice, introduce, in coerenza con la disciplina UE e con la giurisprudenza della CGUE, la ricerca dei latitanti tra le finalità legittimanti l'acquisizione dei dati di traffico, limitatamente ai gravi reati già previsti dal Codice e, inoltre, introduce nel codice di procedura penale l'art. 263-*bis*, che regola l'ordine di conservazione "domestico", con possibilità di intervento urgente della polizia giudiziaria. In assenza di criticità, risultando le disposizioni coerenti con il quadro unionale, il Garante ha espresso parere favorevole, con l'osservazione relativa all'esigenza di integrare l'art. 263-*bis* c.p.p., specificando le

tipologie di dati oggetto dell'ordine di conservazione, per assicurare maggiore trasparenza ai sensi dell'art. 5, par. 1, lett. a), RGPD;

e) parere 25 settembre 2025 n. 525, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto attuativo e integrativo del d.lgs. n. 37/2021, in materia di rapporti di rappresentanza degli atleti e delle società sportive e di accesso ed esercizio della professione di agente sportivo (doc. web n. 10184268). Lo schema di decreto dà attuazione al d.lgs. 37/2021 nell'ambito della riforma dell'ordinamento sportivo prevista dalla l. n. 86/2019, con l'obiettivo di rendere più trasparente e regolata l'attività degli agenti sportivi. Determinante è l'istituzione del Registro nazionale unico degli agenti, articolato in sezioni dedicate a persone fisiche, società, agenti stabiliti e domiciliati, dotato peraltro di un'area destinata ad accogliere i contratti di mandato depositati presso le Federazioni. La gestione del Registro è affidata al CONI – designato titolare del trattamento –, tramite un sistema informatico centralizzato che consente sia la consultazione pubblica delle sezioni sia l'accesso del Dipartimento per lo sport.

Il Garante, pur non rilevando criticità sostanziali, ha suggerito alcune integrazioni tese a chiarire il rapporto tra i registri federali dei contratti e la sezione del Registro nazionale che li raccoglie, anche ai fini della titolarità del trattamento; a specificare quali dati siano effettivamente diffusi al pubblico e quali informazioni siano accessibili al Dipartimento per lo sport e per quali finalità. Ha, infine, suggerito l'introduzione di una disposizione tesa a definire tempi di conservazione dei dati e misure tecniche e organizzative del sistema informatico, così da garantire piena aderenza agli artt. 5 e 32 del Regolamento.

Infine, sono stati forniti elementi informativi alla Presidenza del Consiglio dei ministri in ordine alle esperienze in materia di AIR e VIR dell'Autorità, con riferimento all'anno 2025, in relazione a quanto previsto dall'art. 19, d.P.C.M. n. 169/2017 (nota 31 gennaio 2026).

3.1.3. I pareri sugli atti regolamentari o amministrativi generali

Il Garante ha altresì reso numerosi pareri su schemi di norme regolamentari suscettibili di incidere sulla protezione dei dati personali.

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

a) schema di decreto di novella del decreto del Ministro della giustizia 4 agosto 2023 n. 109, contenente il regolamento relativo all'individuazione di ulteriori categorie dell'albo dei consulenti tecnici di ufficio e dei settori di specializzazione di ciascuna categoria, ai requisiti per l'iscrizione all'albo e alla formazione, tenuta e aggiornamento dell'elenco nazionale di cui all'art. 24-*bis* delle disposizioni per l'attuazione del c.p.c. e disposizioni transitorie, ai sensi dell'art. 13, quarto comma, delle medesime disposizioni per l'attuazione, come aggiunto dall'art 4, comma 2, lett. a), d.lgs. n. 149/2022 (parere 13 novembre 2025, n. 663, doc. web n. 10196765);

b) schema di decreto del Ministro della giustizia, di concerto con il Ministro dell'economia e delle finanze e con il Ministro delle imprese e del made in Italy, recante regolamento, ai sensi dell'art. 67, comma 5-*bis* delle norme di attuazione, di coordinamento e transitorie del c.p.p., di cui al d.lgs. n. 271/1989, relativo all'individuazione delle ulteriori categorie in cui si suddivide l'albo dei periti presso il tribunale nonché ai settori di specializzazione di ciascuna categoria (parere 23 ottobre 2025, n. 624, doc. web n. 10197345);

c) schema di regolamento del Ministro della salute recante la procedura di sperimentazione delle disposizioni relative alla valutazione di base della condizione di disabilità di cui all'art. 33, commi 1 e 3, d.lgs. n. 62/2024 (parere 9 ottobre 2025, n. 578, doc. web n. 10189195);

d) schema di decreto del Ministro dell'economia e delle finanze, avente natura

regolamentare, volto a disciplinare il procedimento di accertamento, contestazione e irrogazione delle penali convenzionali, le modalità di partecipazione e del contraddittorio nell'ambito di tale procedimento, nonché a individuare i criteri e i dati per la definizione delle penali concretamente applicabili nei confronti dei concessionari di gioco inadempienti alle clausole delle convenzioni di concessione per la raccolta a distanza dei giochi pubblici e al rispetto dei livelli di servizio (art. 8, comma 3, d.lgs. n. 41/2024; oggi decreto del Ministro dell'economia e delle finanze 18 marzo 2025, n. 57; vedi parere 4 febbraio 2025, n. 58, doc. web n. 10114742);

e) schema di decreto del Ministro della giustizia, di concerto con il Ministro delle imprese e del made in Italy, di modifica al decreto del Ministro della giustizia 17 febbraio 2022, n. 27, recante regolamento in materia di disciplina dell'elenco pubblico delle organizzazioni e associazioni di cui agli artt. 840-*bis* del c.p.c. e 196-*ter* delle disposizioni per l'attuazione del c.p.c., come introdotti dalla l. n. 31/2019, recante disposizioni in materia di azione di classe (parere 30 gennaio 2025 n. 54, doc. web n. 10112347);

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

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

Si segnalano, in tal senso, i seguenti:

1) parere sulla proposta di legge della Provincia di Trento volta a modificare la l. provinciale 21 aprile 2017, n. 3, recante la struttura organizzativa del servizio sanitario provinciale (parere 9 ottobre 2025, n. 579, doc. web n. 10197070);

2) parere sullo schema di regolamento della Provincia autonoma di Trento di disciplina della costituzione e della gestione dell'elenco telematico degli operatori economici ai sensi dell'art. 19 della l. provinciale 9 marzo 2016, n. 2 (parere 23 giugno 2025, n. 376, doc. web n. 10160948);

3) parere sul disegno di legge regionale e conseguente regolamento attuativo, recanti la disciplina del trattamento dei dati personali per lo svolgimento delle attività istituzionali di competenza della Regione Friuli Venezia-Giulia in materia di sanità penitenziaria (parere 21 maggio 2025, n. 282, doc. web n. 10148604);

4) parere sulla proposta normativa volta a modificare la l. provinciale 13 gennaio 1992, n. 1, recante norme sull'esercizio delle funzioni in materia di igiene e sanità pubblica e medicina legale della Provincia di Bolzano (parere 29 aprile 2025, n. 240, doc. web n. 11141283);

5) parere sulla proposta di legge della Provincia autonoma di Trento volta a definire le modalità, la gestione delle informazioni raccolte nell'ambito del progetto di rifacimento della rete di monitoraggio del traffico (parere 10 aprile 2025, n. 198, doc. web n. 10141264);

6) parere sullo schema di regolamento recante le norme di funzionamento e la disciplina di trattamento dei dati personali relativi al registro grandi traumi della Regione Lombardia (parere 10 aprile 2025, n. 226, doc. web n. 10141363).

3.1.5. La consultazione del Garante sui provvedimenti regolamentari di altre istituzioni

Il Garante ha reso parere su di una proposta di modifica di alcuni commi dell'art. 17 del reg. interno per il funzionamento del Consiglio di presidenza della giustizia amministrativa (parere 29 aprile 2025, n. 241, doc. web n. 10141424).

3.1.6. Segnalazioni

Nel corso dell'anno è stata trasmessa una segnalazione al Parlamento e al Governo volta a evidenziare talune questioni rilevanti per la garanzia del diritto alla protezione

dei dati personali, inerenti all'effettività dei poteri (e degli stessi compiti di tutela) del Garante (note 11 settembre 2025).

Muovendo dalla nuova formulazione dell'art. 170 del Codice in ordine al regime di perseguibilità del delitto di inosservanza dei provvedimenti del Garante, si è evidenziato come la trasformazione della fattispecie in reato perseguibile a querela di parte, di dubbia compatibilità con la natura plurioffensiva della condotta (che incide non solo sul diritto alla protezione dei dati personali, ma anche sulla cogenza dei provvedimenti del Garante e, quindi, sull'effettività dei suoi poteri), possa affievolire l'effettività dei poteri dell'Autorità, affidata in buona parte all'efficacia general-preventiva della sanzione penale e alla comminatoria edittale della pena detentiva. È stata rappresentata, pertanto, la possibilità di ripristinare il regime di perseguibilità d'ufficio del reato, in coerenza con la natura plurioffensiva della fattispecie, al fine di assicurare l'effettività dei poteri del Garante.

Nel tentativo di rendere maggiormente incisiva l'azione di tutela del Garante, è stata poi sottolineata l'opportunità di ascrivere all'Autorità specifici poteri inibitori nei confronti delle piattaforme che offrano servizi digitali in violazione della disciplina in materia di protezione dei dati personali.

Sul paradigma di quanto già previsto, in particolare, per l'AGCOM (artt. 41, d.lgs. n. 208/2021 e 2 della l. n 93/2023, come modificato dall'art. 15-*ter*, c. 1, lett. a), d.l. n. 123/2023, convertito con modificazioni, dalla l. n. 159/2023), l'Autorità ha suggerito di attribuire al Garante il potere di inibire i servizi offerti da piattaforme, anche stabilite all'estero, che violino le norme in materia di protezione dati, ovvero di disabilitare l'accesso a contenuti diffusi in violazione della medesima disciplina, onde garantire la possibilità di un intervento diretto volto a contrastare, con la necessaria tempestività, il rischio di condivisione e dell'incontrollata divulgazione online di dati personali. L'assegnazione di poteri inibitori (comunque configurati) all'Autorità garantirebbe, infatti, la possibilità di intervenire, in maniera rapida ed efficace, contro la diffusione incontrollata di contenuti online (spesso pregiudizievoli e riguardanti minori), evitando al contempo il rischio di pregiudizi spesso irreversibili e irreparabili a danno dei soggetti più fragili.

3.1.7. Quesiti

Nell'anno di riferimento l'Autorità ha fornito riscontro interlocutorio a due quesiti, di analoga natura, volti a sollecitare una riflessione in merito all'opportunità di un intervento del Garante relativamente all'art. 473-*bis*.12, comma 3, lett. a) e c), c.p.c., introdotto dal d.lgs. n. 149/2022 (cd. riforma Cartabia), nella parte in cui richiede, nell'ambito dei procedimenti in materia di persone, minorenni e famiglie (ivi compresi quelli di separazione, scioglimento o cessazione degli effetti civili del matrimonio), l'allegazione al ricorso, per la presentazione di domande di contributo economico o in presenza di figli minori, delle "dichiarazioni dei redditi degli ultimi tre anni", nonché degli "estratti conto dei rapporti bancari e finanziari relativi agli ultimi tre anni".

Considerate le potenziali implicazioni che la questione sollevata riveste sotto il profilo della disciplina di protezione dei dati personali, l'Autorità ha provveduto a effettuare opportuni approfondimenti e ad avviare un confronto con il Ministero della giustizia.

II

LE ATTIVITÀ PER SETTORE

4 Le amministrazioni pubbliche

4.1. *L'attività fiscale, tributaria e doganale*

Come negli anni precedenti, nel corso del 2025 il Garante si è espresso in merito a schemi di decreto e di provvedimento del direttore dell'Agenzia delle entrate concernenti i trattamenti di dati personali da effettuarsi nell'ambito della cosiddetta dichiarazione dei redditi precompilata con specifico riguardo alle tipologie di dati raccolti, alla consultabilità degli stessi da parte dell'Agenzia delle entrate e alle modalità di accesso alla dichiarazione da parte degli interessati e degli altri soggetti autorizzati.

Dichiarazione dei redditi precompilata

In primo luogo, l'Autorità ha reso parere favorevole sullo schema di provvedimento del Direttore dell'Agenzia delle entrate recante accesso alla dichiarazione 730 precompilata da parte del contribuente e degli altri soggetti autorizzati a partire dall'anno di imposta 2024, nel quale è stato previsto, in via sperimentale, che l'Agenzia renda disponibile la dichiarazione precompilata anche del modello redditi persone fisiche, per i soggetti che aderiscono al regime di vantaggio o forfetario utilizzando i dati desumibili dalle fatture elettroniche (cd. dati fattura) e dai corrispettivi. A partire dalle operazioni effettuate dal 1° gennaio 2024, i predetti soggetti sono infatti obbligati ad emettere la fattura elettronica per le cessioni di beni e le prestazioni di servizi effettuate tra soggetti residenti o stabiliti nel territorio dello Stato e non viene più rilasciata agli stessi una certificazione unica (CUA) in relazione ai compensi loro erogati. Per poter quindi proseguire la sperimentazione prevista dall'art. 1, comma 1-*bis,* d.lgs. n. 175/2014 ed elaborare la dichiarazione dei redditi precompilata per i soggetti IVA in regime di vantaggio e forfetario, considerato che la stessa norma prevede che possano essere adoperate per la precompilazione anche le informazioni presenti in Anagrafe tributaria, è stata prevista l'utilizzabilità delle informazioni reddituali tratte dai dati delle fatture e dai dati dei corrispettivi giornalieri inviati nel 2024 dai soggetti in questione.

Inoltre, relativamente all'accesso alla dichiarazione precompilata per il tramite di altri intermediari, nel dare attuazione alle disposizioni contenute nell'art. 2, comma 4, d.lgs. n. 108/2024 è stato disposto che la dichiarazione precompilata (limitatamente al modello redditi persone fisiche) sia resa disponibile, conferendo apposita delega, anche tramite uno degli altri soggetti incaricati della trasmissione telematica delle dichiarazioni, di cui all'art. 3, comma 3, d.P.R. n. 322/1998.

Considerato che nello schema di provvedimento esaminato dal Garante sono state confermate per il resto le misure individuate negli anni passati, anche sulla base delle indicazioni dell'Autorità, lo schema in questione è stato ritenuto conforme al RGPD e al Codice (provv. 10 aprile 2025, n. 199, doc. web n. 10144092).

L'Autorità si è espressa favorevolmente su uno schema di provvedimento del Direttore dell'Agenzia delle entrate recante la disciplina delle modalità tecniche di utilizzo, da parte dei propri operatori, dei dati delle spese sanitarie e veterinarie messe a disposizione dal Sistema TS, ai fini dell'elaborazione della dichiarazione dei redditi precompilata, a decorrere dall'anno di imposta 2024. Lo schema, elaborato sulla base delle recenti modifiche normative di settore, ha tenuto conto delle indicazioni fornite dall'Autorità nelle interlocuzioni informali intercorse volte ad assicurare, in particolare, il rispetto dei principi di liceità, correttezza e trasparenza, di minimizzazione dei dati e di integrità e

riservatezza, nonché dei principi di *privacy by design* e *by default* e di sicurezza del trattamento, limitando l'accesso ai dati di dettaglio relativi alle spese sanitarie. In particolare, lo schema in parola ha circoscritto l'accesso alle informazioni di dettaglio relative alle spese sanitarie ai casi di rettifica (operata direttamente dal contribuente) rispetto ai dati precompilati, anche mediante la compilazione semplificata, o per il tramite del sostituto d'imposta intermediari, limitatamente alle dichiarazioni selezionate in via centralizzata per il controllo formale di cui all'art. 36-*ter*, d.P.R. n. 600/1973, da parte dei soli dipendenti incardinati nell'ufficio territorialmente competente. È stata, altresì, prolungata la conservazione dei log di tutte le operazioni di trattamento sui dati sanitari effettuate dall'Agenzia delle entrate, nonché delle operazioni di consultazione effettuate dal contribuente, nell'ambito del Sistema TS (provv. 13 febbraio 2025, n. 62, doc. web n. 10112254).

Sistema TS

A tal proposito, l'Autorità ha reso parere favorevole anche sul relativo schema di decreto del MEF, con il quale sono state disciplinate le modalità con cui, ai fini dei predetti controlli formali, il Sistema TS mette a disposizione dell'Agenzia delle entrate il servizio di consultazione dei dati di spesa sanitaria e veterinaria e quello di consultazione dei dati risultanti a fronte di rettifica o integrazione da parte del contribuente nell'ambito della compilazione semplificata. Anche in questo caso, è stato mantenuto inalterato il quadro di garanzie già previsto in relazione ai trattamenti ivi disciplinati, prevedendo, in particolare, il tracciamento dell'operatore autorizzato dell'Agenzia delle entrate e un adeguato periodo di conservazione dei log di tracciamento (provv. 21 maggio 2025, n. 285, doc. web n. 10141339).

L'Autorità si è inoltre espressa favorevolmente sullo schema di provvedimento del Direttore dell'Agenzia delle entrate, attuativo del relativo decreto del Viceministro dell'economia e delle finanze 21 gennaio 2025 (sul quale il Garante aveva già reso parere favorevole con provv. 12 dicembre 2024, n. 764, doc. web n. 10097432), concernente le modalità tecniche di comunicazione alla Anagrafe tributaria, da parte del Gestore dei servizi energetici S.p.A., 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. 16 gennaio 2025, n. 1, doc. web n. 10110419).

Provvedimenti correttivi

Il Garante ha adottato un provvedimento di ammonimento nei confronti dell'Agenzia delle entrate-Riscossione, a seguito di una segnalazione con la quale era stata lamentata l'illecita comunicazione, senza il necessario oscuramento, dei dati dei destinatari degli avvisi di deposito nella casa comunale di atti notificati ai sensi degli artt. 26, ultimo comma, d.P.R. n. 602/1973, 60 del d.P.R. n. 600/1973 e 140 c.p.c., al fine di evadere una istanza di accesso agli atti da questi avanzata. All'esito dell'attività istruttoria, è stato accertato che il predetto trattamento era stato effettuato dall'Agenzia delle entrate-Riscossione in violazione dei principi di liceità, correttezza e minimizzazione di cui all'art. 5, par. 1, lett. a) e c) e 6, par. 1, lett. e), RGPD, nonché dell'art. 2-*ter* del Codice. Il Garante ha tuttavia considerato che i predetti atti erano già stati oggetto di pubblicazione sull'albo pretorio comunale ed erano stati trasmessi ad un solo soggetto e la violazione, causata dall'errore materiale di un operatore autorizzato, aveva avuto natura episodica (provv. 29 aprile 2025, n. 242, doc. web n. 10162312).

Sistema informatico doganale - CIS

Nell'ambito delle attività di controllo e assistenza attribuite al Garante con riguardo al trattamento dei dati personali contenuti nel *Customs Information System* (CIS) – quale sistema informativo istituito allo scopo di facilitare l'azione di prevenzione, indagine e repressione di condotte illecite, che violano disposizioni doganali o agricole unionali – è stata assicurata la partecipazione alle riunioni previste in seno al *Customs Information*

System Supervision Coordination Group (CIS SCG), di cui il Garante è membro, e alle connesse attività istituzionali (cfr. artt. 37 del reg. (CE) n. 515/1997; 24 della decisione 2009/917/GAI; 154, comma 2, lett. c), del Codice). In particolare, in tale quadro sono state avviate specifiche interlocuzioni con l'Agenzia delle dogane e dei monopoli e con la Guardia di finanza al fine di procedere all'aggiornamento della guida, liberamente consultabile da chiunque sul sito web del Garante europeo della protezione dei dati, intesa ad agevolare l'esercizio dei diritti di accesso, rettifica e cancellazione in tale specifico ambito (artt. 15, 16 e 17 del RGPD).

4.2. *Previdenza, assistenza e altri benefici*

Anche nel 2025 il Garante è intervenuto con pareri nell'ambito delle politiche sociali e di sostegno, con particolare riferimento a fattispecie relative al riconoscimento di misure di supporto economico in favore di soggetti in condizioni di difficoltà.

Bonus rifiuti

In tema di benefici economici, il Garante è stato consultato sullo schema di delibera dell'ARERA concernente il riconoscimento del bonus sociale rifiuti agli utenti domestici del servizio di gestione integrata dei rifiuti urbani in condizioni economico sociali disagiate, in attuazione dell'art. 57-*bis*, d.l. n. 124/2019, e, conseguentemente, del d.P.C.M. 21 gennaio 2025, n. 24. La delibera di ARERA ha tenuto conto delle indicazioni fornite, soprattutto per quanto concerne l'individuazione dei ruoli assunti dai diversi soggetti coinvolti (INPS, ARERA, Cassa per i servizi energetici e ambientali ed enti erogatori, nonché Acquirente Unico S.p.A. e ANCI in qualità di fornitori dei sistemi tecnologici utilizzati al riguardo) e la definizione dei flussi nei casi di utenze TARI agevolabili intestate a minorenni, al fine di assicurare il rispetto del principio di minimizzazione dei dati. Pertanto, anche in considerazione del fatto che il meccanismo di individuazione della platea dei beneficiari del bonus rifiuti era stato configurato, per quanto compatibile, in linea con quanto già espresso dal Garante con riferimento ai bonus sociali elettrico, gas e idrico (provv. 17 dicembre 2020, n. 279, doc. web n. 9510819), è stato rilasciato parere favorevole (provv. 17 luglio 2025, n. 420, doc. web n. 10168366).

Bonus elettrodomestici

Parere positivo è stato rilasciato dal Garante anche sullo schema di decreto direttoriale del Ministero delle imprese e del made in Italy (MIMIT) in merito al contributo per l'acquisto di elettrodomestici ad elevata efficienza energetica, prodotti in uno stabilimento collocato nel territorio dell'Unione europea, con corrispondente smaltimento dell'elettrodomestico sostituito di classe energetica inferiore a quella dell'elettrodomestico di nuovo acquisto, in attuazione dell'art. 1, commi 107 e ss., l. n. 207/2024, e del decreto del MIMIT, di concerto con il Ministro dell'economia e delle finanze, 3 settembre 2025 (su cui tuttavia l'Autorità non era stata formalmente consultata). Lo schema di decreto direttoriale in esame era stato redatto tenendo conto delle osservazioni formulate nell'ambito delle interlocuzioni informali intercorse, che avevano riguardato, in particolare, il corretto riferimento alle nozioni di nucleo familiare e di famiglia anagrafica in relazione all'esatta individuazione degli interessati coinvolti nel trattamento in esame e l'individuazione delle tipologie di dati personali trattati in ogni fase del trattamento, in relazione sia all'acquisizione dei dati per verificare il possesso dei requisiti ISEE che alle attività di monitoraggio sull'erogazione del beneficio da parte del MIMIT. Inoltre, con riferimento alle modalità e ai termini di comunicazione all'Agenzia delle entrate dei dati relativi ai rimborsi ottenuti dai beneficiari, erano state introdotte misure atte ad assicurare uniformità con la disciplina prevista in materia di dichiarazione dei redditi precompilata. Nel rendere il parere (provv. 25 settembre 2025, n. 527, doc. web n.

10184562), si è tenuto conto del fatto che, nel caso di specie, per l'erogazione del bonus elettrodomestici ci si era avvalsi della piattaforma informatica di cui all'art. 28-*bis*, d.l. n. 152/2021, gestita da PagoPA S.p.A. e disciplinata dal decreto del Ministro per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministro dell'economia e delle finanze, 6 ottobre 2022, su cui il Garante aveva già fornito un parere (provv. 28 luglio 2022, n. 286, doc. web n. 9809029) con indicazioni circa le misure necessarie ad assicurare la conformità al RGPD e al Codice.

Provvedimenti correttivi

L'Autorità ha adottato un provvedimento correttivo nei confronti di un patronato che aveva conservato i dati personali della reclamante (acquisiti diversi anni prima, quando la stessa aveva richiesto al medesimo una prestazione consulenziale) per un arco temporale superiore a quello di cinque anni previsto dalla disciplina di settore per il mandato che ne giustificava il trattamento (cfr., in particolare, artt. 11, comma 3, e 16, comma 1, lett. e), del decreto del Ministero del lavoro e delle politiche sociali n. 193/2008). Grazie a tali dati, un operatore del patronato aveva poi effettuato un accesso alle banche dati dell'INPS, per accertare quanto richiesto dalla reclamante in passato ma senza aver avuto un nuovo specifico mandato, e, quindi, in maniera non conforme ai principi di liceità, correttezza e trasparenza e limitazione della conservazione, nonché in assenza di un idoneo presupposto normativo, in violazione degli artt. 5, par. 1, lett. a) ed e) e 6 del RGPD e degli artt. 2-*ter* e 116, comma 1, del Codice (provv. 10 aprile 2025, n. 200, doc. web n. 10140301).

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

Anche nel 2025 il Garante ha interagito con il Ministero dell'istruzione e del merito (MIM) 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.

IA nelle istituzioni scolastiche

In tale ambito, ha espresso parere favorevole, ai sensi degli artt. 36, par. 4, e 58, par. 3, lett. b), RGPD, sullo schema di decreto ministeriale del MIM concernente l'implementazione di un servizio digitale in materia di IA nell'ambito della piattaforma unica di cui all'art. 21, commi 4-*ter* e seguenti, d.l. n. 75/2023, convertito, con modificazioni, dalla l. n. 112/2023 nonché sulle linee guida per l'introduzione dell'IA nelle istituzioni scolastiche ad esso allegate (provv. 4 agosto 2025, n. 454, doc. web n. 10162698). Lo schema di decreto ha stabilito che, nell'ambito della piattaforma unica, è implementato un servizio digitale, le cui modalità di accesso sono indicate nello stesso schema, mediante il quale il MIM rende disponibili specifici documenti informativi sull'IA, tra i quali apposite linee guida e una mappa delle sperimentazioni avviate dalle singole istituzioni scolastiche, al fine di supportare le scuole, gli studenti e gli esercenti la responsabilità genitoriale all'acquisizione delle necessarie conoscenze digitali. Le linee guida hanno in particolare previsto gli obiettivi perseguiti, la valorizzazione della centralità della persona, la tutela dei diritti e delle libertà fondamentali, la sicurezza dei sistemi e modelli di IA nonché i requisiti etici, tecnici e normativi necessari per assicurare un'adozione responsabile e sicura delle tecnologie di IA e le istruzioni operative.

Lo schema di decreto ha tenuto conto delle osservazioni fornite nel corso delle interlocuzioni informali con specifico riguardo ai divieti concernenti le pratiche di cui all'art. 5 del reg. sull'IA (come quelle preordinate al riconoscimento delle emozioni), al rispetto delle misure regolamentari in relazione all'impiego di sistemi ad alto rischio, al rafforzamento delle garanzie di trasparenza nei confronti degli interessati, alla definizione di ruoli e responsabilità dei soggetti istituzionali coinvolti, anche in qualità di titolari

del trattamento ai fini della contestuale applicazione della disciplina di protezione dei dati personali. Quanto a quest'ultima, si è fatto particolare riferimento alla necessità di utilizzare i dati personali riferibili a studenti e docenti laddove strettamente indispensabili, ricorrendo ove possibile all'utilizzo di dati sintetici e prevedendo l'impiego di configurazioni che impediscano la conservazione dei *prompt*, la profilazione o il tracciamento degli studenti, nel rispetto del principio di minimizzazione dei dati. Lo schema di decreto ha inoltre previsto una attività formativa adeguata, audit o valutazioni periodiche volti a verificare l'affidabilità, la trasparenza e la correttezza del funzionamento dei sistemi utilizzati.

Nell'esprimere il parere, l'Autorità ha in particolare rilevato che spetta ai soggetti che svolgono attività di trattamento dei dati personali, nel rispetto della cornice di liceità sopra richiamata, adottare le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi per gli interessati connessi al delicato contesto scolastico ed educativo, previa valutazione d'impatto svolta anche alla luce delle valutazioni formulate dai soggetti a vario titolo coinvolti, in ossequio al principio di *accountability*.

Curriculum della studentessa e dello studente

Il Garante ha espresso, inoltre, parere favorevole sullo schema di decreto del MIM attuativo dell'art. 1, comma 4, d.l. 9 settembre 2025 n. 127 e dell'art. 11, comma 4, d.m. n. 192/2023, concernente l'implementazione del modello di curriculum della studentessa e dello studente. Tale schema di decreto ha introdotto le disposizioni volte a modificare e implementare il modello di curriculum adottato con d.m. n. 88/2020, integrandolo con un'ulteriore sezione nella quale sono descritti i livelli di apprendimento conseguiti nelle prove scritte a carattere nazionale e la certificazione sulle abilità di comprensione e uso della lingua inglese; inoltre ha stabilito che il curriculum sia associato, tramite un numero identificativo, al diploma e possa essere acquisito, attraverso una scelta informata degli studenti, separatamente dal diploma; infine, che esso si compone complessivamente di quattro parti (numerate da I a IV), delle quali la Parte IV riporta, in particolare, la descrizione dei livelli di apprendimento conseguiti nelle prove scritte a carattere nazionale di cui all'art. 19 del d.lgs. n. 62/2017 a cura dell'Istituto nazionale per la valutazione del sistema educativo di istruzione e di formazione (INVALSI).

Lo schema prevede, altresì, che l'alimentazione del curriculum avvenga in fasi distinte: nel corso dell'anno scolastico, con compilazione a cura degli studenti della Parte III; a seguito dello scrutinio finale, con riferimento alle Parti I, II, III; all'esito dell'esame di maturità, con riferimento alla Parte IV, da parte dell'INVALSI. Inoltre, il curriculum comprensivo delle sole Parti I, II e III è messo a disposizione delle commissioni prima dello svolgimento dell'esame di maturità e, a seguito dell'emissione del diploma conclusivo, viene messo a disposizione degli studenti diplomati, nella sua versione definitiva, all'interno del servizio digitale *E-portfolio* della piattaforma unica.

In base a quanto previsto nello schema, gli studenti diplomati possono, attraverso una scelta informata, acquisire il proprio curriculum nella versione integrale o scaricando solo determinate sezioni del documento. Lo schema disciplina l'adozione nella piattaforma di misure (es. informative, *alert*) idonee ad aumentare il grado di consapevolezza degli studenti interessati circa il trattamento dei propri dati personali, l'individuazione dei soggetti coinvolti nel trattamento dei dati personali nonché il rispetto dei principi in materia di protezione dei dati personali e le misure di sicurezza. Il Ministero, su suggerimento del Garante, ha previsto, nello schema di decreto, in particolare, che il curriculum non costituisce parte integrante del diploma cosicché la sua allegazione è a discrezione dello studente, che ha la facoltà di allegarlo nella versione integrale o nelle singole parti che lo costituiscono inclusa la facoltà di acquisire o meno la Parte IV del curriculum, riguardante le prove nazionali INVALSI.

A tale ultimo riguardo, nell'esprimere il parere, l'Autorità ha rilevato la necessità che i trattamenti di dati personali effettuati in tale ambito siano conformi ai principi di liceità, correttezza e trasparenza e di limitazione della finalità, tenendo conto che le prove INVALSI non perseguono uno scopo valutativo dei singoli studenti, ma sono finalizzate a valutare la qualità complessiva dell'offerta formativa delle istituzioni scolastiche in un'ottica di progressivo miglioramento dell'efficacia dell'azione didattica in generale (cfr. art. 3, l. n. 53/2003) (provv. 18 dicembre 2025, n. 747, doc. web n. 10209920).

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

Il Garante è intervenuto nei confronti di alcune scuole in relazione alla illecita diffusione e/o comunicazione di convocazioni relative alle riunioni del Gruppo di lavoro operativo per l'inclusione scolastica (GLO), irrogando, in relazione ad una specifica fattispecie, una sanzione amministrativa pecuniaria e censurando gli istituti scolastici con un ammonimento nei restanti casi. In un caso, una circolare relativa alle convocazioni del GLO, riferita a più alunni, era stata pubblicata sul sito web istituzionale della scuola. In un altro caso l'istituto scolastico aveva inviato, in due diverse occasioni, la convocazione del richiamato Gruppo di lavoro − contenente l'indicazione del nominativo dell'alunno per il quale il GLO era stato organizzato − all'indirizzo di un soggetto estraneo alla comunità scolastica. In un ulteriore caso tale convocazione, riferita ad un alunno, era stata resa accessibile sulla bacheca del registro elettronico a tutti i genitori degli alunni di una classe, insieme al riferimento del piano educativo individualizzato (PEI) previsto per l'alunno stesso. In tali occasioni il Garante ha prioritariamente ricordato che i minori, in quanto "persone fisiche vulnerabili" meritano una specifica protezione relativamente ai loro dati personali, in quanto potenzialmente poco consapevoli dei rischi e dei diritti in materia di protezione dei dati personali. L'Autorità ha poi chiarito che, considerata la definizione di dato personale e di dato relativo alla salute (art. 4, punti 1 e 15, del RGPD), la convocazione di una riunione del GLO, e, in un caso, il riferimento esplicito al PEI, previsti dalla normativa di settore in materia di disabilità, costituiscono informazioni relative allo stato di salute degli alunni e in quanto tali 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 (provv.ti 10 luglio 2025, n. 385, doc. web n. 10162203; 27 febbraio 2025, n. 117, doc. web n. 10118264; 10 aprile 2025, n. 203, doc. web n. 10144156).

Un'altra istruttoria ha riguardato la messa a disposizione ad opera di una docente, nella sezione del registro elettronico accessibile a tutti i genitori di una classe, del Piano educativo individualizzato riguardante i ragazzi con disabilità (PEI) elaborato per il figlio dei reclamanti. In sede istruttoria è inoltre emerso che l'immagine/screenshot dell'avviso di visibilità del PEI sul registro elettronico era stata resa disponibile da un genitore sulla chat di classe. Con riguardo al profilo relativo alla messa a disposizione sulla chat di classe del richiamato documento, il Garante ha rappresentato che la creazione, da parte di alunni, genitori o rappresentanti di classe, di chat di cui fanno parte i genitori degli studenti e l'utilizzo di tali strumenti come canali di comunicazione di notizie riguardanti i diversi aspetti della vita scolastica, non risulta riconducibile alle attività istituzionali o didattiche dell'istituto scolastico come titolare del trattamento ma ad autonomi comportamenti posti in essere da privati, dei quali la scuola non è tenuta a rispondere. Con riguardo al diverso profilo relativo alla messa a disposizione del PEI sul

registro elettronico da parte dell'istituto scolastico, il Garante ha evidenziato che il PEI è il documento nel quale vengono descritti gli interventi integrati ed equilibrati tra di loro, predisposti per l'alunno in situazione di handicap, in un determinato periodo di tempo, ai fini della realizzazione del diritto all'educazione e all'istruzione (cfr. art. 5, comma 1, d.P.R. 24 febbraio 1994) e comprende una pluralità di informazioni relative alla condizione di disabilità dell'alunno per il quale tale documento è predisposto tra cui un'apposita sezione dedicata ai dati relativi alla diagnosi funzionale. Tale documento, elaborato e approvato dal GLO, contiene informazioni che, come già ricordato, possono essere fornite 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. Considerato che l'evento si era verificato per un mero errore materiale, che il documento era stato visibile sul registro elettronico per un breve lasso temporale e che non era stato provato che i genitori avessero effettivamente preso visione del contenuto del PEI, il Garante si è limitato a censurare la scuola con un ammonimento per la violazione degli artt. artt. 5, par. 1, lett. a), 6 e 9 del RGPD nonché dell'art. 2-*ter* e 2-*sexies* del Codice (provv. 27 febbraio 2025, n. 115, doc. web n. 10126123).

La comunicazione illecita di dati relativi alla salute è stata oggetto anche di due provvedimenti sanzionatori tra loro collegati, comminati dal Garante nei confronti di un comune e di una cooperativa sociale. Quest'ultima, in vista di uno sciopero, aveva inviato a un comune e ai responsabili di unità territoriali una e-mail recante in allegato alcuni file in formato excel contenenti l'elenco dei servizi integrativi non garantiti per effetto dello sciopero, distinti per scuola, che riportavano anche dati personali molto delicati relativi alla salute dei bambini iscritti a talune scuole dell'infanzia, quali le tipologie di disabilità, le specifiche patologie sofferte, talune certificazioni possedute e l'attribuzione agli stessi di risorse per l'integrazione scolastica. La medesima e-mail era stata successivamente inoltrata da un ufficio del comune a numerose scuole dell'infanzia comunali, ai responsabili di unità territoriali e a taluni coordinatori pedagogici; in un secondo momento, una collaboratrice scolastica di una delle scuole dell'infanzia comunale, che aveva ricevuto la predetta e-mail, aveva inoltrato uno dei file allegati alla stessa, contenente i richiamati dati personali, a cinquantatré indirizzi di posta elettronica intestati ai genitori dei bambini iscritti a tale scuola. Il Garante in entrambi i casi ha ricordato che, considerata la definizione di dato personale e di dato relativo alla salute (art. 4, punti 1 e 15, RGPD), le informazioni relative alle tipologie di disabilità, l'indicazione del codice di classificazione delle stesse e delle certificazioni possedute o meno dai bambini nonché l'attribuzione agli allievi di risorse per l'integrazione scolastica (insegnati/educatori), consentono di ricavare informazioni sullo stato di salute dei minori riportati negli elenchi. Nel comminare la sanzione amministrativa pecuniaria al comune, il Garante ha chiarito che i predetti soggetti coinvolti nella vicenda di cui trattasi e destinatari delle predette informazioni, in virtù del ruolo da essi ricoperto e delle funzioni svolte, potevano trattare i dati personali degli alunni nell'ambito delle attività educative e di istruzione di loro competenza; tuttavia, essi non erano legittimati a trattare, come nel caso di specie, i dati personali, anche relativi allo stato di salute di particolare dettaglio e delicatezza, di minori iscritti a scuole diverse da quelle di propria competenza. Con riferimento all'invio da parte della scuola dell'infanzia del file contenente i sopra citati dati personali agli indirizzi di posta elettronica di circa cinquanta genitori di alunni della scuola, il Garante ha rappresentato che tali dati erano stati resi conoscibili, ancorché per un errore materiale, in favore di un novero determinato o determinabile di soggetti terzi (art. 4, par. 1 n. 10, RGPD), cosicché si era configurata una comunicazione illecita di numerosi dati personali, anche relativi alla salute degli

interessati, soggetti minori di età e, in quanto tali, comunque particolarmente vulnerabili (provv. 29 aprile 2025, n. 273, doc. web n. 10146543). Nel comminare la sanzione amministrativa pecuniaria nei confronti della cooperativa, il Garante ha evidenziato che questa, nell'inviare la documentazione contenente le richiamate informazioni, ultronee rispetto alle finalità perseguite di mera comunicazione delle possibili riduzioni dei servizi integrativi nella giornata di sciopero, non aveva utilizzato la perizia necessaria né aveva adottato misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento e aveva agito in violazione delle istruzioni fornite dal titolare del trattamento, ai sensi dell'art. 28 del RGPD (provv. 29 aprile 2025, n. 274, doc. web n. 10146337).

In altro caso il Garante ha censurato, con una sanzione amministrativa pecuniaria, il comportamento di una scuola che aveva inviato, dall'indirizzo di posta elettronica istituzionale, una e-mail riguardante gli adempimenti vaccinali relativi a taluni alunni a circa trentasette interessati, lasciando in chiaro gli indirizzi e-mail dei diversi destinatari del messaggio. In tale ambito 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 e che risulta necessario mantenere riservati, magari utilizzando apposite funzionalità (cfr. punto 5 delle linee guida in materia di attività promozionale e contrasto allo spam 4 luglio 2013, n. 330, doc. web n. 2542348). Inoltre, l'Autorità ha chiarito che, considerata la definizione di dato personale e di dato relativo alla salute, il riferimento agli adempimenti vaccinali di cui alla l. n. 119/2017, rappresentava di per sé un'informazione relativa allo stato di salute degli alunni a cui tale informazione era riferita; pertanto inviando tale e-mail, la scuola aveva messo a conoscenza i destinatari della predetta comunicazione, oltre che dell'indirizzo di posta elettronica degli altri destinatari dell'e-mail, anche del fatto che i figli di questi ultimi non erano in regola con gli adempimenti vaccinali, dando luogo a una comunicazione di dati personali e di categorie particolari di dati personali, in violazione degli artt. 5, par. 1, lett. a), 6, parr. 1, lett. c) ed e), 2, 3 e 9, parr. 1, 2, lett. g) e 4 del RGPD e 2-*ter*, commi 1 e 3, e 2-*sexies*, commi 1 e 2, lett. bb), del Codice (provv. 4 dicembre 2025, n. 732, doc. web n. 10209089).

In diverse occasioni il Garante si è occupato della pubblicazione sul sito web istituzionale, o in piattaforme usate in ambito scolastico di dati personali relativi a specifici alunni. In un caso due genitori avevano reclamato l'avvenuta pubblicazione sul sito web istituzionale di una scuola di una circolare relativa alla convocazione di un consiglio di classe straordinario riguardante un procedimento disciplinare nei confronti del figlio. Tale circolare, pur non riportando l'indicazione del nominativo dell'interessato all'interno del documento, recava il cognome dell'alunno nella denominazione del documento consultabile online (provv. 23 ottobre 2025, n. 626, doc. web n. 10195414).

In altri due casi erano stati resi disponibili, su una piattaforma, a tutti i genitori degli alunni di una classe, alcuni messaggi con i quali si richiedevano ai genitori colloqui urgenti riguardanti tre alunni indicati nominativamente (provv. 9 ottobre 2025, n. 583, doc. web n. 10192761) e una nota contenente informazioni riguardanti le vicende personali e familiari di un alunno (provv. 25 settembre 2025, n. 529, doc. web n. 10184924). Un ulteriore caso ha riguardato la messa a disposizione, nell'area pubblica di una piattaforma, accessibile a genitori, insegnanti e personale amministrativo della scuola, di due messaggi indirizzati alla reclamante, contenenti informazioni personali relative al figlio (provv. 27 marzo 2025, n. 169, doc. web n. 10136982). In tutti i menzionati casi il Garante, dopo aver ricordato la definizione di titolare del trattamento (art. 4 par. 1, n. 7, RGPD) e la sua responsabilità − anche quando una violazione del RGPD si sia verificata per negligenza o inadempimento di un autorizzato e la specifica

protezione prevista per i minori, in considerazione della loro particolare "vulnerabilità" (cfr. cons. 38 del RGPD) – ha ribadito la necessità di un bilanciamento tra il diritto-dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica e la tutela della personalità dei minori; nel caso specifico, ciò si traduce nell'evitare l'inserimento, nelle circolari e nelle comunicazioni scolastiche non rivolte a specifici destinatari, di dati personali che rendano identificabili, ad esempio, gli alunni coinvolti in casi di bullismo o destinatari di provvedimenti disciplinari (cfr. "La scuola a prova di privacy - Vademecum" ed. 2025, doc. web n. 9886884, vedi anche le FAQ "Scuola e privacy - Domande più frequenti", in particolare la FAQ n. 7).

Nel primo caso, avendo la scuola dato luogo ad una diffusione di dati personali in violazione degli artt. 5, par. 1, lett. a) e 6, parr. 1, lett. c) ed e), 2 e 3 del RGPD e 2-*ter*, commi 1 e 3, del Codice e non avendo provveduto a nominare, per un certo periodo di tempo, il RPD e a comunicarne all'Autorità i dati di contatto, in violazione dell'art. 37, par. 1 e 7 del RGPD, il Garante ha comminato un provvedimento sanzionatorio, anche in ragione delle carenze individuate nelle informative sul trattamento fornite agli interessati ai sensi dell'art. 13 del RGPD.

Nei restanti casi, avendo le scuole dato luogo, in assenza di idoneo presupposto di liceità, a una comunicazione illecita di dati personali a terzi, il Garante ha stabilito di censurarne la condotta con un ammonimento in relazione alla violazione degli artt. 5, par. 1, lett. a) e 6, parr. 1, lett. c) ed e), 2 e 3 del RGPD e 2-*ter*, commi 1 e 3, del Codice.

Il Garante ha comminato una sanzione amministrava anche nei confronti di un istituto scolastico che aveva pubblicato, sul proprio canale YouTube, un video di auguri di Natale nel quale apparivano alcuni studenti. Il Garante ha evidenziato che la pubblicazione del predetto video aveva determinato una diffusione dei dati personali in assenza di un idoneo presupposto di liceità, non rientrando tale trattamento tra le finalità di interesse pubblico attribuite all'istituto e non sussistendo alcuna altra condizione di liceità. Con riferimento al consenso come presupposto di liceità del trattamento, il Garante pur non ritenendolo applicabile quale base giuridica nel caso di specie, ha chiarito che, in linea generale, il consenso deve essere espresso da un alunno maggiorenne o da un soggetto esercente la responsabilità genitoriale dell'alunno minorenne. Nel caso in esame, inoltre, il modulo di iscrizione all'istituto, nella sezione "Autorizzazione trattamento dell'immagine", faceva riferimento alla eventuale pubblicazione di foto o video sul sito istituzionale effettuata esclusivamente nell'esercizio delle funzioni istituzionali e non alla pubblicazione di video, come quello in esame, sul canale YouTube. Nel modulo utilizzato dalla scuola, inoltre, non era presente un campo/*flag* attraverso il quale esprimere esplicitamente il consenso al trattamento di immagini e/o video, difformemente da quanto previsto dall'art. 7, par. 2, RGPD. Al riguardo, anche le linee guida 5/2020 sul consenso ai sensi del RGPD, adottate il 4 maggio 2020, prevedono che "il titolare del trattamento deve evitare ambiguità e garantire che l'azione con cui viene espresso il consenso possa essere distinta da altre azioni" (par. 84) e che "se spetta al genitore prestare il consenso, può essere necessario fornire un insieme di informazioni che consentano agli adulti di prendere una decisione informata" (par. 126) (provv. 13 marzo 2025, n. 134, doc. web n. 10127792).

La questione della pubblicazione di video ritraenti studenti è stata oggetto anche di un'altra istruttoria, all'esito della quale il Garante ha censurato con una sanzione amministrativa pecuniaria la condotta di un istituto scolastico che aveva incaricato un influencer di effettuare, all'interno della scuola stessa, un breve video promozionale. In sede istruttoria era emerso che il video, contenente immagini ritraenti un'alunna, di spalle, intenta a suonare il pianoforte, era stato pubblicato sui profili social dell'influencer (Instagram, Facebook, TikTok, ecc.) e che la scuola non aveva provveduto a designare

quest'ultimo responsabile del trattamento ai sensi dell'art. 28 del RGPD. Il Garante dopo aver richiamato la definizione di dato personale, ha chiarito che la diffusione di immagini di persone fisiche, anche nel caso in cui il cui volto non sia visibile, può, in taluni casi, consentire l'identificazione delle stesse e che l'istituto aveva dato luogo ad una diffusione dei dati personali in assenza di un idoneo presupposto di liceità. Il Garante ha inoltre rappresentato che l'informativa fornita ai genitori dell'interessata aveva contemplato la pubblicazione eventuale di foto o video nell'ambito di viaggi d'istruzione e/o per finalità didattica e non aveva incluso alcun riferimento al trattamento riguardante la pubblicazione su profili social, oltretutto non riconducibili all'istituto scolastico, e che di conseguenza il consenso fornito, in ogni caso, non era stato conforme ai requisiti contemplati dal RGPD in termini di trasparenza e inequivocabilità. Il Garante ha, infine, evidenziato che il potere-dovere dei genitori di prestare o negare il consenso al trattamento dei dati personali dei minori incontra il limite del perseguimento del superiore interesse del minore medesimo, interesse certamente incompatibile con la pubblicazione del video per asserite finalità promozionali (provv. 27 novembre 2025, n. 725, doc. web n. 10211243).

Un'altra istruttoria avviata a seguito di un reclamo aveva evidenziato che un asilo aveva pubblicato sul sito istituzionale, e sul profilo di Google Maps, numerose immagini di minori in diversi momenti e fasi della giornata, anche in contesti particolarmente delicati (sonno, mensa, utilizzo dei servizi igienici, cambio pannolino, massaggi infantili). Il Garante, nel ricordare che la normativa in materia di protezione dei dati personali non prevede un diverso regime applicabile in ambito educativo ai soggetti pubblici e a quelli privati, ma tiene conto del solo profilo funzionale nel trattamento dei dati riguardante il perseguimento di un interesse pubblico sotteso, rappresentato nel caso di specie, dall'offerta di servizi educativi, ha evidenziato che la pubblicazione sul sito web istituzionale dell'asilo di numerosissime immagini di minori si poneva in contrasto non solo con la disciplina in materia di protezione dei dati personali, ma più radicalmente con l'assetto, anche a livello costituzionale, dei diritti fondamentali della persona. Il Garante, inoltre, nel rappresentare che non erano state fornite agli interessati le informazioni necessarie ad assicurare un trattamento corretto e trasparente, ha chiarito che il trattamento non poteva trovare fondamento neanche nel consenso reso dai soggetti esercenti la responsabilità genitoriale, che è recessivo, come sopra ricordato, rispetto al perseguimento del superiore interesse del minore.

Nel corso dell'istruttoria è emerso, inoltre, che l'asilo aveva attivato alcune telecamere di videosorveglianza, anche durante l'orario in cui era offerto il servizio educativo, in aree interne (inclusi i bagni, limitatamente all'area in cui sono presenti i lavandini, il refettorio, la zona riposo, il guardaroba) ed esterne della struttura, che riprendevano non solo il personale scolastico ma anche i bambini, in maniera non conforme ai principi di "liceità, correttezza e trasparenza" nonché in assenza di un idoneo presupposto di liceità (cfr. parr. 4.7. e 13.3.1.3). Considerato che l'asilo non aveva svolto una previa valutazione di impatto sulla protezione dei dati e non aveva effettuato la comunicazione dei dati di contatto del RPD all'Autorità e che, da ultimo, aveva assegnato tale incarico a un soggetto che si trovava in posizione di conflitto d'interessi, il Garante ha adottato un provvedimento prescrittivo e sanzionatorio nei confronti dell'asilo (provv. 10 luglio 2025, n. 410, doc. web n. 10162731; v. anche Newsletter 10 settembre 2025, doc. web n. 10163470).

Vademecum

Infine, occorre ricordare che nel corso dell'anno il Garante ha aggiornato il Vademecum "La scuola a prova di privacy", in conformità all'evoluzione della normativa di settore, dei recenti provvedimenti dell'Autorità, dei pareri forniti al MIM, fornendo nuove indicazioni sull'utilizzo dell'IA in ambito scolastico e sulla creazione di chat di classe (doc. web n. 9886884).

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 suddivise in relazione alle questioni della pubblicazione di dati personali online e dell'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 redatti da ANAC

Nel periodo di riferimento si ritiene utile segnalare il parere reso su sei schemi standard di pubblicazione predisposti da ANAC – riguardanti gli obblighi di pubblicazione previsti dagli artt. 14, 15-*bis,* 15-*ter*, 33, 37 e 41 del d.lgs. n. 33/2013 – ai sensi dell'art. 48, commi 1 e 3, d.lgs. n. 33/2013 (provv. 10 luglio 2025, n. 412, doc. web n. 10168235).

Il parere segue quello già dato nel 2024 sugli altri 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 del d.lgs. n. 33/2013 (provv. 22 febbraio 2024, n. 92, doc. web n. 9996090). Il Garante ha evidenziato che gli schemi tenevano conto delle osservazioni già fornite dall'Ufficio, ma ha anche chiesto ad ANAC di apportare ulteriori modifiche. In particolare è stato chiesto di modificare lo schema standard di pubblicazione relativo:

- all'art. 14, suggerendo di richiamare nello schema di pubblicazione dei dati personali riferiti a titolari di incarichi politici, di amministrazione, di direzione o di governo e ai titolari di incarichi dirigenziali, la possibilità di consultare le linee sul trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati (provv. 15 maggio 2014, n. 243, doc. web n. 3134436) che contengono ulteriori indicazioni sulle cautele da adottare. Inoltre, con riferimento ai dati del coniuge non separato e parenti entro il secondo grado del titolare dell'incarico è stato chiesto di modificare lo schema, in modo che non venga specificato anche il grado di parentela, in quanto elemento non previsto dall'art. 14, comma 1, lett. f), d.lgs. n. 33/2013 (che dispone unicamente di dare evidenza del mancato consenso dei parenti);
- all'art. 15-*ter*, nella parte riguardante «Tecnici e altri soggetti qualificati e coadiutori Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati alla criminalità organizzata (ANBSC)», evidenziando che la disciplina di settore fa riferimento all'obbligo di pubblicare unicamente «gli incarichi conferiti […] nonché i compensi a ciascuno di essi liquidati» per cui è stato ritenuto che non possano essere diffusi ulteriori dati e informazioni personali, laddove non previsti da ulteriori discipline di settore;
- all'art. 41, chiarendo come in relazione alle procedure di conferimento degli incarichi riguardanti la dirigenza sanitaria si applicano gli obblighi di trasparenza previsti per i concorsi pubblici (art. 19 del d.lgs. n. 33/2013) in cui non è prevista la pubblicità di curriculum e nominativi di candidati non vincitori. È stato, inoltre, fatto presente – per la parte intitolata «Schemi di pubblicazione» e per la parte intitolata «b) Schema di pubblicazione sugli incarichi dirigenziali (art. 14, co. 1-*bis* e 41, comma 2 e 3) per la dirigenza sanitaria» – che va omessa l'indicazione per la quale, in relazione alla dirigenza sanitaria, sono applicabili gli obblighi di pubblicazione di cui all'art. 14 del d.lgs. n. 33/2013, e inserito il riferimento all'art. 15 del d.lgs. n. 33/2013, richiamato dall'art. 41, comma 3, del medesimo decreto. In alternativa, considerando anche la circostanza indicata nello schema, ossia che «per i dirigenti sanitari di cui all'articolo 41, comma 2,

l'applicazione degli obblighi dell'art. 14 – eccetto il comma 1-*ter* – è sospesa, nelle more dell'adozione del reg. di cui all'art. 1, comma 7, d.l. n. 162/2019», è stato chiesto di valutare la possibilità di sospendere, temporaneamente, l'iter di approvazione dello schema di modello riguardante l'art. 41, in attesa della citata revisione legislativa.

Sempre in tema di schemi standard di pubblicazione, è stato fornito un ulteriore parere all'ANAC (provv. 13 marzo 2025, n. 132, doc. web n. 10138925) su dieci modelli standardizzati di dichiarazione sull'assenza di cause di inconferibilità e incompatibilità negli incarichi pubblici, rese secondo quanto previsto dall'art. 20 del d.lgs. n. 39/2013. In tale occasione, anche se i modelli sono stati ritenuti complessivamente idonei, sono state chieste alcune modifiche per evitare trattamenti di dati non conformi al RGPD. In particolare è stato chiesto di eliminare il riferimento all'autorizzazione al consenso al trattamento, non necessaria per i soggetti pubblici, e quello alla dichiarazione di comprensione dell'informativa di cui all'art. 14 del RGPD. È stato, inoltre, chiesto di eliminare la frase riguardante la richiesta generica di documenti (come sentenze), perché comportante una raccolta eccessiva di dati personali, anche di terzi, e di inserire un'indicazione, per i soggetti che ricevono le dichiarazioni, di oscurare in sede di pubblicazione online la sottoscrizione autografa del soggetto interessato. Si è, infine, invitata l'ANAC a valutare, allo scopo di responsabilizzare i soggetti interessati in relazione alla veridicità delle dichiarazioni rese, la possibilità di inserire una specifica frase nei modelli in ordine alla sussistenza dei poteri di accertamento e controllo previsti dalla disciplina vigente in capo all'ente che riceve la dichiarazione riguardanti la relativa veridicità, anche tramite acquisizione di informazioni sulle iscrizioni esistenti nel casellario giudiziale.

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

Diffusione illecita di dati personali

Diversi sono stati gli interventi che hanno portato anche all'adozione di specifici 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 oppure per violazione del divieto di diffusione di dati sulla salute (art. 2-*septies*, comma 8, del Codice; art. 9, parr. 1, 2 e 4, RGPD).

In particolare, si ricorda il caso in cui è stata dichiarata l'illiceità del trattamento effettuato da alcuni enti locali per aver pubblicato online sul sito web istituzionale:

- registri delle richieste di accesso agli atti (civico e documentale), contenenti dati relativi a 1.455 istanze presentate tra il 2017 e settembre 2023 in cui comparivano nomi e cognomi dei mittenti e dei destinatari, numeri di protocollo, oggetto e descrizione delle istanze. In alcuni casi erano stati riportati i nominativi di proprietari di immobili o di intestatari di pratiche edilizie e in uno anche informazioni sullo stato di salute di un cittadino. La diffusione di tali informazioni, come sottolineato nel provvedimento, si poneva in contrasto con la disciplina in materia di protezione dei dati personali nonché con le stesse indicazioni contenute nelle linee guida ANAC (det. n. 1309/2016) e con la circolare del Ministro per la p.a. n. 1/2019, che richiedono espressamente l'oscuramento dei dati personali presenti nel registro degli accessi pubblicati online, inclusi i nomi dei richiedenti e delle persone fisiche citate nei documenti (provv. 10 luglio 2025, n. 387, doc. web n. 10167956);
- documenti allegati a una delibera di una giunta comunale pubblicati online, riguardante la costituzione in giudizio da parte dell'ente e la nomina del proprio difensore legale. Tali allegati contenevano, in alcuni casi, le sole iniziali mentre, in altri, anche i nominativi dei soggetti ricorrenti che avevano agito contro il comune, comprensivi della data di nascita, indirizzo di residenza e codice fiscale. Il Garante è tornato

sull'argomento, ribadendo che, ai fini della pubblicazione sul sito web istituzionale, risulta «del tutto irrilevante, e dunque sproporzionato, diffondere su Internet anche i nominativi delle parti in causa […]», essendo sufficiente, nel rispetto del principio di adeguata motivazione, indicare gli elementi essenziali della vicenda o «anche solo il numero di ruolo generale della causa» (provv. 20 aprile 2025, n. 245, doc. web n. 10145821). Sotto tale profilo, non basta sostituire il nome e cognome delle parti con le relative iniziali, ma è necessario oscurare del tutto il nominativo e le altre informazioni riferite agli interessati che ne possono consentire l'identificazione anche a posteriori;

- dati e informazioni personali, contenuti nella dichiarazione dell'insussistenza di cause di inconferibilità e incompatibilità presentata al tempo dal reclamante in qualità di consigliere comunale, quali la data e il luogo di nascita, l'indirizzo di residenza e di domicilio, nonché la firma autografa (provv. 23 giugno 2025, n. 361, doc. web n. 10161361).

4.4.3. Accesso civico

In materia di accesso civico, il Garante è intervenuto in numerosi casi fornendo il parere previsto dalla disciplina di settore sulle questioni sottoposte. Tra i casi trattati si ritiene utile ricordare in primo luogo le fattispecie in cui il Garante ha precisato il proprio ambito di intervento o l'impossibilità di richiamare il limite derivante dalla protezione dei dati personali oppure la possibilità di fornire l'accesso civico ai documenti richiesti oscurando i dati personali eccedenti.

Ambito del diritto di accesso

Sul primo punto, è stato rilevato come è possibile fornire un parere sull'accesso civico solo se la richiesta riguarda atti nella disponibilità dell'amministrazione. Di conseguenza, in un caso sottoposto all'attenzione il Garante è stato risposto di non potersi pronunciare nel merito, in quanto dagli atti emergeva come il soggetto destinatario dell'istanza di accesso non deteneva i provvedimenti oggetto della domanda di accesso (provv. 4 dicembre 2025, n. 742, doc. web n. 10209869).

Insussistenza dei limiti derivanti dalla protezione dei dati

In diverse situazioni, il Garante ha evidenziato che l'amministrazione non poteva richiamare il limite della protezione dati personali per negare l'accesso. Tale rilevazione è avvenuta ad esempio nei casi in cui i documenti richiesti riguardavano:

- persone giuridiche e società. In diversi casi è stato evidenziato come non fosse possibile condividere la soluzione adottata dall'amministrazione, laddove aveva negato l'accesso civico alla documentazione richiesta riferita a una società e a un ente pubblico, indistintamente e sulla base della presenza di dati personali di soggetti terzi, senza valutare la possibilità di oscuramento di tali informazioni, fornendo un accesso parziale ai sensi dell'art. 5-*bis*, comma 4, d.lgs. n. 33/2013 (provv. 13 febbraio 2025, n. 80, doc. web n. 10111138. Cfr. anche provv.ti 26 ottobre 2025, n. 653, doc. web n. 10193192; 17 aprile 2025, n. 235, doc. web n. 10140385 e 10 luglio 2025, n. 408, doc. web n. 10161017);
- eventuali morosità degli amministratori e consiglieri comunali che avevano occupato immobili di proprietà comunale in ordine a mancati pagamenti dei canoni/indennità. Le informazioni riguardanti il fatto che un soggetto, titolare di un incarico politico (quali sindaco o consigliere comunale), abbia un debito liquido ed esigibile verso il comune e sia stato legalmente messo in mora (oppure, nel caso di mancato pagamento per imposte, tasse e tributi nei riguardi dell'ente, abbia ricevuto invano la notificazione dell'avviso di cui all'art. 46 del d.P.R. n. 602/1973) sono strumentali rispetto alla possibilità di esercitare l'azione popolare prevista dall'art. 70 del d.lgs. n. 267/2000 per far dichiarare la decadenza derivante dalle situazioni di incompatibilità dall'incarico politico, disciplinate dall'art. 63, comma 1, n. 6, d.lgs. n. 267/2000. Per tali motivi, è stato ritenuto che l'accesso civico generalizzato alle predette informazioni – contrariamente

a quanto affermato dal comune nel provvedimento di diniego dell'accesso civico – non poteva essere negato richiamando generici riferimenti alla riservatezza dei soggetti interessati o il limite previsto dall'art. 5-*bis*, comma 2, lett. a), d.lgs. n. 33/2013 in materia di protezione dei dati personali (provv. 27 febbraio 2025, n. 102, doc. web n. 10112195);

- rendiconti delle spese, dei contributi e delle donazioni riguardanti candidati di una circoscrizione per le elezioni europee del 2024 detenuti dal collegio regionale di garanzia elettorale (provv. 24 maggio 2025, n. 309, doc. web n. 10143703). Al riguardo, è stato rappresentato che la disciplina statale di settore prevede uno specifico regime di conoscibilità delle dichiarazioni e dei rendiconti depositati dai candidati sia eletti che non eletti, che sono liberamente consultabili presso gli uffici del collegio regionale di garanzia elettorale, cosicché non è possibile richiamare i limiti di riservatezza o di protezione dei dati per negarne la relativa conoscibilità (art. 14, comma 2, l. n. 515/1993);

- dati riferiti al soggetto istante. In tale fattispecie, è stato evidenziato che è possibile rifiutare l'accesso civico richiamando l'esistenza di un pregiudizio concreto alla protezione dei dati personali. Tuttavia, è stato aggiunto che lo strumento dell'accesso civico nel caso in esame non era quello utile per la soddisfazione degli interessi del richiedente. Si è quindi concordato con quanto rappresentato dall'amministrazione al soggetto istante in ordine alla possibilità di utilizzare più correttamente, trattandosi di dati e documenti a lui riferiti, «gli istituti rinvenibili sia nella disciplina in materia di protezione dei dati personali, ai sensi degli artt. 15-22 del Reg. UE 2016/679, sia nella disciplina in materia di accesso documentale, ai sensi degli artt. 22 e ss. della legge 241/90». Come rappresentato da questa Autorità anche in altre occasioni (cfr. parere 12 settembre 2024, n. 558, doc. web n. 10062415), gli strumenti normativi «azionabili e previsti dall'ordinamento – a tutela dello stesso soggetto interessato – sono di tipo (sostanziale e procedurale) diverso da quello utilizzato e rinvenibili sia nella disciplina in materia di protezione dei dati personali (cfr. l'accesso ai propri dati personali disciplinato dall'art. 15 del RGPD) sia nella disciplina in materia di accesso documentale (cfr. l'accesso previsto dagli artt. 22. ss. della l. n. 241/1990)» (provv. 1° marzo 2025, n. 113, doc. web n. 10119782).

Oscuramento dati personali eccedenti

Utili indicazioni sono state fornite in ordine alla possibilità di adottare provvedimenti favorevoli all'ostensione dei documenti, oscurando i dati personali eccedenti, quali nominativi, dati di contatto e firme autografe, in quanto non necessari alla soddisfazione dell'interesse conoscitivo del soggetto istante e capaci di determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei controinteressati, in violazione del principio di minimizzazione dei dati (art. 5, par. 1, lett. c), RGPD) (provv.ti 9 dicembre 2025, n. 744, doc. web n. 10209660 e 24 dicembre 2025, n. 791, doc. web n. 10213911).

Casi di esclusione dell'accesso civico ai sensi dell'art. 5-*bis*, comma 3, d.lgs. n. 33/2013

Come in passato, il Garante ha inoltre ribadito la sussistenza di casi di esclusione dell'accesso civico laddove l'istanza ha avuto a oggetto dati sulla salute.

Tra questi, si ricorda la delicata questione dell'accesso civico a dati numerici di particolari soggetti presi in carico presso il servizio per le dipendenze (Ser.D.) di aziende sanitarie e, in particolare, dei dati numerici di soggetti con ludopatie, disaggregati tramite diversi parametri (numero di soggetti diviso per singole tipologie di dipendenze e numero di soggetti con disturbo da gioco d'azzardo con indicazione di eventuale altra dipendenza come alcool o stupefacenti; ulteriormente suddiviso per età, sesso, occupazione e livello di istruzione). Nel caso in esame, l'azienda sanitaria aveva negato parzialmente l'accesso civico generalizzato, evidenziando di non poter fornire ulteriori dati rispetto a quelli già comunicati al soggetto istante (quali il numero degli utenti in carico ai Ser.D.

dell'azienda nel 2024 e di casi di disturbo da giochi d'azzardo, DGA, divisi per occupazione e titolo di studio), in quanto non idonei a eliminare il rischio di identificazione degli utenti. Il Garante ha evidenziato che dagli atti non emergevano elementi per potersi discostare dalle valutazioni effettuate dall'azienda sanitaria, in concreto, in ordine alla natura identificativa dei dati e al rischio di re-identificazione dei soggetti interessati derivante dalla richiesta di ostensione dei dati richiesti prima descritti (artt. 5, par. 2, e 24 del RGPD), in particolare tenendo conto anche della possibilità per il soggetto istante (nonché, dato il regime di pubblicità propria dell'accesso civico prevista dall'art. 3, comma 1, d.lgs. n. 33/2013, per soggetti terzi) di incrociare e raffrontare i dati ottenuti con altre informazioni ausiliarie già conosciute o contenute in ulteriori banche dati. L'eventuale re-identificazione dei soggetti interessati avrebbe infatti portato alla conoscenza di dati di natura delicata e idonei a rivelare lo stato di salute (art. 9 del RGPD), per i quali l'accesso civico è comunque escluso (art. 5-*bis*, comma 3, d.lgs. n. 33/2013), determinando, peraltro, un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei soggetti controinteressati (art. 5, par. 1, lett. c), RGPD) (provv.ti 13 agosto 2025, n. 475, doc. web n. 10169132 e 22 agosto 2025, n. 480, doc. web n. 10170285. Sul diniego di ostensione di dati sulla salute cfr. anche provv. 6 marzo 2025, n. 118, doc. web n. 10120270).

Sussistenza del limite di cui all'art. 5-*bis*, comma 2, lett. a), d.lgs. n. 33/2013

In altri numerosi casi, infine, 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-*bis*, comma 2, lett. a), d.lgs. n. 33/2013. Ciò con particolare riferimento a:

- atti e documenti riguardanti procedimenti disciplinari (provv.ti 6 marzo 2025, n. 118, doc. web n. 10120270; 24 luglio 2025, n. 419, doc. web n. 10167100; 25 settembre 2025, n. 566, doc. web n. 10171152 e 5 ottobre 2025, n. 575, doc. web n. 10196854);
- atti e documenti riguardanti valutazioni e punteggi riferiti ai dipendenti (provv.ti 4 luglio 2025, n. 378, doc. web n. 10167082; 4 agosto 2025, n. 466, doc. web n. 10164354 e 10 novembre 2025, n. 661, doc. web n. 10195295);
- accordi individuali di lavoro in modalità agile stipulati da una procura con i propri dipendenti (provv. 17 aprile 2025, n. 234, doc. web n. 10140423);
- fogli di presenza e/o corrispondenti strumenti, anche informatici, di rilevazione delle presenze sul luogo di lavoro (provv. 10 marzo 2025, n. 130, doc. web n. 10120228);
- schede dettagliate per ogni singolo appalto, contenenti la ripartizione delle somme destinate ai i dipendenti a titolo di incentivi per funzioni tecniche (provv.ti 10 marzo 2025, n. 129, doc. web n. 10120246 e 8 agosto 2025, n. 471, doc. web n. 10169170);
- copia della disposizione di servizio con la quale un dipendente comunale è stato collocato in ferie (provv. 18 agosto 2025, n. 478, doc. web n. 10168570);
- note contenenti dati e informazioni personali riguardanti le misure adottate da un comune per gestire un conflitto di interessi fra due dipendenti. Al riguardo, il Garante ha però precisato che non vi sono invece analoghi motivi ostativi all'ostensione delle parti dei documenti richiesti, contenenti le sole misure organizzative adottate dal comune per la gestione del conflitto di interessi, previo oscuramento dei dati identificativi dei dipendenti controinteressati e di tutte le informazioni di dettaglio contenute nei documenti oggetto di accesso civico che, tenuto conto del contesto di riferimento, consentono di re-identificare gli stessi (provv. 17 novembre 2025, n. 698, doc. web n. 10217105);
- verbali di una commissione di concorso, comprensivi di valutazioni e punteggi su ciascun candidato, nonché tutti i documenti prodotti dai candidati ai fini concorsuali, per l'ammissione a un dottorato di ricerca (provv. 19 giugno 2025, n. 354, doc. web n. 10232000); modulo con la dichiarazione dei titoli e servizi presentati da un docente ai

fini dell'inserimento in graduatoria per l'individuazione dei docenti soprannumerari (provv. 26 giugno 2025, n. 377, doc. web n. 10161035); documentazione con dati personali riguardante l'attivazione e la gestione di tirocini finalizzati all'inclusione sociale, a favore di persone in condizioni di vulnerabilità prese in carico dal servizio sociale professionale e/o dai servizi sanitari competenti (provv. 7 novembre 2025, n. 660, doc. web n. 10195762);

- nota di un ministero recante il parere sull'accoglimento di una istanza di trasferimento straordinario di uno studente, ai sensi dell'art. 9 del r.d. n. 1269/1938 (provv. 4 dicembre 2025, n. 729, doc. web n. 10209690);
- copia del certificato di laurea (provv. 23 gennaio 2025, n. 31, doc. web n. 10110495, cfr. anche provv. 12 giugno 2025, n. 352, doc. web n. 10147170);
- informazioni sull'avvenuto pagamento da parte di un cittadino dell'imposta municipale unica (IMU), per gli anni dal 2019 al 2024 (provv. 9 giugno 2025, n. 351, doc. web, n. 10167218);
- copia dei permessi di costruire e della SCIA. In particolare il Garante ha ritenuto che l'integrale ostensione della documentazione richiesta tramite l'accesso civico nel caso in esame riferiti a permessi di costruire e SCIA – quali documenti di riconoscimento, bonifici bancari, asseverazioni e relazioni illustrative particolareggiate, progetti, tavole ed elaborati grafici, prospetti del fabbricato con piantine interne dei diversi piani – forniscono notizie private relative alla proprietà posseduta e alle relative caratteristiche, investendo, dunque, aspetti che rientrano anche nella sfera personale privata e familiare del proprietario del fabbricato. È stato quindi ritenuto che la trasmissione di tali atti, anche considerando il particolare regime di pubblicità dei dati e informazioni ricevuti tramite l'istituto dell'accesso civico (cfr. art. 3, comma 1, d.lgs. n. 33/2013,) determina un'interferenza ingiustificata e sproporzionata nei diritti e libertà del controinteressato, arrecando, a seconda delle ipotesi e del contesto in cui le informazioni fornite possono essere utilizzate da 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, art. 5, par. 1, lett. b) e c), RGPD) (provv. 14 agosto 2025, n. 476, doc. web n. 1017023 - cfr. anche provv.ti 13 febbraio 2025, n. 80, doc. web n. 10111138; 17 aprile 2025, n. 235, doc. web n. 10140385; 10 luglio 2025, n. 408, doc. web n. 10161017).

4.5. *Mobilità e trasporti*

4.5.1. Regolamentazione e trattamenti effettuati a livello centrale

L'Autorità si è espressa con parere favorevole (provv. 18 dicembre 2025, n. 746, doc. web n. 10212724) in merito allo schema di decreto del Ministero delle infrastrutture e dei trasporti, concernente la disciplina della piattaforma telematica istituita presso il CED della Direzione generale per la motorizzazione, ai fini della richiesta e del rilascio dei contrassegni identificativi dei monopattini a propulsione prevalentemente elettrica. All'esito dell'istruttoria, sono state parzialmente recepite le indicazioni fornite informalmente dall'Autorità ed è stata, in particolare, esclusa la possibilità per gli operatori degli studi di consulenza automobilistica di ottenere la pre-compilazione automatica dei dati personali del soggetto richiedente il contrassegno, attraverso il collegamento con la piattaforma dell'Anagrafe nazionale della popolazione residente (ANPR), in considerazione dei rischi per i diritti e le libertà degli interessati, nonché alla luce delle misure individuate a garanzia degli interessati dall'attuale quadro normativo che disciplina l'accesso alla predetta piattaforma (cfr. art. 62 del d.lgs. n. 82/2005 e d.P.C.M. n. 194/2014; cfr. altresì i pareri resi dal Garante, tra cui, in particolare, i provv.ti 17 aprile

2014, n. 202, doc. web n. 3105794; 24 giugno 2020, n. 110, doc. web n. 9445130; 14 ottobre 2021, n. 367, doc. web n. 9717543). Nonostante i miglioramenti apportati allo schema, sono stati rilevati profili di criticità su cui il Garante ha indicato alcune condizioni volte, in particolare a:

- escludere la verifica automatica con ANPR dei dati dei soggetti richiedenti il contrassegno accedenti alla piattaforma con SPID di secondo livello o CIE (artt. 5, par. 1, lett. a), c) e f), 25 e 32 del RGPD);
- specificare le banche dati che si intende utilizzare, attraverso l'interoperabilità con le Camere di commercio, industria, artigianato e agricoltura, per le finalità di verifica dei poteri di rappresentanza di un soggetto richiedente il contrassegno per conto di un'impresa (artt. 5, par. 1, lett. a), c) e f), 25 e 32 del RGPD);
- prevedere che, con riferimento ai trattamenti di dati personali posti in essere nell'ambito della piattaforma, gli adempimenti connessi al rilascio delle informazioni di cui agli artt. 13 e 14 del RGPD, nonché alla gestione dell'esercizio dei diritti riconosciuti agli interessati ai sensi degli artt. 15 e ss. del RGPD, siano di competenza del solo Ministero (artt. 5, parr. 1, lett. a) e 2, nonché 12 e 24 del RGPD);
- e da ultimo, identificare, nell'allegato tecnico, un termine uniforme per la conservazione dei log – precisando che la stessa debba essere effettuata sempre nell'ambito della medesima piattaforma – nel rispetto del principio di limitazione della conservazione (art. 5, par. 1, lett. e), RGPD).

4.5.2. Mobilità in ambito locale

Nel corso di un'istruttoria originata da quattro reclami, l'Autorità ha rilevato che il verbale di contestazione di violazioni stradali notificato a ciascuno degli interessati era privo di idonea informativa ai sensi degli artt. 13 e 14 del RGPD, essendo previsto un generico rinvio alla consultazione della stessa in Internet al link indicato, o presso le sedi del Corpo di Polizia locale del comune. L'Autorità ha inoltre accertato che nell'informativa reperibile sul sito web istituzionale del comune erano presenti riferimenti non aggiornati né conformi alla normativa sulla protezione dei dati personali, tra cui il richiamo al consenso (indicato, in alcuni casi, come obbligatorio) quale base giuridica del trattamento. Nel corso dell'istruttoria il comune aveva rappresentato di aver provveduto, a seguito della richiesta d'informazioni inviata da parte dell'Autorità, ad integrare il modello di informativa di primo livello presente nei verbali di accertamento e di aver aggiornato l'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 (tra cui la corretta indicazione del titolare del trattamento e dei dati di contatto del RPD, anche ai fini dell'esercizio dei diritti riconosciuti agli interessati ai sensi degli artt. da 15 a 22 del RGPD) e non facilmente raggiungibile da parte degli interessati nell'ambito della navigazione del sito web istituzionale. Per tali ragioni l'Autorità ha sanzionato il comune, per violazione degli artt. 5, par. 1, lett. a), 12 e 13 del RGPD, ingiungendogli, inoltre, ai sensi dell'art. 58, par. 2, lett. d), RGPD, di adottare le misure idonee ad inserire i corretti riferimenti nell'informativa di primo livello e a rendere l'informativa di secondo livello facilmente reperibile e accessibile da parte degli interessati, provvedendo alla cancellazione di eventuali informative obsolete e/o duplicate, all'indicazione omogenea e coerente dei dati di contatto del RPD nelle diverse sezioni del sito web istituzionale, nonché alla riorganizzazione dello stesso in modo da evitare percorsi di navigazione eccessivamente complessi per raggiungere l'informativa (provv. 27 marzo 2025, n. 165, doc. web n. 10201385).

Con distinto reclamo, da cui è originata l'istruttoria concernente l'utilizzo di un sistema di videosorveglianza per l'accertamento di infrazioni stradali (nello specifico,

per gli accessi a un'area ZTL in assenza della relativa autorizzazione), è stata lamentata, in particolare, la scarsa chiarezza nell'individuazione del titolare del trattamento in quanto, nella cartellonistica presente all'epoca dei fatti, era stato indicato un comune in luogo del nuovo ente di riferimento, con conseguente pregiudizio in merito al principio di trasparenza anche ai fini del corretto esercizio dei diritti da parte degli interessati. Il predetto ente aveva rappresentato in corso d'istruttoria di aver provveduto, in particolare, ad aggiornare l'informativa di primo livello e di aver adottato un'informativa estesa, pubblicata sul proprio sito web istituzionale. L'Autorità ha, pertanto, adottato un provvedimento sanzionatorio nei confronti dell'ente, per la violazione degli artt. 5, par. 1, lett. a), 12 e 13 del RGPD (provv. 27 marzo 2025, n. 168, doc. web n. 10138999).

In un altro caso, originato da un reclamo, era stata lamentata, in particolare, l'omissione di apposita cartellonistica informativa da parte di un comune in merito alla presenza di sistemi elettronici di rilevazione automatizzata delle violazioni stradali, nonché il mancato oscuramento dei volti dei soggetti a bordo del veicolo nell'immagine attestante l'infrazione rilevata. Il comune aveva rappresentato di aver provveduto, a seguito dell'istruttoria avviata da parte dell'Autorità, ad aggiornare l'informativa di primo livello, e di avere effettuato l'acquisto di apposita cartellonistica e disposto la progressiva installazione sul territorio comunale, senza aver provveduto, tuttavia, a dare evidenza di tale aggiornamento e dell'informativa di secondo livello adottata. In aggiunta, l'Autorità aveva accertato che la predetta informativa non era risultata facilmente raggiungibile da parte degli interessati nell'ambito della navigazione del sito web. Il comune ha rappresentato, altresì, di aver adottato misure volte a garantire, in caso di accesso degli aventi diritto alle immagini pertinenti l'infrazione al codice della strada, l'oscuramento degli eventuali occupanti o soggetti e/o informazioni estranei alla violazione. L'Autorità ha, pertanto, irrogato una sanzione pecuniaria nei confronti del comune ingiungendo, altresì, di adottare le misure idonee a fornire agli interessati l'informativa di primo livello, anche completando l'installazione della cartellonistica aggiornata in prossimità dei dispositivi di ripresa foto/video installati nel territorio comunale, e a rendere l'informativa di secondo livello facilmente reperibile e accessibile da parte degli interessati sul proprio sito web istituzionale, provvedendo alla cancellazione di eventuali informative obsolete e/o duplicate nonché a rivedere l'organizzazione del proprio sito web istituzionale in modo da evitare la cosiddetta *click fatigue* per gli interessati a causa di percorsi di navigazione multipli e/o eccessivamente complessi per raggiungere la predetta informativa (provv. 29 aprile 2025, n. 244, doc. web n. 10144974).

Con riferimento, infine, ad un'ulteriore istruttoria, originata da una segnalazione, l'Autorità aveva appreso dell'iniziativa riguardante il trattamento di dati personali nell'ambito della procedura online per la richiesta di abbonamento agevolato per il trasporto pubblico locale. In particolare, nel modulo online per presentare la suddetta richiesta erano presenti due riquadri contenenti riferimenti non aggiornati alla normativa sulla protezione dei dati personali e indicanti l'acquisizione del consenso (obbligatorio per poter inviare la richiesta di abbonamento scontato) quale base giuridica per il trattamento dei dati personali per finalità di marketing diretto. In aggiunta, l'Autorità ha accertato che nell'informativa presente nel relativo bando per l'acquisto dell'abbonamento annuale agevolato erano presenti elementi non conformi agli artt. 13 e 14 del RGPD (base giuridica, finalità, indicazione del medesimo soggetto come titolare e responsabile del trattamento). Al riguardo, l'Autorità ha ritenuto che, nella fattispecie in esame, il comune doveva essere considerato titolare del trattamento e il gestore responsabile del trattamento (artt. 4, par. 1, nn. 7 e 8, 24 e 28 del RGPD). Sul punto, il Garante ha ricordato che l'erogazione del servizio pubblico locale inerisce alle finalità istituzionali del comune, suscettibili di essere perseguite anche avvalendosi di uno o più soggetti terzi

– responsabili del trattamento – che agiscono in nome e per conto del titolare, disciplinando il rapporto, per quanto concerne la protezione dei dati personali, ai sensi dell'art. 28 del RGPD. Nel caso di specie, l'Autorità ha tenuto conto, altresì, di quanto previsto dalle linee guida CEPD 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento, tra cui la legittima aspettativa degli interessati in merito ai ruoli ricoperti dai soggetti coinvolti, anche sulla base delle modalità di presentazione e dei riferimenti presenti nel bando per l'assegnazione di abbonamenti agevolati. Alla luce di tali elementi, il Garante ha rilevato la violazione, da parte del titolare del trattamento, degli artt. 5, par. 1, lett. a) e par. 2, 12, 13, 24, 25, par. 1 e 28 del RGPD e, per quanto concerne il responsabile del trattamento, degli artt. 5, par. 1, lett. a), 6 e 9 del RGPD, nonché 2-*ter* e 2-*sexies* del Codice. Tenuto conto di tutte le circostanze del caso, il Garante ha ritenuto sufficiente ammonire sia il titolare del trattamento sia il responsabile con riguardo ai predetti trattamenti. Il giudizio di impugnazione avverso il provvedimento adottato nei confronti del gestore del servizio di trasporto pubblico locale è, allo stato, pendente (provv.ti 17 luglio 2025, nn. 421 e 422, doc. web nn. 10171816 e 10172146).

4.6. *Trattamenti in ambito locale*

4.6.1. Ambiente

A seguito di un reclamo il Garante ha provveduto a verificare la contestata omissione di apposita cartellonistica informativa da parte di un comune in prossimità di una zona sottoposta a videosorveglianza, nonché il mancato conferimento di un'informativa completa in merito al trattamento dei dati personali effettuato ai fini dell'accertamento dello scorretto conferimento dei rifiuti urbani. Al riguardo, il comune aveva rappresentato di aver provveduto, a seguito dell'istruttoria avviata dall'Autorità, ad aggiornare la cartellonistica contenente l'informativa di primo livello e a ripristinare la stessa presso la zona interessata dai fatti oggetto di reclamo, ad adattare la configurazione del sistema foto/video di rilevazione di violazioni in merito al conferimento dei rifiuti nonché ad aggiornare l'informativa di secondo livello. Tuttavia, in sede istruttoria era stato accertato che nell'informativa di primo livello risultavano ancora indicate una pluralità di finalità – nonostante lo specifico posizionamento del sistema foto/video, per rilevare lo scorretto conferimento di rifiuti urbani – che erano altresì menzionate (oltre ad ulteriori elementi non conformi alla normativa in materia di protezione dei dati personali) nell'informativa di secondo livello; quest'ultima, inoltre, risultava non facilmente raggiungibile sul sito web istituzionale del comune. L'Autorità ha, pertanto, irrogato una sanzione pecuniaria ingiungendo al comune, altresì, di adottare le misure idonee a fornire agli interessati l'informativa di primo livello anche completando l'installazione della cartellonistica aggiornata in prossimità dei dispositivi di ripresa foto/video, ad adattare il contenuto della stessa, provvedendo ad indicare la specifica finalità concernente il trattamento in esame, eliminando le finalità ultronee nonché a rendere l'informativa di secondo livello facilmente reperibile e accessibile e conforme alla normativa in materia di protezione dei dati personali (provv. 4 giugno 2025, n. 322, doc. web n. 10163530).

Con riferimento a un'istruttoria, originata da una segnalazione, l'Autorità ha appreso dell'installazione, da parte di un comune, in base a un'ordinanza comunale, di un sistema foto/video per il controllo del corretto conferimento dei rifiuti urbani, nonché per l'accertamento del corretto adempimento degli obblighi relativi alla TARI. Quest'ultima finalità, in particolare, era perseguita acquisendo, attraverso l'esame delle immagini oggetto di registrazione, a partire dalla targa del veicolo, i dati del proprietario del veicolo mediante interrogazione al PRA, e verificando attraverso la banca dati TARI

le eventuali pendenze/inadempienze. L'Autorità ha evidenziato l'assenza nella normativa nazionale di una base giuridica idonea per rango e qualità che giustifichi il trattamento dei numeri di targa dei veicoli per tale finalità; né il comune aveva provato la sussistenza di un quadro giuridico idoneo a giustificare tale trattamento per le finalità prospettate. È stato, pertanto, accertato che il comune aveva agito in modo non conforme al principio di liceità, correttezza e trasparenza e in assenza di un'idonea base giuridica; inoltre, avendo il comune trattato i dati concernenti le immagini dei veicoli per perseguire una finalità diversa (quale l'accertamento del corretto pagamento della TARI), l'Autorità ha accertato che lo stesso aveva agito in maniera non conforme al principio di limitazione della finalità. Sotto diverso ma connesso profilo, è stato accertato che il comune aveva violato il principio di trasparenza, non avendo provveduto a fornire agli interessati un'idonea informativa di primo livello in merito al trattamento dei dati personali effettuato, mediante il sistema foto/video in esame, ai fini dell'accertamento del non corretto conferimento dei rifiuti urbani, e omettendo, altresì, di fornire un'informativa estesa di secondo livello, che è risultata peraltro inidonea quando successivamente è stata resa disponibile. Il Garante ha adottato, pertanto, un provvedimento correttivo e sanzionatorio nei confronti del comune, ingiungendo allo stesso, inoltre, di adottare le misure idonee a fornire agli interessati l'informativa di primo livello adattando il contenuto della stessa, provvedendo ad indicare la specifica finalità amministrativa di rilevazione del non corretto conferimento dei rifiuti ed eliminando le finalità ultronee, nonché a rendere l'informativa di secondo livello conforme alla normativa in materia di protezione dei dati personali (provv. 23 ottobre 2025, n. 700, doc. web n. 10211816).

L'Autorità ha inoltre svolto un'istruttoria, avviata d'ufficio sulla base di notizie stampa, nei confronti di un comune e di un'università, concernente la somministrazione di questionari relativi alla raccolta dei rifiuti, trasmessi ai cittadini di un comune mediante e-mail o con un link cliccabile da siti web e pagine social. In sede istruttoria, il Garante ha chiarito la necessità di esaminare, sul piano sostanziale e non meramente formale, le attività in concreto svolte dai soggetti coinvolti nella vicenda contestata allo scopo di individuare in concreto il ruolo rispettivamente svolto in qualità di titolare o responsabile del trattamento. Nel caso in esame, anche tenendo conto di quanto previsto dalle linee guida 07/2020, adottate dal CEPD il 7 luglio 2021, l'Autorità ha ritenuto il comune e l'università due autonomi titolari del trattamento. Ha quindi rilevato, da parte del comune, una comunicazione dei dati personali dei propri contribuenti TARI ad un soggetto terzo (l'università) effettuata in assenza di un idoneo presupposto normativo, in violazione del principio di liceità, correttezza e trasparenza e senza rispettare i principi di responsabilizzazione e della "protezione dei dati fin dalla progettazione"; quanto all'università, ha ritenuto che il successivo trattamento dei dati personali dei contribuenti coinvolti nel progetto di ricerca fosse stato effettuato in assenza di un idoneo presupposto normativo e di un'idonea informativa, in violazione del principio di liceità, correttezza e trasparenza e, ancora una volta, senza rispettare i principi di responsabilizzazione e della "protezione dei dati fin dalla progettazione". Alla luce di tali elementi, il Garante ha adottato due provvedimenti sanzionatori, per violazione, da parte del comune, degli artt. 5, parr. 1, lett. a), e 2, 6, parr. 1, lett. c) ed e), 2 e 3, 24 e 25 del RGPD e 2-*ter*, commi 1-3, del Codice e, per quanto concerne l'università, degli artt. 5, parr. 1, lett. a), e 2, 6, parr. 1, lett. a), c) ed e), 2 e 3, 12, 13, 14, 24 e 25 del RGPD e 2-*ter*, commi 1- 3, del Codice (provv.ti 11 settembre 2025, nn. 523 e 524, doc. web nn. 10183866 e 10183882).

4.6.2. Diffusione di video sui social network

Nell'ambito di un'istruttoria, originata da una segnalazione, l'Autorità ha sanzionato un comune per la pubblicazione, su una pagina Facebook riferibile a tale comune, di

numerosi post contenenti foto e video di minori e di persone con disabilità presso un centro diurno. A seguito dell'avvio del procedimento, il Garante aveva altresì accertato che, contrariamente a quanto dichiarato dal comune, alcuni dei post oggetto della segnalazione risultavano ancora reperibili sulla medesima pagina Facebook e ulteriori post, contenenti immagini di minori grossolanamente pixelate, erano stati pubblicati successivamente. Inoltre i dati di contatto del RPD non erano risultati reperibili sul sito istituzionale, né indicati nell'informativa pubblicata sullo stesso. Al riguardo, il Garante ha ricordato che, di regola, i soggetti pubblici, contrariamente a quanto rappresentato dal comune in corso d'istruttoria, non possono avvalersi del consenso come base giuridica per i trattamenti effettuati, potendo sussistere un evidente squilibrio tra l'interessato e il titolare del trattamento (v. cons. 43 del RGPD). Per tali ragioni, l'Autorità ha sanzionato il comune per la diffusione delle immagini di numerosi minori e persone disabili sulla pagina Facebook dello stesso comune, in assenza di una adeguata base giuridica, in violazione degli artt. 5, par. 1, lett. a) e c), 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b) e 9 del RGPD, nonché degli artt. 2-*ter*, commi 1 e 3, 2-*sexies* e 2-*septies*, comma 8, del Codice e per la mancata pubblicazione dei dati di contatto del RPD in violazione degli artt. 13, par. 1, lett. b) e 37, par. 7, RGPD. Con il medesimo provvedimento l'Autorità ha adottato misure correttive nei confronti del comune, ingiungendo allo stesso di cessare l'ulteriore diffusione dei dati personali pubblicati sulla pagina Facebook, di pubblicare i dati di contatto del RPD sul sito web istituzionale nonché di indicarli nell'informativa presente sul predetto sito web (provv. 11 settembre 2025, n. 483, doc. web n. 10177128; v. anche par. 4.7).

In un altro caso, a seguito di una segnalazione, l'Autorità ha avviato un'istruttoria in merito alla pubblicazione, sul profilo Facebook del sindaco di un comune, di dati personali relativi a numerosi cittadini residenti risultati positivi al COVID-19, nonché di dati personali e foto di minori all'atto della vaccinazione. Nell'ambito dell'istruttoria, era stato rappresentato che la pubblicazione di quei dati era avvenuta nella prima fase di gestione della pandemia e su richiesta degli interessati che, nell'ottica di un comportamento responsabile volto alla riduzione del contagio, avevano inteso ricorrere al "profilo pubblico" del sindaco per rendere nota tale informazione e consentire alle persone con le quali erano stati in contatto di adottare a loro volta le necessarie misure precauzionali. Analogamente, anche la pubblicazione delle foto di minori intenti alla vaccinazione era stata effettuata unicamente con il consenso dei genitori, i quali avevano inviato al sindaco le foto, spesso già pubblicate sui propri profili personali, con la richiesta di pubblicarle con l'intento di promuovere l'importanza della vaccinazione nella situazione di emergenza sanitaria. In tale contesto, il sindaco aveva fornito evidenze dei messaggi inviati via WhatsApp o SMS, in cui alcuni cittadini lo avevano autorizzato a pubblicare la propria positività al COVID-19 sul suo profilo Facebook. Nel richiamare la straordinarietà della situazione e, soprattutto nella prima fase dell'emergenza, il cattivo funzionamento dei circuiti di tracciamento dei positivi – flussi informativi successivamente strutturati tra le ASL e il sindaco in qualità di autorità sanitaria comunale – il sindaco aveva evidenziato i poteri straordinari riconosciuti nel contesto dell'emergenza, nell'ambito del quadro normativo delle funzioni assegnate ai sindaci dagli artt. 50 e 54 del d.lgs. n. 267/2000, richiamando altresì l'art. 17-*bis* del d.l. n. 18/2020. L'Autorità ha osservato che la disciplina in materia di protezione dei dati personali vieta la diffusione dei dati relativi alla salute, e che tale divieto non è stato derogato dalla normativa d'urgenza sul COVID-19 (art. 9 del RGPD; artt. 2-*septies*, comma 8 e art. 166, comma 2, del Codice; art. 14 del d.l. n. 14/2020 e art. 17-*bis* del cit. d.l. n. 18/2020, convertito con modificazioni, dalla l. n. 27/2020). Con specifico riferimento alla diffusione sui social e sugli organi di stampa, anche online, di dati personali come quelli sopra citati, il

Garante aveva ricordato che anche in una situazione di emergenza non possono essere disattese alcune garanzie a tutela della riservatezza e della dignità delle persone contenute nella normativa vigente e nelle regole deontologiche relative all'attività giornalistica (cfr. comunicato stampa 31 marzo 2020, doc. web n. 9303613). Pertanto, pur prendendo atto delle circostanze rappresentate dal sindaco, l'Autorità ha ritenuto che la diffusione dei dati era stata effettuata in contrasto al principio di liceità, correttezza e trasparenza e in assenza di una base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) ed e), e 9 del RGPD, nonché degli artt. 2-*ter*, commi 1 e 3, 2-*sexies* e 2-*septies*, comma 8, del Codice (provv. 23 ottobre 2025, n. 627, doc. web n. 10195910).

In un altro caso, a seguito di notizie stampa, l'Autorità ha avviato un'istruttoria, in relazione ai trattamenti di dati personali connessi all'erogazione della carta "Dedicata a te" per il 2023 consistente nell'erogazione di 380 euro per l'acquisto di beni alimentari e altri generi a favore di persone a basso reddito escluse da altri sussidi ed in particolare alla pubblicazione degli elenchi dei beneficiari sul sito istituzionale di un comune. Al riguardo, la procedura per l'erogazione prevedeva che i comuni, ricevuto dall'INPS l'elenco dei beneficiari ricavato dai dati in possesso dello stesso ente, avrebbero dovuto verificare la posizione anagrafica dei nuclei familiari e consolidare gli elenchi mediante l'applicazione web dell'INPS entro 15 giorni, in modo che, nei successivi 10 giorni, l'INPS potesse comunicare l'elenco definitivo a Poste italiane per la predisposizione delle carte. Ai comuni era stato, infine, assegnato il compito di comunicare agli interessati l'assegnazione del beneficio e le modalità di ritiro della carta. In tale contesto, al fine di raggiungere il maggior numero di interessati nei ristretti termini temporali previsti, il comune aveva pubblicato sul sito istituzionale l'avviso pubblico e un documento di 29 pagine recante la lista dei beneficiari della carta, individuati mediante l'indicazione delle prime tre lettere del cognome, dei primi nove elementi del codice fiscale e dalla data di nascita.

Pur prendendo atto delle specifiche circostanze rappresentate dal comune e della scelta di effettuare la pubblicazione senza i dati identificativi per esteso degli interessati, l'Autorità ha ritenuto che, nel caso in esame, il rischio di identificazione doveva considerarsi elevato, tenuto conto che le informazioni rese disponibili potevano essere raffrontate o incrociate con altre fonti, o comunque con informazioni di contesto in possesso di terzi nell'ambito della comunità o del contesto familiare o sociale e del ristretto bacino territoriale di riferimento, limitato al comune.

Nel ricordare che la diffusione di dati personali è ammessa solo quando è prevista da un'idonea base giuridica (art. 2-*ter*, commi 1 e 3, del Codice), e che l'art. 7 del decreto 18 aprile 2023, pur imponendo agli enti locali l'obbligo di comunicare agli interessati l'assegnazione del beneficio e le modalità di ritiro delle carte presso gli uffici postali abilitati, non poteva in alcun modo ritenersi autorizzativa della pubblicazione generalizzata dei dati personali relativi ai beneficiari, ha sanzionato il comune in quanto il trattamento era avvenuto in assenza di una base giuridica adeguata, in violazione dell'art. 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), RGPD, nonché degli artt. 2-*ter*, commi 1 e 3, del Codice (provv. 4 giugno 2025, n. 321, doc. web n. 10163483).

4.6.3. Tributi locali

Contributo d'accesso del Comune di Venezia

All'esito di una complessa istruttoria avviata a seguito di notizie di stampa, comprensiva anche di un'attività ispettiva urgente delegata al Nucleo speciale privacy e nuove tecnologie della Guardia di finanza, l'Autorità ha adottato un provvedimento sanzionatorio nei confronti del Comune di Venezia, in relazione all'attuazione del regolamento volto ad introdurre il contributo d'accesso alla città di Venezia e alle isole minori della laguna. Nel corso dell'istruttoria, il Comune aveva apportato miglioramenti alla disciplina

istitutiva del predetto contributo, i quali tuttavia non sono risultati sufficienti a garantire il rispetto della normativa in materia di protezione dei dati personali.

Anche in considerazione degli elementi acquisiti in sede dell'accertamento ispettivo – in particolare relativi alle impostazioni di sicurezza dei totem dislocati in alcuni punti di accesso alla città per il pagamento del contributo o per l'acquisizione del titolo di esenzione – il Garante ha ritenuto che il predetto trattamento fosse stato effettuato in violazione dei principi di necessità e di proporzionalità, di liceità, correttezza e trasparenza, di limitazione della finalità, di minimizzazione, di limitazione della conservazione, di integrità e riservatezza, nonché di *privacy by design* e *privacy by default* (artt. 5, par. 1, lett. a), b), c), e) ed f), e 6, parr. 1, lett. e), e 3, nonché 25 e 32 del RGPD) e pertanto ha disposto l'adozione di specifiche misure correttive di cui all'art. 58, par. 2, RGPD (provv. 4 agosto 2025 n. 468, doc. web n. 10164311).

4.7. *Il Responsabile della protezione dei dati (RPD) in ambito pubblico*

Nell'ambito dell'indagine avviata nel 2023 nei confronti di grandi enti locali per verificare il rispetto dell'obbligo di comunicazione dei dati di contatto del RPD (cfr. Relazione 2023, par. 4.8, p. 53), il Garante ha adottato alcuni provvedimenti sanzionatori nei confronti di comuni con riferimento agli obblighi di designazione del RPD e di pubblicazione e comunicazione all'Autorità dei relativi dati di contatto, di cui all'art. 37, parr. 1 e 7, RGPD (provv.ti 16 gennaio 2025, n. 5, doc. web n. 10110910; n. 6, doc. web n. 10110989; 27 marzo 2025, n. 166, doc. web n. 10138964 e 10 luglio 2025, n. 384, doc. web n. 10161611).

Un provvedimento sanzionatorio è stato adottato anche nei confronti di un asilo per avere omesso di effettuare la pubblicazione e la comunicazione dei dati di contatto del RPD all'Autorità e per avere assegnato tale incarico a un soggetto che, in ragione del proprio ruolo di dirigente e legale rappresentante, era in posizione di conflitto d'interessi, in violazione degli artt. 37, par. 7, e 38, par. 6, RGPD (provv. 10 luglio 2025, n. 410, doc. web n. 10162731).

In un altro caso l'Autorità aveva rilevato un altro profilo di conflitto d'interessi nei confronti di una società *in house* di un comune che aveva chiesto al RPD di occuparsi della redazione e sottoscrizione della valutazione d'impatto sulla protezione dei dati. Tale circostanza si era posta in violazione dell'art. 38, par. 6, in riferimento agli artt. 35, par. 2, e 39, par. 1, lett. c), RGPD in merito al fatto che il RPD deve fornire il proprio parere indipendente in merito alla valutazione d'impatto sulla protezione dei dati predisposta dal titolare del trattamento, svuotando così le specifiche prerogative di consultazione che gli spettano (provv. 10 aprile 2025, n. 202, doc. web n. 10140338).

Inoltre, il Garante ha adottato un provvedimento sanzionatorio nei confronti di un ordine professionale per violazione dell'art. 37, par. 1, lett. a), RGPD, avendo designato il RPD solo a partire da una certa data, e, peraltro, con atti caratterizzati da inesattezze e incongruenze, in particolare facendo riferimento erroneamente alla diversa figura del responsabile del trattamento di cui all'art. 28 del RGPD (provv. 9 ottobre 2025, n. 589, doc. web n. 10192819).

Provvedimenti sanzionatori sono stati infine adottati anche nei confronti di un istituto scolastico per avere nominato un nuovo RPD ed effettuato la comunicazione all'Autorità con notevole ritardo rispetto alla data di cessazione dell'incarico del precedente RPD, in violazione dell'art. 37, parr.1 e 7, RGPD (provv. 4 giugno 2025, n. 317, doc. web n. 10162966), e nei confronti di un comune per non avere pubblicato i dati di contatto del RPD sul proprio sito web istituzionale, neanche nell'informativa in merito al

trattamento dei dati personali presente nel *footer* del sito medesimo, in violazione degli artt. 13, par. 1, lett. b) e 37, par. 7, RGPD (provv. 11 settembre 2025, n. 483, doc. web n. 10177128 - cfr. par. 4.6).

4.8. *Ordini professionali*

Il Garante è intervenuto, a seguito di alcuni reclami e della notifica di *data breach* effettuata da un ordine regionale degli psicologi, su un sofisticato attacco *ransomware* messo in atto da un gruppo di cybercriminali. La violazione aveva comportato l'accesso abusivo alla rete informatica dell'ordine, la cifratura e l'esfiltrazione di numerosi documenti contenenti, in particolare, dati personali degli iscritti all'albo sottoposti a procedimenti disciplinari e di diversi pazienti, tra cui minori, e di altre persone a vario titolo coinvolte. L'attacco aveva riguardato anche dati appartenenti a categorie particolari, nonché dati relativi a condanne penali e reati, esponendo gli interessati a rischi di discriminazione, furto d'identità, frodi, rischi reputazionali e altri pregiudizi nella sfera economica e sociale. A seguito del mancato pagamento del riscatto, i cybercriminali avevano pubblicato sul *dark web* i dati esfiltrati. Non sono risultate, invece, compromesse la disponibilità e l'integrità dei dati personali, recuperati grazie alle procedure e ai sistemi di backup. Tenuto conto che l'ordine non aveva adottato misure adeguate a rilevare tempestivamente le violazioni dei dati e a garantire la sicurezza dei sistemi di trattamento, il Garante ha adottato un provvedimento sanzionatorio per la violazione degli artt. 5, par. 1, lett. f), e 32, par. 1, RGPD (provv. 29 aprile 2025, n. 271, doc. web n. 10134827; v. anche Newsletter 30 maggio 2025, doc. web n. 10135126).

A seguito di una segnalazione, l'Autorità ha appreso che su un sito web riconducibile a un ordine provinciale delle professioni infermieristiche era possibile accedere liberamente al pannello di controllo dei dati di tutti i professionisti iscritti e consultare o modificare i dati personali degli stessi. A seguito della successiva notifica di *data breach* e degli accertamenti istruttori svolti, era emerso che l'ordine non aveva adottato alcuna procedura di autenticazione informatica volta a garantire che soltanto le persone debitamente autorizzate potessero accedere al pannello di controllo in questione, che era, invece, liberamente accessibile da parte di chiunque fosse a conoscenza dell'URL del sito web riconducibile all'ordine, con la conseguente esposizione dei dati anagrafici e di contatto degli iscritti a possibili trattamenti illeciti. Il Garante ha, pertanto, adottato un provvedimento sanzionatorio nei confronti dell'ordine per la violazione degli artt. 5, par. 1, lett. f), e 32, par. 1, RGPD (provv. 23 giugno 2025, n. 362, doc. web n. 10161390).

Un diverso ordine provinciale delle professioni infermieristiche aveva, invece, pubblicato sul proprio sito web istituzionale una versione dell'albo professionale in cui comparivano l'indirizzo di residenza del reclamante e di tutti altri professionisti iscritti, a causa di un errore materiale commesso da un proprio dipendente, che aveva involontariamente pubblicato sul sito una versione dell'albo redatta per uso interno. Tenuto conto della delicatezza del dato personale relativo all'indirizzo di residenza degli iscritti, che può esporre gli stessi a rischi di frode, furto d'identità e aggressione, il Garante ha adottato un provvedimento sanzionatorio nei confronti dell'ordine, per la violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. e), e parr. 2 e 3, RGPD, nonché 2-*ter* del Codice (provv. 9 ottobre 2025, n. 585, doc. web n. 10192784).

In un altro caso, un ordine interprovinciale dei tecnici sanitari di radiologia medica e delle professioni sanitarie tecniche della riabilitazione e della prevenzione aveva annotato sull'albo da esso tenuto un provvedimento disciplinare di sospensione adottato nei

confronti di una professionista, nonostante quest'ultima lo avesse impugnato dinanzi alla competente commissione disciplinare, con conseguente sospensione dell'efficacia del provvedimento. Conseguentemente, l'ordine aveva dato luogo a una diffusione online dei dati personali della reclamante in maniera non conforme ai principi di liceità, correttezza, trasparenza ed esattezza ed in assenza di base giuridica. Ritenendo complessivamente violati gli artt. 5, par. 1, lett. a) e d), 6, par. 1, lett. c) ed e), RGPD, nonché 2-*ter* del Codice, il Garante ha adottato un provvedimento sanzionatorio nei confronti dell'ordine (provv. 9 ottobre 2025, n. 586, doc. web n. 10192819).

L'Autorità ha poi accertato, a seguito di un reclamo, che un ordine territoriale degli avvocati aveva pubblicato sul proprio sito web istituzionale un documento redatto dal locale tribunale, contenente un elenco di tredici procedimenti giudiziari penali, con il dettaglio del numero di fascicolo, degli estremi identificativi di diciotto imputati, dei nominativi di quattro avvocati difensori, dell'imputazione, dello stato del procedimento, della data di fissazione dell'udienza e del giudice competente. Pur considerando che la diffusione online di tali dati era avvenuta a causa di un mero errore umano nel difficile periodo della pandemia da SARS-CoV-2, il Garante, ritenuti violati gli artt. 5, par. 1, lett. a), 6, parr. 1, lett. c) ed e), 2 e 3, e artt. 10 del RGPD, nonché 2-*ter* e 2-*octies* del Codice, ha adottato un provvedimento sanzionatorio nei confronti dell'ordine (provv. 23 ottobre 2025, n. 625, doc. web n. 10196142).

4.9. *Digitalizzazione e banche dati pubbliche*

4.9.1. Vigilanza sulle banche dati pubbliche

Come già rappresentato nella Relazione 2024, per fronteggiare il grave fenomeno degli accessi abusivi alle banche dati pubbliche e della rivendita delle informazioni riservate ivi contenute, il Garante ha istituito una task force incaricata di verificare le misure di sicurezza tecniche e organizzative poste a tutela delle grandi banche dati pubbliche e individuare le azioni da intraprendere al fine di offrire maggiori garanzie in ordine agli accessi da parte del personale autorizzato (p.a. centrali e locali, forze di polizia, società, intermediari e altri soggetti privati) e alle operazioni di gestione e manutenzione delle stesse.

Nel corso del 2025, nell'ambito della predetta task force, sono state effettuate complesse attività istruttorie, anche attraverso impegnativi accertamenti ispettivi. In particolare, sono state esaminate le principali applicazioni in uso e i sistemi di cooperazione applicativa, soffermandosi sulle tipologie di operatori autorizzati (interni ed esterni), sulle procedure di gestione delle utenze e delle abilitazioni, sui sistemi di autenticazione informatica e di tracciamento delle operazioni eseguite, sui meccanismi di *alerting* attivati per rilevare comportamenti anomali o a rischio, sulle procedure di controllo poste in essere per verificare la liceità delle operazioni eseguite, nonché sulla gestione delle violazioni dei dati personali, anche con riferimento a quelle determinate da accessi abusivi.

Come negli anni passati, inoltre, in sede istruttoria sono state rilevate condotte aventi profili penali in relazione a ipotesi di accesso abusivo alle banche dati dell'Agenzia delle entrate e dell'INPS, con conseguente segnalazione e attività di collaborazione con l'autorità giudiziaria.

4.9.2. 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 2025 il

4

Sistema IT-Wallet

Garante ha proseguito la propria attività consultiva sugli atti volti a disciplinare la digitalizzazione dei servizi pubblici, la realizzazione e riorganizzazione di banche dati e l'utilizzo di piattaforme tecnologiche a supporto dell'attività amministrativa e istituzionale.

Uno dei principali temi affrontati dall'Autorità in sede consultiva è stato quello relativo al "Sistema di portafoglio digitale italiano - Sistema IT-Wallet" di cui all'art. 64-*quater*, d.lgs. n. 82/2005 (CAD), che, ai commi 3 e 5, prevede l'adozione di due d.P.C.M. attuativi. Il contributo fornito dall'Autorità ha consentito di rendere conformi i trattamenti di dati personali effettuati nel complesso contesto del Sistema IT-Wallet, anche tenuto conto del quadro normativo europeo, mutato per effetto del reg. (UE) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica il reg. (UE) 910/2014 (cd. reg. eIDAS) – nonché dei relativi regolamenti di esecuzione – introducendo, tra l'altro, il "Portafoglio europeo di identità digitale" (cd. EUDI-Wallet). In particolare, i profili oggetto di specifica attenzione hanno riguardato:

- la definizione dei ruoli nei trattamenti, con particolare riferimento all'individuazione della veste di responsabile del trattamento, ai sensi dell'art. 28 del RGPD, da parte dei "Fornitori di attestati elettronici di attributi" quando emettono tali attestati in relazione a informazioni per le quali non sono titolari di fonti autentiche (compreso l'Istituto Poligrafico e Zecca dello Stato S.p.A., cui spettano i compiti di rilascio e gestione degli attestati elettronici di attributi di interesse pubblico);
- l'adozione di misure che i "Fornitori di soluzioni IT-Wallet" e i "Fornitori di attestati elettronici di attributi" devono adottare a tutela dei diritti e delle libertà fondamentali degli interessati, impedendo trattamenti ulteriori (compresi quelli che comportano l'associazione con dati personali acquisiti mediante altri servizi), nonché attività di monitoraggio delle operazioni svolte dagli interessati medesimi con le proprie istanze IT-Wallet;
- la puntuale individuazione dei dati personali contenuti nell'attestato elettronico di dati di identificazione personale. Inoltre, gli schemi di decreto hanno previsto la definizione di misure tecniche e organizzative adeguate da adottarsi con un decreto del capo del Dipartimento per la trasformazione digitale presso la Presidenza del Consiglio dei ministri (cd. DTD), all'esito della valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, par. 10, RGPD, su cui il Garante sarà chiamato a pronunciarsi. Nel parere, complessivamente favorevole, il Garante ha tuttavia rilevato la necessità che siano sottoposti alla sua consultazione preventiva anche lo schema di regolamento dell'AgID in merito alle procedure amministrative necessarie alla registrazione al Sistema IT-Wallet (che andrà a disciplinare anche i requisiti di onorabilità delle persone fisiche di riferimento dei soggetti che intendono aderire al Sistema IT-Wallet) e il decreto che disciplinerà i trattamenti di dati personali connessi all'utilizzo dei servizi remunerabili.

In ogni caso, l'Autorità ha evidenziato la complessità dei trattamenti posti in essere nel contesto del Sistema IT-Wallet – caratterizzati dal coinvolgimento di numerosi soggetti, con vari ruoli e relativi ad aspetti delicati della vita delle persone, quali le attestazioni concernenti dati, prerogative, deleghe, caratteristiche, licenze o qualità degli interessati necessarie ai fini della fruizione di servizi online, anche in ambito pubblico – e, dunque, gli elevati rischi per i diritti e le libertà fondamentali degli interessati. Pertanto, considerato che gli schemi di decreti sottoposti ad esame prevedono comunque una prima fase di sperimentazione (nella quale sono sicuramente messi a disposizione, tramite la soluzione IT-Wallet pubblica, attestati elettronici di dati di identificazione personale e attestati elettronici di interesse pubblico), tenendo altresì conto che il Sistema IT-Wallet dovrà essere progressivamente coordinato con l'impianto giuridico e tecnologico di funzionamento dell'EUDI-Wallet, ancora in corso di definizione, il Garante, nel parere, ha richiesto al DTD di predisporre e trasmettere, alla conclusione della predetta sperimentazione, e comunque non oltre il 31 marzo 2026, una relazione

che indichi una serie di elementi, al fine di valutare l'adeguatezza delle garanzie adottate ed eventualmente l'introduzione di ulteriori cautele (provv. 4 agosto 2025, n 469, doc. web n. 10162651).

Piattaforma digitale nazionale dati - PDND

Nel 2025 l'Autorità è stata chiamata a pronunciarsi sullo schema delle linee guida sull'infrastruttura tecnologica della Piattaforma digitale nazionale dati per l'interoperabilità dei sistemi informativi e delle basi di dati (la cd. PDND), da adottarsi da parte dell'AgID ai sensi dell'art. 50-*ter*, comma 2, CAD, in una versione aggiornata rispetto alle linee guida del 2021 (su cui il Garante si era espresso con provv. 16 dicembre 2021, n. 433, doc. web n. 9732758). Posto che la PDND è un'infrastruttura di interoperabilità volta a favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto per finalità istituzionali dalle p.a., gestori di servizi pubblici e società a controllo pubblico, nonché la condivisione dei dati e delle informazioni tra i soggetti che hanno diritto di accedervi in conformità alla normativa vigente, la necessità di un aggiornamento delle linee guida è connessa all'introduzione di nuove funzionalità (ad es., oltre a quella di erogazione ordinaria, già presente a partire dal 2021, anche quelle di erogazione inversa e di distribuzione del segnale di variazione) nonché all'esigenza di chiarire taluni profili di funzionamento.

A quest'ultimo riguardo, anche su indicazione del Garante sulla base di alcune criticità emerse nel corso del tempo in relazione all'operatività concreta della PDND, è stato necessario precisare gli obblighi di sicurezza posti in capo agli aderenti, relativi alla prevenzione, rilevazione e gestione di accessi non autorizzati alle banche dati dell'erogatore. Infatti, l'utilizzo dell'infrastruttura PDND non muta gli obblighi che il RGPD e il Codice pongono in capo ai soggetti a vario titolo coinvolti nel trattamento circa le misure da adottare al fine di assicurare il rispetto dei principi di liceità e di integrità e riservatezza, nonché degli obblighi di sicurezza, in relazione, in particolare, agli accessi alle banche dati. Nel corso delle interlocuzioni sono state recepite anche altre osservazioni (quale quella concernente l'individuazione del gestore della piattaforma quale responsabile del trattamento del produttore con riferimento ai trattamenti effettuati ai fini della distribuzione dei segnali di variazione). Tutto ciò posto, il Garante ha espresso parere favorevole sullo schema di linee guida (provv. 21 maggio 2025, n. 283, doc. web n. 10142331).

PDND-OD - Osservatorio dati

Al Garante è stato sottoposto, su richiesta della Presidenza del Consiglio dei ministri, anche lo schema di d.P.C.M. di cui all'art. 50-*ter*, comma 4, del CAD, relativo alle modalità di messa a disposizione, all'interno della Piattaforma digitale nazionale dati - Osservatorio dati (cd. PDND-OD), dei dati aggregati e anonimizzati di cui sono titolari le p.a., gestori di pubblici servizi e società a controllo pubblico. Essendo state recepite, nel corso delle interlocuzioni informali intercorse con l'Ufficio, le osservazioni, in particolare, sull'adozione di garanzie concernenti l'aggregazione e l'anonimizzazione dei dati personali in tal modo messi a disposizione nella PDND-OD (anche con riferimento alle verifiche a campione effettuate dal DTD), il Garante ha espresso parere favorevole, evidenziando altresì come spetti al medesimo Dipartimento, tramite atto espresso, individuare i progetti per i quali richiedere i dati ai soggetti obbligati nonché comunicare al Garante i progetti per i quali la predetta anonimizzazione presenta un rischio elevato per i diritti e le libertà delle persone fisiche (provv. 25 settembre 2025, n. 526, doc. web n. 10184542).

Soggetti abilitati alla vendita di gas naturale a clienti finali

Il Ministero dell'ambiente e della sicurezza energetica ha chiesto un parere al Garante sullo schema di decreto direttoriale con cui vengono approvate le indicazioni operative in materia di elenco dei soggetti abilitati alla vendita di gas naturale a clienti finali di cui al decreto del Ministro dell'ambiente e della sicurezza energetica 19 maggio 2025, n. 85 e approvazione dell'elenco provvisorio dei soggetti abilitati, il modello di delega a operare sul portale elenco venditori e quello di comunicazione delle variazioni relative ai

requisiti di onorabilità delle persone fisiche con incarichi delle imprese di vendita, nonché l'elenco provvisorio dei soggetti abilitati alla vendita di gas naturale a clienti finali, ai sensi dell'art. 17 del d.lgs. n. 164/2000, e del decreto del Ministro dell'ambiente e della sicurezza energetica 19 maggio 2025, n. 85. Premesso che tali indicazioni operative presentano contenuti speculari rispetto alla circolare riferita all'elenco dei venditori di energia elettrica, allegata al decreto direttoriale 16 gennaio 2023, n. 1294 (cfr. provv. 21 dicembre 2022, n. 440, doc. web n. 9843415), il Garante si è pronunciato favorevolmente, anche in ragione del recepimento delle osservazioni informalmente fornite nel corso delle interlocuzioni riguardanti l'individuazione di garanzie per i diritti e le libertà degli interessati, tra le quali quelle sul trattamento di dati personali riferiti ai requisiti di onorabilità dichiarati e verificati (ovvero i dati personali relativi a condanne penali o reati di cui all'art. 10 del RGPD e all'art. 2-*octies* del Codice) (provv. 4 agosto 2025, n. 453, doc. web n. 10165075).

Patente a crediti per le imprese

L'Ispettorato nazionale del lavoro ha richiesto il parere del Garante sullo schema di decreto volto a disciplinare le modalità di ostensione delle informazioni concernenti la patente a crediti per le imprese e i lavoratori autonomi operanti nei cantieri temporanei o mobili, ai sensi dell'art. 2, comma 2, del decreto del Ministro del lavoro e delle politiche sociali n. 132/2024.

In sede istruttoria lo schema di decreto è stato modificato secondo le interlocuzioni informali intercorse, al fine di precisare, in particolare, il ruolo svolto dall'Ispettorato nell'ambito dei trattamenti in esame. Tuttavia, considerati i profili di criticità residui relativi, in particolare, alle funzioni crittografiche utilizzate per la per la conservazione delle password e alle garanzie volte ad assicurare l'immodificabilità e l'integrità dei file di log, il Garante ha ritenuto necessario formulare due condizioni, al fine di rendere i trattamenti disciplinati conformi alla normativa in materia di protezione dei dati personali e, in particolare, agli artt. 5, par. 1, lett. f), nonché 25 e 32 del RGPD (provv. 21 maggio 2025, n. 284, doc. web n. 10141315).

Condizionalità sociale

Il Ministero dell'agricoltura, della sovranità alimentare e delle foreste aveva trasmesso al Garante lo schema di protocollo volto a disciplinare i rapporti con il Ministero della salute, le regioni e province autonome, nonché l'Agenzia per le erogazioni in agricoltura (AGEA), al fine di favorire le procedure di interscambio delle informazioni necessarie per l'attuazione della cd. condizionalità sociale in agricoltura.

Nel corso dell'istruttoria, sono emersi profili di criticità (rilevati anche in sede di Conferenza Stato-Regioni) afferenti principalmente all'inidoneità della base giuridica a disciplinare i trattamenti prefigurati, atteso che le fonti normative europee e statali indicate dal Ministero non sono apparse idonee a fungere da base giuridica del trattamento in adempimento di un obbligo legale o in esecuzione di un compito di interesse pubblico, con particolare riguardo anche al trattamento di dati giudiziari (artt. 6, par. 3, e 10 del RGPD e 2-*ter* e 2-*octies* del Codice). È stata altresì evidenziata la necessità di un intervento sul piano della normativa in materia di condizionalità sociale volto, da un lato, a chiarire il ruolo delle regioni come autorità competenti, dall'altro gli elementi essenziali del trattamento, specificando i ruoli assunti dai vari soggetti coinvolti in tale contesto (tra cui, AGEA, le regioni e le ASL).

Di conseguenza, considerato che nell'ambito dell'attuale quadro regolatorio di settore sono risultati difettare gli elementi essenziali del trattamento richiesti dalla normativa in materia di protezione dei dati personali, l'Autorità (anche tenuto conto di analoghe precedenti istruttorie condotte - cfr. provv. 18 novembre 2024, n. 723, doc. web n. 10095723, cui ha fatto seguito il provv. 29 aprile 2025, n. 255, doc. web n. 10129880) ha formulato un parere condizionato al completamento del quadro normativo di settore attraverso una base giuridica idonea – nel sistema gerarchico delle fonti, nonché alla

luce dei principi del RGPD e del Codice – che specificamente disciplini gli elementi essenziali del trattamento (in osservanza di quanto previsto dagli artt. 5, par. 1, lett. a), 6, par. 3, nonché 9 e 10 del RGPD, nonché dagli artt. 2-*ter*, 2-*sexies* e 2-*octies* del Codice), richiedendo altresì la tempestiva comunicazione all'Autorità delle iniziative assunte in ordine alla completa definizione del predetto quadro giuridico (provv. 4 agosto 2025, n. 470, doc. web n. 10166305).

4.10. *La materia anagrafica*

Il Ministero dell'interno ha sottoposto all'Autorità lo schema di decreto ministeriale ai sensi dell'art. 62, comma 6-*bis*, d.lgs. n. 82/2005 recante la disciplina delle modalità di accesso ai servizi di certificazione resi disponibili dall'ANPR tramite la PDND, al fine di consentire ai notai di richiedere, attraverso la Rete unitaria del notariato (RUN) gestita dal Consiglio nazionale del notariato (CNN), per finalità connesse all'esecuzione dell'incarico professionale, i certificati anagrafici. Lo schema è stato corredato da un allegato e un disciplinare tecnico che ha individuato, in particolare, le misure di sicurezza e le modalità di tracciamento delle operazioni compiute nell'ambito dell'utilizzo del predetto servizio. Anche in questa occasione lo schema ha tenuto conto delle indicazioni fornite nel corso delle interlocuzioni intercorse con il Ministero dell'interno, concernenti, in particolare, la necessità di qualificare il Ministero quale soggetto "erogatore" dei servizi messi a disposizione tramite la PDND, nonché quella di indicare che l'estrazione del campione di notai su cui effettuare le verifiche relative alla sussistenza compete al Ministero e non al CNN.

Tuttavia, in considerazione dei profili di criticità residui, sono state formulate prescrizioni volte a conformare i trattamenti in questione alla disciplina in materia di protezione dei dati personali, con particolare riguardo alla necessità di precisare che il Ministero, in relazione ai trattamenti necessari alle verifiche sulla legittimità degli accessi dei notai, riveste il ruolo di titolare del trattamento, nonché specificare in cosa si sostanzi la valutazione che il CNN è chiamato ad effettuare sul campione di notai estratto per le predette verifiche, in conformità ai principi di liceità, correttezza e trasparenza, e *accountability* (artt. 5, par. 2, 6, par. 3, lett. b) e 24 del RGPD). È stato, altresì, richiesto di espungere dalle operazioni di tracciamento effettuate dal CNN i riferimenti all'identificativo ANPR del soggetto oggetto della consultazione, non essendo necessario trattare il predetto dato.

Inoltre, è stato ingiunto al Ministero dell'interno di trasmettere al Garante, trascorsi sei mesi dall'avvio del trattamento, una relazione sull'efficacia dei criteri e delle misure adottate, che evidenzi le eventuali criticità riscontrate, tenendo conto anche degli esiti delle attività di verifica poste in essere dal Ministero stesso e dai Consigli distrettuali competenti (provv. 4 giugno 2025, n. 314, doc. web n. 10149075).

Audit ANPR

Il Ministero dell'interno, in ottemperanza a quanto previsto dall'art. 62 del CAD, ha trasmesso le risultanze dell'audit annuale sull'ANPR. All'esito di tale attività è stata accertata la rispondenza delle misure di sicurezza adottate a quelle indicate da SOGEI S.p.A. – cui è affidata la gestione dell'infrastruttura ANPR – nel documento "*Assessment* sicurezza infrastruttura ANPR". Tale conformità è stata accertata anche con riguardo alla conformità delle procedure di sicurezza, oggetto di controllo a campione, con quelle previste nella valutazione di impatto sulla protezione dei dati personali. L'attività di controllo effettuata dal Ministero ha messo in luce alcune difformità lievi, con riguardo alla modalità di implementazione dei tempi di conservazione che il fornitore si è impegnato a superare. In conclusione, le attività controllate sono risultate conformi ai requisiti previsti, con esito positivo dell'audit.

CIE-Agenda Online

A seguito di un reclamo, il Garante ha adottato un provvedimento sanzionatorio nei confronti del Ministero dell'interno in relazione al trattamento di dati personali effettuato mediante il servizio denominato CIE-Agenda Online, che consente ai cittadini di prenotare l'appuntamento presso un comune per la richiesta della carta di identità elettronica (CIE).

Nel caso specifico, il reclamante aveva fissato un appuntamento accedendo al sistema tramite SPID, e a fine processo aveva visualizzato una schermata di riepilogo dalla quale aveva rilevato che, nonostante i dati rilevati da SPID fossero corretti, tra i dati di contatto era risultato un indirizzo e-mail a lui sconosciuto. Dagli accertamenti svolti dall'Istituto Poligrafico dello Stato per conto del Ministero sul sistema CIE-Agenda Online, era emerso che l'indirizzo e-mail associato all'account del reclamante corrispondeva a quello di un dipendente comunale che aveva supportato il reclamante nel fissare l'appuntamento, utilizzando erroneamente la procedura riservata ai cittadini, anziché quella per gli operatori, e inserendo, quale dato di contatto, il proprio indirizzo e-mail in luogo di quello dell'utente. All'epoca dei fatti, la durata della conservazione dei dati personali nel sistema CIE-Agenda Online, era stata fissata in due anni dalla data della registrazione dell'account o dell'ultimo appuntamento fissato. Verificando la tempistica dei fatti oggetto del reclamo, non essendo trascorsi due anni, i dati del reclamante risultavano ancora conservati nel profilo utente, riproducendo l'errore originario.

L'istruttoria aveva evidenziato che, nella vicenda oggetto del reclamo, le impostazioni del sistema di prenotazione implementate dal Ministero avevano comunque svolto un ruolo rilevante. La previsione di tempi lunghi di conservazione dei dati e delle utenze, che restavano attive anche successivamente alla data degli appuntamenti, scaduti o cancellati, financo successivamente al rilascio della CIE, anche in assenza di un errore umano come quello sopra indicato, comportavano comunque il rischio di riproporre dati obsoleti (per es. indirizzi di posta elettronica e numeri di telefono non più attivi o non più utilizzati dall'utente), pregiudicando il raggiungimento delle finalità sottese alla raccolta dei dati di contatto ed indicate nella base giuridica, ovvero quella di ricevere comunicazioni inerenti allo stato di avanzamento del processo di rilascio della CIE (d.m. 23 dicembre 2015, all. b). Nell'ambito dell'istruttoria era stato inoltre accertato che, all'epoca dei fatti in esame, il sistema CIE-Agenda Online conservava l'utenza creata in occasione della richiesta di un appuntamento anche successivamente alla spedizione o al ritiro del documento da parte del cittadino, unitamente allo storico di tutti gli appuntamenti fissati dall'interessato. La conservazione dei dati era stata stabilita in due anni dalla data di registrazione al servizio o dell'ultimo appuntamento. Il Garante ha ritenuto non proporzionata e adeguata alle finalità previste la scelta di prevedere obbligatoriamente la creazione di un account, nonché quella di conservare i dati delle prenotazioni anche successivamente all'appuntamento, soprattutto con riguardo a quelle cancellate o scadute. Parimenti, è stato ritenuto non proporzionato alle finalità perseguite il termine di conservazione di due anni dei predetti dati. Difatti, i dati raccolti all'atto della richiesta dell'appuntamento, in conformità al principio di liceità, correttezza e trasparenza, avrebbero dovuto essere utilizzati esclusivamente per le finalità di gestione dello stesso, o di eventuali contestazioni, e, in applicazione del principio di limitazione della conservazione, essere cancellati trascorso un tempo adeguato dalla data prevista per l'appuntamento. Oltre a ciò, la conservazione dell'intero storico degli appuntamenti cancellati dall'utente, anche oltre i predetti termini, è stata ritenuta non conforme al principio di limitazione delle finalità. Infine, il Garante ha ritenuto che la possibilità di creare un'utenza avrebbe dovuto essere lasciata facoltativamente all'interessato, in vista di eventuali utilizzi successivi.

Per tali motivi, il Ministero dell'interno è stato sanzionato per aver effettuato i trattamenti in violazione degli artt. 5, par. 1, lett. a), b) ed e), e 6 del RGPD (provv. 27 febbraio 2025, n. 116, doc. web n. 10126141).

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

Anche nel corso 2025, l'Autorità si è occupata dell'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.

A seguito di una notizia di stampa, l'Autorità ha avviato un'istruttoria nei confronti di una società strumentale di un comune, che, al fine di rilevare i flussi di traffico veicolare nel proprio territorio, aveva sviluppato uno strumento di IA per rendere più efficiente la raccolta dei dati e consentire l'analisi in tempo reale dei filmati ottenuti da due telecamere mobili installate sulla pubblica via. Nel ribadire che anche l'acquisizione e la temporanea memorizzazione di dati personali, come l'immagine del volto ripresa da dispositivi video, costituisce un trattamento di dati personali, il Garante ha evidenziato che, sebbene i volti e i numeri di targa fossero stati oscurati, i dati raccolti non potevano comunque considerarsi anonimi. È stato, inoltre, accertato che la società non aveva garantito un sufficiente livello di trasparenza del trattamento nei confronti degli interessati e non aveva provato di aver svolto una previa valutazione di impatto sulla protezione dei dati. Ritenuti violati gli artt. 5, par. 1, lett. a), 12, par. 1, 13, e 35 del RGPD, il Garante ha adottato un provvedimento sanzionatorio nei confronti della società (provv. 10 aprile 2025, n. 202, doc. web n. 10140338; cfr. par. 4.7).

Sempre a seguito di notizie di stampa, il Garante si è occupato di un progetto posto in essere da una provincia – quale contitolare del trattamento assieme ad un'altra provincia – che aveva previsto l'impiego di telecamere dotate di funzionalità di lettura automatizzata delle targhe dei veicoli in transito ed estrazione di informazioni utili per l'analisi dei flussi di traffico, consentendo di orientare le scelte amministrative in materia. Il Garante, affermata la natura di dati personali delle informazioni trattate nell'ambito del progetto in questione, e ravvisata la mancanza di un'idonea base giuridica che potesse giustificare il trattamento delle stesse, ha accertato che la provincia non aveva stipulato un accordo di contitolarità del trattamento con l'altra provincia coinvolta nel progetto, e, a fronte della complessiva violazione degli artt. 5, par. 1, lett. a) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 21, par. 4, 26 e 35 del RGPD, ha ritenuto di adottare un provvedimento sanzionatorio nei confronti dell'ente (provv. 25 settembre 2025, n. 532, doc. web n. 10223383).

A seguito di una segnalazione su di una questione similare, è emerso che un comune aveva attivato un sistema di videosorveglianza per la tutela della cosiddetta sicurezza urbana, stipulando con la prefettura territorialmente competente uno specifico patto per l'attuazione della sicurezza urbana (v. artt. 4 e 5, comma 2, lett. a), d.l. n. 14/2017). Tale patto faceva, tuttavia, riferimento, in modo generico, ad aree molto ampie del territorio comunale, senza indicare il numero complessivo di telecamere attivate e gli specifici siti d'installazione delle stesse, non essendo state, pertanto, effettuate specifiche valutazioni, unitamente alle competenti autorità di pubblica sicurezza, in merito all'effettiva necessità e proporzionalità del trattamento. Nell'impossibilità di ricondurre effettivamente l'impiego di tali dispositivi all'ambito della sicurezza urbana, il Garante ha ritenuto che i connessi trattamenti di dati fossero sprovvisti di un'idonea base giuridica. Tenuto conto che il comune non aveva neanche assicurato un sufficiente livello di trasparenza nei confronti degli interessati, né condotto una valutazione di impatto sulla protezione dei dati prima di dare avvio al trattamento e aveva omesso di fornire un tempestivo riscontro a una richiesta d'informazioni rivoltagli dall'Autorità, lo stesso è stato destinatario di un provvedimento sanzionatorio per la violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) ed e), 12, par. 1, 13 e 35 del RGPD, nonché 2-*ter* e

157 del Codice (provv. 13 novembre 2025, n. 669, doc. web n. 10198694).

In un altro caso di analoga natura, il Garante ha adottato un provvedimento sanzionatorio nei confronti di un comune per avere installato alcune telecamere di videosorveglianza sulla pubblica via per la tutela della cosiddetta sicurezza urbana, e due dispositivi video dotati di funzionalità di lettura automatica delle targhe dei veicoli in transito per fini di sicurezza stradale e controllo della circolazione dei veicoli, senza, tuttavia, aver rispettato i requisiti e i limiti previsti dalla disciplina di settore, con un insufficiente livello di trasparenza nei confronti degli interessati e in assenza di una previa valutazione di impatto sulla protezione dei dati (provv. 23 novembre 2025, n. 628, doc. web n. 10196164; cfr. par. 13.3.1.3).

A seguito di un reclamo, è stata avviata un'istruttoria nei confronti di un comune, che, nel corso del procedimento, è stato destinatario di un provvedimento correttivo e sanzionatorio per non aver fornito pieno e tempestivo riscontro alle richieste d'informazioni rivoltegli dall'Autorità, con conseguente violazione dell'art. 157 del Codice (provv. 13 febbraio 2025, n. 68, doc. web n. 10114785). Successivamente, in sede di valutazione del merito della questione oggetto di reclamo, è stato accertato che il comune aveva attivato un sistema di videosorveglianza sulla pubblica via, dotato anche di funzionalità di lettura automatizzata delle targhe dei veicoli in transito, in assenza dei necessari presupposti di liceità. In particolare, l'ente, pur avendo stipulato con la prefettura territorialmente competente un cosiddetto patto per l'attuazione della sicurezza urbana, non aveva ivi indicato il numero di telecamere di videosorveglianza costituenti l'impianto, le funzionalità e le specifiche aree del territorio comunale sottoposte a videosorveglianza, in violazione pertanto della disciplina di settore. L'ente non aveva, inoltre, assicurato un sufficiente livello di trasparenza nei confronti degli interessati, aveva omesso di svolgere una previa valutazione di impatto sulla protezione dei dati e non aveva comprovato di aver stipulato, in data certa, i necessari accordi sulla protezione dei dati con i fornitori esterni affidatari della manutenzione del sistema, quali responsabili del trattamento. Inoltre il medesimo ente aveva opposto un diniego alla richiesta della reclamante di poter esercitare il diritto di accesso a propri dati personali contenuti in un filmato di videosorveglianza, sul presupposto che la stessa non avesse fornito un'adeguata motivazione, come previsto da un regolamento comunale, che erroneamente equiparava le istanze di esercizio del diritto di accesso ai documenti amministrativi a quelle di esercizio del diritto di accesso ai propri dati personali di cui all'art. 15 del RGPD, per le quali non è necessario indicare alcuna motivazione. Da ultimo, è stato contestato al titolare il mancato pieno adempimento alle prescrizioni impartite con il citato provvedimento del 13 febbraio 2025, con la conseguente necessità di adottare ulteriori misure correttive, tra cui anche la limitazione del trattamento in corso e la cancellazione dei dati relativi ai numeri di targa già raccolti. A fronte della complessiva violazione degli artt. 5, par. 1, lett. a), 6, parr. 1, lett. c) ed e), 2, 3, 12, 13, 15, 28, 35 e 58, par. 1, RGPD, nonché 2-*ter* e 157 del Codice, il Garante ha adottato un provvedimento correttivo e sanzionatorio nei confronti dell'ente (provv. 4 dicembre 2025, n. 730, doc. web n. 10213467).

Un diverso comune, coinvolto in un'istruttoria originata da un reclamo, aveva invece installato numerose telecamere, di cui tre dotate di un sistema di lettura automatizzata delle targhe dei veicoli in transito, connesso con le banche dati della motorizzazione civile, per la verifica in tempo reale della copertura assicurativa, della revisione periodica e della classe ambientale dei veicoli, senza, tuttavia, aver rispettato i requisiti e i limiti previsti dalla disciplina di settore. L'ente aveva, inoltre, impiegato i medesimi dispositivi per finalità di sicurezza urbana, ma senza aver previamente stipulato il patto sopra ricordato per l'attuazione della sicurezza urbana con la prefettura territorialmente competente. Al riguardo, il Garante ha ribadito la necessità della stipula di tali patti,

quale condizione per poter attivare qualsiasi impianto di videosorveglianza comunale finalizzato alla prevenzione e al contrasto dei fenomeni di criminalità diffusa e predatoria, indipendentemente dalla circostanza che si tratti o meno di progetti di sicurezza integrata tra comuni e autorità di pubblica sicurezza. Dall'istruttoria è, altresì, emerso che il comune aveva trasmesso alla regione di appartenenza alcuni dati aggregati sui flussi di traffico rilevati, sebbene questi fossero raccolti a monte in assenza di un'idonea base giuridica e i finanziamenti regionali riguardassero il diverso ambito del controllo dei flussi di traffico per la tutela dell'ambiente. Nel ribadire la necessità di tenere distinte le varie finalità di trattamento perseguite mediante stessi dispositivi video, individuando per ciascuna di esse un'idonea base giuridica, il Garante, rilevato che il comune non aveva assicurato un sufficiente livello di trasparenza nei confronti degli interessati, non aveva svolto una previa valutazione di impatto sulla protezione dei dati e non aveva fornito riscontro a un'istanza dell'interessata di esercizio del diritto di cancellazione dei dati, ha adottato un provvedimento correttivo sanzionatorio nei confronti dell'ente, stante la violazione degli artt. 5, parr. 1, lett. a), 6, parr. 1, lett. c) ed e), 2 e 3, 12, parr. 1, 3 e 4, 13 e 35 del RGPD, nonché 2-*ter* del Codice, ordinando, in particolare, allo stesso di effettuare una ricognizione di tutte le telecamere installate sul proprio territorio per valutarne finalità e basi giuridiche del trattamento (provv. 18 dicembre 2025, n. 752, doc. web n. 10213486).

5 La sanità

Nel 2025 è proseguita un'intensa attività istruttoria e consultiva nel settore sanitario.

L'attività consultiva si è confermata centrale, con 28 pareri resi su schemi di decreti ministeriali e regolamenti in ambito sanitario, prevalentemente favorevoli, volti a garantire un equo bilanciamento tra diritti fondamentali nonché l'attuazione dell'innovazione tecnologica nel rispetto dei principi di *privacy by design*, di minimizzazione dei dati, liceità e trasparenza e di *accountability*.

Parallelamente, l'attività istruttoria, effettuata anche con accertamenti ispettivi, ha evidenziato criticità ricorrenti nella gestione dei dossier sanitari aziendali, nelle procedure di identificazione dei pazienti, nella comunicazione e diffusione dei dati sanitari e nella prevenzione degli accessi abusivi ai sistemi informativi sanitari.

5.1. *La sanità digitale*

La sanità digitale si è confermata nel 2025 un settore di assoluta rilevanza strategica per la protezione dei dati personali caratterizzato da un'intensa attività del Garante volta ad accompagnare la transizione digitale del SSN nel rispetto dei diritti fondamentali degli interessati. Si è potuto constatare un'accelerazione significativa dell'attuazione dei progetti previsti dal PNRR, con particolare riferimento alle infrastrutture digitali sanitarie e ai sistemi informativi centrali.

L'Autorità ha operato attraverso una molteplicità di strumenti: pareri preventivi su schemi normativi, verifiche ispettive, provvedimenti correttivi e sanzionatori, sempre fornendo indicazioni puntuali e funzionali ad assicurare, in tale particolare settore, la rigorosa applicazione della normativa in materia di protezione dati.

5.1.1. Il Fascicolo sanitario elettronico (FSE) e l'Ecosistema dati sanitari (EDS)

Il FSE ha continuato a rappresentare uno snodo cruciale della sanità digitale, caratterizzato da numerosi interventi normativi volti a perfezionarne l'assetto regolamentare. Con parere 23 giugno 2025, il Garante ha espresso una valutazione favorevole sullo schema di decreto di modifica del decreto 7 settembre 2023, che ha introdotto una proroga delle fasi transitorie della disciplina di attuazione del FSE (I fase al 30 giugno 2025, II fase al 31 dicembre 2025) e previsto di integrare i servizi di notifica delle operazioni sul FSE già in uso (applicazione per dispositivi mobili, invio e-mail) anche con il punto di accesso telematico di cui all'art. 64-*bis* del CAD (app IO) nel rispetto delle specifiche misure previste dalle linee guida sul punto di accesso telematico (app IO) (provv. 23 giugno 2025, n. 360, doc. web n. 10161000).

FSE 2.0 - PSS

L'introduzione di fasi transitorie della disciplina sul FSE ha concluso le attività istruttorie avviate dall'Ufficio nei confronti di tutte le regioni e province autonome in merito alle difformità riscontrate sul territorio nazionale circa l'attuazione delle garanzie a tutela dei dati personali previste nella normativa sul FSE. Le interlocuzioni intercorse con gli enti nazionali e locali coinvolti e i successivi interventi normativi hanno evidenziato che allo stato non era consentito alle regioni/province autonome la

realizzazione di tutte le componenti (es. profilo sanitario sintetico - PSS) e le funzionalità (es. delega) del FSE 2.0, ed anche di garantire tutti i contenuti informativi previsti dal decreto 7 settembre 2023 nonché il raggiungimento delle diverse finalità perseguibili, sulle quali ha avuto un significativo impatto anche l'adozione della disciplina sull'EDS (es. finalità di governo e di profilassi internazionale).

I più recenti interventi normativi hanno consolidato alcuni istituti giuridici propri della disciplina sul FSE 2.0, come quelli relativi all'identificazione dell'assistito, alla titolarità dei trattamenti e all'accesso in emergenza. In particolare, per quanto concerne le modalità di identificazione, nelle more dell'attivazione dell'ANA, l'anagrafe degli assistiti del Sistema TS deve costituire – per espressa previsione legislativa – l'unica base dati di riferimento per l'identificazione dell'assistito ai fini del FSE, non potendo le regioni/province autonome avvalersi delle anagrafi aziendali o regionali.

In merito alla titolarità dei trattamenti effettuati attraverso il FSE 2.0, in coerenza con gli orientamenti dell'Ufficio, la Corte di cassazione, con sentenza 15 ottobre 2025, n. 27558, ha ribadito che la titolarità dei trattamenti effettuati attraverso il FSE è espressamente prevista dal quadro normativo di settore, al quale le regioni e province autonome devono attenersi, essendo alle stesse preclusa la possibilità di attribuzioni diverse da quelle *ex lege* (v. anche linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del RGPD, EDPB, 7 luglio 2021, punto 24).

Con riferimento ai ruoli del trattamento, in armonia con le posizioni dell'Autorità, la Corte di cassazione con sentenza 6 marzo 2025, n. 6067 ha altresì ribadito il dovere del titolare di esercitare tutte le sue prerogative a tutela dell'utilizzo dei dati custoditi nei FSE, non ricorrendo alcuna causa di esenzione da responsabilità nei riguardi del titolare medesimo.

In merito all'accesso al FSE 2.0 cd. in emergenza, l'art. 20 del decreto 7 settembre 2023 prevede che, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato e di rischio grave, imminente ed irreparabile per la sua salute o incolumità fisica i sanitari possano consultare il FSE anche di un paziente che non abbia prestato il consenso, accedendo prioritariamente al PSS e, ove necessario, agli ulteriori dati e documenti del FSE che non siano stati oscurati, per il tempo strettamente necessario ad assicurare allo stesso le cure e fino a quando non sia nuovamente in grado di esprimere la propria volontà.

Parallelamente all'esame della disciplina transitoria del FSE 2.0, con parere 4 giugno 2025, l'Autorità si è espressa favorevolmente anche sullo schema di decreto concernente i contenuti informativi del profilo sanitario sintetico (PSS), ovvero quella partizione del FSE volta a sintetizzare le informazioni sanitarie essenziali dell'assistito. Il decreto individua i campi obbligatori e facoltativi del PSS e quelli che saranno compilati attraverso i servizi resi dall'EDS non modificando la tipologia delle informazioni trattate attraverso il PSS, né le misure poste a garanzia dei diritti e delle libertà degli interessati previste nei decreti sul FSE 2.0 e sull'EDS (provv. 4 giugno 2025, n. 316, doc. web n. 10148622).

L'esigenza di superare le difficoltà relative alla compilazione del PSS da parte dei medici di medicina generale/pediatri di libera scelta (MMG/PLS) è stata coniugata con un complesso di misure di garanzia da ritenersi appropriate a tutelare i diritti fondamentali e gli interessi delle persone fisiche coinvolte nelle operazioni di trattamento dei dati personali.

Con parere 13 novembre 2025, il Garante si è espresso sullo schema di decreto del MEF, di concerto con il Ministero della salute e il Sottosegretario di Stato alla Presidenza del Consiglio dei ministri con delega all'innovazione tecnologica, concernente il Portale nazionale FSE. Il Portale sarà caratterizzato da una sezione pubblica che fornirà a chiunque servizi informativi sul FSE (con trattamento limitato ai dati di navigazione e cookie) e una

sezione privata (accessibile da parte dell'assistito mediante l'utilizzo della propria identità digitale) volta a garantire all'assistito senza regione di assistenza (RdA) di accedere a specifiche funzionalità (es. informativa, gestione dei consensi, diritto di oscuramento) (provv. 13 novembre 2025, n. 665, doc. web n. 10196797). Lo schema di decreto è risultato coerente con la disciplina del Portale nazionale FSE e quella del FSE 2.0 e dell'EDS, anche con riferimento all'attribuzione dei ruoli del trattamento, assicurando agli assistiti senza RdA le medesime garanzie poste a tutela degli assistiti con RdA.

Con specifico riferimento all'EDS, con parere 27 marzo 2025, l'Autorità si è espressa sullo schema di decreto che modifica il decreto 31 dicembre 2024, introducendo alcune modifiche allo scopo di garantire un complessivo miglioramento tecnico-funzionale attraverso una diversa modalità di archiviazione dei dati in chiaro, basata non più sulla regione di erogazione (RdE) della prestazione sanitaria, ma su quella di assistenza (RdA) (provv. 27 marzo 2025, n. 164, doc. web n. 10131261). In particolare, è stato ritenuto necessario integrare l'articolato e l'all. c) al decreto dell'EDS al fine di assicurare la cooperazione delle Unità di archiviazioni regionali per un corretto allineamento dei dati.

5.1.2. Piattaforma nazionale di telemedicina (PNT)

Con parere 16 gennaio 2025, l'Autorità si è espressa sullo schema di decreto, di cui alla Missione 6 salute del PNRR, che disciplina i trattamenti di dati personali effettuati attraverso Piattaforma nazionale di telemedicina (PNT) e le relative articolazioni regionali (IRT); trattasi di una Piattaforma che si propone di offrire servizi minimi di telemedicina alle regioni e province autonome che intendano avvalersene, ferma restando, dunque, la facoltà delle stesse di erogare prestazioni di telemedicina con modalità diverse nel rispetto della disciplina sulla protezione dei dati personali e di quella di settore (provv. 16 gennaio 2025, n. 2, doc. web n. 10105743).

Lo schema di decreto supera il rilievo formulato dall'Autorità nel 2023 in quanto prevede che i trattamenti dei dati personali effettuati dalla PNT per finalità diverse da quelle di diagnosi, cura e riabilitazione descritti nelle linee guida per i servizi di telemedicina del 2022 siano sospesi fino all'aggiornamento delle medesime con decreto da adottare previo parere del Garante.

Infrastruttura nazionale di telemedicina (INT)

Su richiesta del Garante, è stato specificato che, per assicurare la piena operatività dei servizi minimi di telemedicina che necessitano di interoperabilità tra IRT di regioni o province autonome diverse da quella di assistenza, la infrastruttura nazionale di telemedicina (INT), per mezzo di uno specifico modulo a disposizione delle strutture, assicura, senza meccanismi di persistenza di dati, l'interoperabilità delle IRT interessate, al fine di garantire la trasmissione dei dati, immagini e documenti, nel rispetto delle misure di sicurezza che sono state indicate nell'allegato.

In coerenza con le disposizioni in materia di protezione dei dati personali previste nella disciplina sul FSE 2.0 e sull'EDS, le IRT delle RdE consentono, previo consenso dell'assistito, l'erogazione dei servizi di telemedicina e la conseguente generazione di dati e documenti che saranno poi conferiti al FSE e all'EDS. Tali dati personali potranno essere consultati, attraverso il FSE o l'EDS, dai professionisti sanitari solo se l'interessato preso in cura avrà manifestato i consensi previsti dalla disciplina sul FSE 2.0 e sull'EDS.

Quale ulteriore garanzia lo schema di decreto ha previsto per fini di cura esclusivamente servizi di consultazione dei dati e non di estrazione, allo scopo di superare i rilievi mossi dall'Autorità con riferimento al fatto che l'estrazione dei dati da parte del professionista sanitario avrebbe potuto vanificare il diritto di oscuramento eventualmente esercitato dall'interessato sui dati del FSE in un momento successivo all'estrazione dei dati da parte di tale professionista. Analoghe perplessità erano state manifestate con riferimento alla eventuale revoca del consenso dell'interessato.

Con specifico riferimento ai servizi resi disponibili dalla PNT per finalità di governo, lo schema di decreto ha superato la preliminare visione della PNT, e in particolare della INT, quale banca dati in cui far confluire i dati estratti dall'EDS relativi alle prestazioni rese in telemedicina. Tale visione avrebbe comportato una duplicazione, nella PNT/INT, dei dati relativi alle prestazioni di telemedicina già presenti in EDS, con specifici rischi legati all'aggiornamento, all'esattezza dei dati e delle manifestazioni di volontà dell'interessato relative all'oscuramento e alla revoca del consenso. Su indicazione dell'Autorità, è stata pertanto modificata l'impostazione iniziale prevedendo, nello schema in esame, che i dati personali siano conservati in EDS e non siano duplicati in INT, e che i servizi di elaborazione dei dati siano effettuati, su richiesta delle predette istituzioni, non più da INT bensì da EDS che fornirà alle stesse dati pseudonimizzati estratti secondo le caratteristiche richieste. Al riguardo, su richiesta dell'Autorità, è stata inserita nello schema di decreto una specifica garanzia per il rispetto dei principi di aggiornamento, esattezza e correttezza dei dati: le predette istituzioni potranno estrarre i dati elaborati da EDS con una frequenza massima di una volta nelle ventiquattro ore e conservarli per non più di ventiquattro ore dall'estrazione, dopo di che i dati estratti dovranno essere cancellati in modo sicuro e definitivo.

In merito ai trattamenti effettuati dall'Agenzia nazionale per i servizi sanitari regionali (AGENAS) attraverso la PNT, in coerenza con il quadro normativo in materia di protezione dei dati personali e delle disposizioni di settore, è stato specificato che l'accesso sarà consentito ai soli dati privati degli elementi identificativi diretti, pseudonimizzati in modo irreversibile, nonché a dati aggregati, in modo automatico, senza intervento umano e con una frequenza massima di una volta nelle ventiquattro ore. Sono state poi previste ulteriori misure di garanzia: nello specifico, il personale dell'AGENAS che, per altre finalità, accede a flussi di dati pseudonimizzati, non potrà accedere ai dati messi a disposizione dai servizi dell'EDS per finalità di governo, e i predetti dati saranno conservati da AGENAS per non più di ventiquattro ore dall'estrazione e successivamente cancellati in modo sicuro e definitivo.

In considerazione delle funzioni e dei compiti attribuiti dall'art. 12, comma 15-*undecies*, lett. g) e h) e dal comma 15-*duodecies*, d.l. n. 179/2012, AGENAS è stato considerato titolare dei trattamenti effettuati dalla INT, mentre la titolarità dei trattamenti svolti dalle IRT è stata attribuita alle regioni e alle province autonome. I titolari delle IRT sono tenuti a fornire all'interessato l'informativa relativa ai trattamenti effettuati, che sarà ad ogni buon conto pubblicata sul portale web dedicato e messa a disposizione dell'assistito in fase di autenticazione e accesso alla IRT. Su proposta dell'Autorità, è stato inoltre previsto che, al fine di garantire all'interessato informazioni omogenee e uniformi nel territorio nazionale, AGENAS predisponga, in collaborazione con le regioni e province autonome, un modello di informativa per i trattamenti svolti mediante le IRT da rendere disponibile sull'area pubblica del portale web dedicato. Su tale modello, e sui successivi aggiornamenti, è stata prevista l'acquisizione del preventivo parere del Garante (art. 5, comma 5 dello schema di decreto).

5.1.3. I sistemi informativi sanitari centrali

Nel 2025 l'attività consultiva del Garante ha riguardato numerosi sistemi informativi sanitari centrali con riferimento ai quali è stata prestata particolare attenzione alla coerenza con il quadro normativo europeo e nazionale in materia di protezione dei dati personali.

SIAP - NSIS

Con parere favorevole 4 giugno 2025, il Garante ha esaminato lo schema di decreto sul Sistema informativo per l'assistenza primaria (SIAP), alimentato con i dati non direttamente identificativi forniti dalle regioni e dalle province autonome relativi alle attività e alle prestazioni erogate nell'ambito dell'assistenza sanitaria di base, al fine di

consentire il monitoraggio e la programmazione delle attività e delle prestazioni erogate, nonché il monitoraggio dei livelli essenziali e uniformi di assistenza. L'Ufficio, al riguardo, ha verificato che il sistema di interconnessione del SIAP con il Nuovo sistema informativo del Ministero della salute (NSIS) fosse in conformità a quanto previsto dall'art. 3 del decreto n. 262/2016, secondo cui ad ogni assistito è assegnato, da parte della regione o della provincia autonoma inviante, un codice univoco non invertibile (CUNI) – che non consente alcuna correlazione immediata con i dati anagrafici – e che il Ministero della salute, in fase di acquisizione dei dati, effettuasse la generazione ed assegnazione del codice univoco nazionale dell'assistito (CUNA) agli assistiti rappresentati dal CUNI attraverso la diretta sostituzione del codice identificativo non invertibile ricevuto (provv. 4 giugno 2025, n. 315, doc. web n. 10149310).

Lo schema di decreto tiene conto delle osservazioni formulate nell'ambito delle interlocuzioni intercorse con il Ministero della salute che hanno riguardato in particolare: l'ambito di accesso ai dati del SIAP in forma aggregata; la necessità di prevedere una modalità di trasmissione sicura dei dati dall'assistenza di base alle regioni/province autonome; l'assenza di campi a compilazione libera; il rafforzamento del monitoraggio degli eventi di sicurezza e gestione di possibili incidenti oltre che mediante l'utilizzo di SIEM (*Security Information and Event Management*) anche attraverso il SOAR (*Security Orchestration, Automation and Response*); la necessità che i file di log debbano possedere caratteristiche di integrità e inalterabilità, essere protetti con idonee misure contro ogni uso improprio ed essere accessibili solo a personale opportunamente incaricato e autorizzato; l'introduzione di misure idonee ad attenuare il rischio connesso all'utilizzo fraudolento di identità digitali, suscettibili di comportare accessi abusivi e non autorizzati; l'adozione di misure di conservazione delle password con funzioni crittografiche (es. MD5, SHA 1, Argon2id, PBKDF2) (cfr. provv. 7 dicembre 2023, n. 594, doc. web n. 9962283 - linee guida per la conservazione delle password).

SIOC

Analoga valutazione favorevole è stata espressa con parere 23 giugno 2025 sullo schema di decreto relativo al Sistema informativo per il monitoraggio degli ospedali di comunità (SIOC), alimentato con i dati non direttamente identificativi forniti dalle regioni e dalle province autonome relativi alle prestazioni erogate dagli ospedali di comunità, alle motivazioni e alle caratteristiche dell'episodio di cura, al fine di consentire il monitoraggio delle prestazioni erogate dagli ospedali di comunità, nonché dei livelli essenziali e uniformi di assistenza (provv. 23 giugno 2025, n. 359, doc. web n. 10160983).

Come per il SIAP, anche per il SIOC il sistema di interconnessione con il NSIS è in conformità all'art. 3 del citato decreto n. 262/2016 (CUNI/CUNA). Lo schema di decreto tiene conto delle osservazioni formulate dall'Autorità nell'ambito delle interlocuzioni intercorse con il Ministero della salute che hanno riguardato in particolare: l'ambito di accesso ai dati del SIOC in forma aggregata; la necessità di prevedere una modalità di trasmissione sicura dei dati dal livello regionale/provinciale; l'assenza di campi a compilazione libera; il rafforzamento del monitoraggio degli eventi di sicurezza e gestione di possibili incidenti e l'introduzione di misure idonee ad attenuare il rischio connesso all'utilizzo fraudolento di identità digitali, come per il SIAP.

ANA

Con parere 23 ottobre 2025, il Garante si è espresso sullo schema di decreto concernente l'aggiornamento dell'anagrafe degli assistiti (ANA), già disciplinata dal d.P.C.M. 1° giugno 2022, per corrispondere a nuove esigenze informative, di sicurezza e alla necessità di realizzare ulteriori servizi per le finalità previste dalla legislazione in materia sanitaria (provv. 23 ottobre 2025, n. 623, doc. web n. 10195312).

Anche in tale circostanza lo schema di decreto e i relativi allegati tengono conto delle osservazioni espresse dall'Autorità che hanno riguardato, in particolare, l'ambito di

applicazione del decreto, al fine di limitare le integrazioni solo a quelle previste dall'art. 19, comma 2, d.P.C.M. 1° giugno 2022, e la valutazione circa la proporzionalità dei trattamenti effettuati in relazione ai nuovi dati e servizi offerti in ANA.

Con parere 16 gennaio 2025, il Garante si è espresso sullo schema di decreto del Ministero della salute, di concerto con il MEF, concernente la disciplina delle caratteristiche e dei contenuti delle prescrizioni mediche rilasciate in territorio italiano su richiesta di pazienti che intendano utilizzarle in altri stati membri dell'Unione europea (provv. 16 gennaio 2025, n. 3, doc. web n. 10110520). Lo schema di decreto supera i numerosi rilievi formulati dal Garante nel parere non positivo del 26 gennaio 2023, n. 24 (doc. web n. 9856677), tiene conto dell'innovata disciplina sul FSE 2.0, a cui è stata data attuazione, da ultimo, con il decreto 7 settembre 2023, e di quanto previsto nello schema di decreto del MEF 12 settembre 2024, inerente le modalità con cui il Sistema TS, tramite l'INI del FSE, mette a disposizione dei FSE i dati relativi alle prescrizioni e prestazioni erogate di farmaceutica e specialistica, nonché delle numerose osservazioni sollevate nel corso delle molteplici interlocuzioni intercorse tra il Garante, il Ministero della salute e il MEF.

NCPeH e Sistema TS

Come richiesto dall'Autorità nel parere del 2023, è stato descritto il sistema di generazione delle prescrizioni transfrontaliere elettroniche che sono rilasciate dal medico prescrittore sul territorio nazionale e, nel momento in cui sono richieste dalle farmacie estere degli Stati membri che hanno attivato gli scambi elettronici con l'Italia, vengono generate dal *National Contact Point for eHealth* (NCPeH - Punto di contatto nazionale per l'*eHealth*) a partire dalle ricette elettroniche nazionali, secondo le modalità di cui al decreto del MEF 2 novembre 2011. Su richiesta dell'Autorità è stata disciplinata anche la fattispecie in cui la farmacia estera, ove si vuole chiedere la dispensazione del medicinale, si trovi in uno Stato membro che non ha attivato gli scambi elettronici con l'Italia. In tal caso e in quello in cui l'interessato lo richieda espressamente, la prescrizione transfrontaliera, contenente tutte le indicazioni e i requisiti di cui all'art. 12, d.lgs. n. 38/2014 è rilasciata dal medico prescrittore in forma cartacea per poi essere esibita per la dispensazione del medicinale in una farmacia estera.

Per le prescrizioni dematerializzate, lo schema di decreto precisa che la farmacia estera, tramite il *National Connector* estero interrogherà il *National Connector* italiano (realizzato nell'ambito dell'infrastruttura del Sistema TS), che, attraverso specifici servizi del Sistema TS, verificherà l'esistenza e la spendibilità della prescrizione transfrontaliera elettronica, secondo quanto previsto nel d.m. 2 novembre 2011. A seguito di esito positivo delle predette verifiche, il *National Connector* italiano accerterà che la prescrizione transfrontaliera contenga i dati espressamente richiesti e che non sussistano le esclusioni alla dispensazione sopra richiamate. Inoltre, il *National Connector* italiano genererà e trasmetterà la prescrizione transfrontaliera al *National Connector* estero e la farmacia estera dispenserà il medicinale e invierà le informazioni relative alla dispensazione del medicinale, attraverso i predetti *National Connector*, al Sistema TS, che chiuderà la procedura di dispensazione. Qualora, invece, la predetta verifica dovesse avere esito negativo, il *National Connector* estero invierà al farmacista estero un messaggio di errore e il medicinale non verrà dispensato. È stato inoltre precisato, che il Sistema TS non conserverà i dati relativi ai predetti servizi di verifica. Come richiesto dall'Autorità, lo schema di decreto in esame prevede che i dati trattati dal *National Connector* italiano siano cancellati decorsi dieci anni dalla richiesta effettuata dal *National Connector* estero, e che i dati relativi alla dispensazione del medicinale siano cancellati dal Sistema TS decorsi trent'anni dal decesso dell'assistito con periodicità annuale.

Nel parere 26 gennaio 2023 il Garante aveva rilevato sostanziali criticità con riferimento al mancato rispetto dei principi di correttezza e trasparenza, evidenziando in particolare,

la necessità che fossero fornite all'interessato informazioni chiare in merito alle operazioni eseguite sui dati personali (art. 5, par. 1, lett. a), RGPD). Sul punto, nello schema esaminato è stato previsto che l'interessato possa esercitare i diritti previsti dagli artt. 15, 16, 17 e 18 del RGPD, presentando apposita istanza al Ministero della salute, secondo le modalità indicate nell'ambito delle informazioni rese, ai sensi degli artt. 13 e 14 del RGPD, sul sito istituzionale del predetto Ministero.

Nella Newsletter 21 marzo 2025 (doc. web n. 10114986) il Garante, a fronte di numerosissime istanze pervenute dagli operatori del settore, ha chiarito che il nuovo sistema di fatturazione elettronica per i professionisti sanitari (vigente dal 1° gennaio 2026) è in linea con la normativa in materia di protezione dei dati personali. Con il parere favorevole 7 dicembre 2023, il Garante aveva infatti ritenuto che il decreto del MEF sulle modalità di utilizzo da parte dell'Agenzia delle entrate dei dati fiscali delle fatture e dei corrispettivi trasmessi al Sistema TS individuasse misure appropriate a tutela dei dati sanitari degli assistiti. L'Agenzia delle entrate potrà acquisire i soli dati effettivamente indispensabili ai fini fiscali, mentre saranno esclusi i dati relativi alla salute degli interessati (descrizione della prestazione e codice fiscale dell'assistito) (cfr. Relazione 2023, p. 37).

In materia di ricetta dematerializzata, con nota del Segretario generale del Garante, nel mese di febbraio 2025, è stato espresso al MEF e al Ministero della salute, per i profili di competenza, il nulla osta all'adozione del cronoprogramma di adeguamento all'autenticazione a due o più fattori della ricetta elettronica a carico del SSN, tenuto conto della molteplicità degli utenti interessati, dell'esigenza di garantire la disponibilità delle ricette a tutta la popolazione assistita e agli organi di governo sanitario ai fini del perseguimento delle rispettive finalità di monitoraggio, nonché dell'elevato numero delle operazioni online previste (circa 700 milioni di ricette elettroniche annue).

5.1.4. La medicina di iniziativa

Anche nel 2025 l'Autorità è intervenuta sul tema della medicina di iniziativa/predittiva e sulla connessa attività di stratificazione della popolazione sulla base delle classi di morbilità effettuata con le informazioni sanitarie detenute dal servizio sanitario nazionale e regionale.

Come ricordato nel parere del 5 marzo 2020 (provv. n. 43, doc. web n. 9304455) una profilazione dell'utente del SSN sulla base delle informazioni sanitarie, consistendo in un trattamento automatizzato di dati personali volto a valutare determinati aspetti privati, relativi a una persona fisica, in particolare, per analizzarne e prevederne la situazione sanitaria, necessita di una espressa previsione normativa che disciplini le finalità perseguibili e le misure a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato (artt. 4 e 22 del RGPD).

Il primo intervento normativo in materia è avvenuto con il d.l. n. 34/2020, che all'art. 7 disciplina per la prima volta le metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione. Tale impianto normativo attribuisce al Ministero della salute il compito di trattare dati personali, anche relativi alla salute degli assistiti, raccolti nei sistemi informativi del SSN, per lo sviluppo di metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione.

L'Ufficio ha pertanto più volte ribadito in alcune note indirizzate a regioni e province autonome che tale attività potrà essere effettuata con le modalità e i limiti che saranno individuati attraverso un decreto del Ministero della salute, previa acquisizione del parere del Garante.

Nelle more dell'adozione di tale decreto, la predetta disposizione prevede che il Ministero della salute possa avviare le attività relative alla classificazione delle patologie

croniche presenti nella popolazione italiana, limitatamente alla costruzione di modelli analitici prodromici alla realizzazione del modello predittivo del fabbisogno di salute della popolazione, garantendo che gli interessati non siano direttamente identificabili.

5.1.5. Il dossier sanitario

La gestione del dossier sanitario elettronico ha continuato a rappresentare nel 2025 un'area critica, oggetto di molteplici accertamenti ispettivi che hanno evidenziato diffuse difformità rispetto alle linee guida adottate dal Garante nel 2015. Le verifiche hanno riguardato sia strutture ospedaliere pubbliche che private, rilevando violazioni sistematiche dei principi fondamentali in materia di protezione dei dati personali.

Con provvedimento 4 agosto 2025, il Garante ha contestato ad una azienda ospedaliero-universitaria alcune violazioni della disciplina sulla protezione dei dati personali nella configurazione del dossier sanitario con particolare riferimento: ai profili di autorizzazione che consentivano ai medici l'accesso a cartelle cliniche storiche anche senza avere il paziente in cura; all'assenza di meccanismi di oscuramento parziale dei dati sensibili; ai sistemi di log inadeguati per il monitoraggio degli accessi; all'informativa obsoleta e alla mancanza di consenso specifico (provv. 4 agosto 2025, n. 474, doc. web n. 10166336). A seguito delle contestazioni, l'azienda si è puntualmente conformata alle indicazioni dell'Autorità.

Analoghe criticità sono emerse sul dossier sanitario di un'altra azienda ospedaliera universitaria. Nello specifico, è stato accertato che la predetta azienda utilizzava utenze generiche per l'accesso ai dossier sanitari dei pazienti; consentiva ad utenti amministrativi di reparto, utenti medici del lavoro, utenti medici legali che svolgevano attività di certificazione, di accedere al dossier; nonché agli utenti medici di accedere al dossier di pazienti non in cura motivando l'accesso con la generica indicazione di "altra motivazione". Infine, anche le guardianie avevano accesso al dossier dei pazienti ricoverati. Nel provvedimento l'Autorità ha ricordato che l'utilizzo di utenze non nominali, da parte di più soggetti, impedisce di attribuire le azioni compiute in un sistema informatico a un determinato soggetto, con pregiudizio anche per il titolare che è di fatto privato della possibilità di controllare l'operato dei soggetti che agiscono sotto la sua autorità (artt. 29 del RGPD e 2-*quaterdecies* del Codice). Ciò può comportare situazioni in cui non c'è coerenza tra i profili di autorizzazione attribuiti e le effettive esigenze di operatività, favorendo accessi illeciti e lo svolgimento di attività da parte di soggetti non autorizzati (provv. 25 settembre 2025, n. 533, doc. web n. 10185490).

È stato poi contestato l'utilizzo del dossier anche da parte del personale delle guardianie (sebbene con riguardo un novero ridotto di informazioni), del personale amministrativo, delle utenze infermieristiche che emettono l'attestazione di avvenuta prestazione specialistica e dei medici del lavoro, in violazione del principio di limitazione della finalità; il dossier sanitario può essere utilizzato infatti, solo dal personale sanitario che ha in cura l'interessato, essendo inteso come strumento per agevolare il percorso di cura di quest'ultimo, e non invece per le richiamate esigenze organizzative e amministrative, perseguibili con i tipici strumenti che il datore di lavoro possiede per la gestione del personale e nel rispetto dei limiti previsti dalla disciplina di settore.

L'azienda, successivamente all'intervento dell'Ufficio, ha adottato misure correttive consistenti nell'eliminazione delle utenze generiche, nella restrizione dei profili di accesso e aggiornamento del sistema di dossier sanitario.

Un ulteriore intervento ha riguardato un'AUSL del nord, presso cui l'Autorità ha accertato accessi abusivi al dossier sanitario da parte di un'infermiera dell'assistenza domiciliare integrata (ADI) per motivi personali, evidenziando criticità strutturali legate ai profili di autorizzazione di medici e personale ADI non limitati ai soli pazienti in cura, all'assenza di meccanismi di *alert* automatici sugli accessi anomali e alla mancanza

di controlli sistematici sui log (provv. 10 aprile 2025, n. 206, doc. web n. 10144184). L'Autorità è intervenuta in un contesto in cui tutti i medici e il personale ADI dei presidi ospedalieri e dei distretti erano abilitati all'accesso del dossier sanitario di qualsiasi paziente della struttura intra-aziendale di un altro distretto senza alcuna limitazione dettata dall'effettivo coinvolgimento degli stessi nel percorso di cura dell'interessato cui il dossier si riferisce.

In merito alla mancanza di autonomia nella configurazione del dossier da parte dell'azienda, atteso che l'impianto del SSR prevedeva la centralizzazione degli investimenti, il Garante ha richiamato la recente sentenza della Corte di cassazione 6 marzo 2025, n. 6067 secondo cui l'azienda sanitaria, quale titolare del trattamento, ha il dovere di esercitare tutte le sue prerogative a tutela dell'utilizzo dei dati di cui è titolare, non ricorrendo alcuna causa di esenzione di responsabilità da parte del titolare del trattamento in merito ad eventuali disposizioni regionali adottate in materia.

Un ulteriore intervento sul dossier sanitario ha interessato una casa di cura privata. A seguito di una attività ispettiva è stato accertato che il consenso acquisito al trattamento dei dati effettuato attraverso il dossier comportava automaticamente l'espressione del consenso anche al trattamento delle informazioni relative ad eventi sanitari pregressi all'istituzione del dossier, profili di accesso per medici e infermieri che consentivano la consultazione di documentazione storica anche di pazienti non in cura, assenza di sistemi di log delle consultazioni, una informativa incompleta, e la mancata garanzia per gli interessati di esercitare il diritto di accesso e quello di oscuramento (provv. 11 settembre 2025, n. 487, doc. web n. 10169116).

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

L'impiego di sistemi di IA in ambito sanitario ha rappresentato nel 2025 un tema di crescente rilevanza, oggetto di specifiche indicazioni da parte del Garante volte ad assicurare il rispetto dei principi di protezione dei dati personali e la tutela dei diritti degli interessati. In continuità con l'adozione del decalogo in materia di IA (cfr. Relazione 2023, par. 5.2), l'Autorità ha proseguito le interlocuzioni con il Ministero della salute e AGENAS relative alla realizzazione di una piattaforma informatica di IA a supporto dell'assistenza primaria nell'ambito dei SSR (cfr. Relazione 2024, p. 90).

Merita in tale contesto evidenziare l'istruttoria concernente una procedura di gara per la conclusione di un accordo quadro per l'affidamento di servizi applicativi e di supporto in ambito «Sanità digitale - *Data Governance* e *Artificial Intelligence*» per le p.a. del SSN. Tale istruttoria è stata l'occasione per ribadire i principi sanciti dal Consiglio di Stato ed applicabili al trattamento di dati sulla salute con logiche algoritmiche basate su sistemi di IA ovvero il principio di conoscibilità, per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e di ricevere informazioni significative sulla logica utilizzata, il principio di non esclusività della decisione algoritmica e quello di non discriminazione algoritmica (Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472).

È stato inoltre evidenziato come l'utilizzo di sistemi di IA che comportano il trattamento dei dati sulla salute dei pazienti potrebbe ricadere tra quelli considerati ad alto rischio dal reg. IA, e pertanto richiedere un riesame e un aggiornamento costanti e sistematici dei rischi nel corso dell'intero ciclo di vita del sistema (cfr., in particolare, Capo III, sez. I e II del reg. IA).

Sul piano nazionale, è stato evidenziato che allo stato, l'art. 12, comma 15-*undecies*, lett. g), d.l. n. 179/2012, convertito, con modificazioni, dalla l. n. 221/2012, conferisce ad

AGENAS la funzione di gestione della piattaforma nazionale di intelligenza artificiale da esercitare nel rispetto degli indirizzi del Ministro della salute, del Ministro delegato per l'innovazione tecnologica e la transizione digitale e del Ministro dell'economia e delle finanze (comma 15-*duodecies*) e che non risulta ancora adottata la disciplina di attuazione di tale disposizione, in conformità a quanto previsto dall'art. 2-*sexies* del Codice.

Con il comunicato stampa 30 luglio 2025 (doc. web n. 10154670) il Garante è intervenuto sulla sempre più diffusa prassi di caricare analisi cliniche, radiografie e altri referti medici sulle piattaforme di IA generativa chiedendo interpretazioni e diagnosi. L'Autorità ha in particolare invitato gli utenti utilizzatori di tali piattaforme a valutare con attenzione l'opportunità di procedere alla condivisione di dati di carattere sanitario con i fornitori di servizi di IA generativa, nonché a diffidare dalle risposte generate automaticamente da tali servizi, che dovrebbero sempre essere verificate da un professionista sanitario. Il Garante ha richiamato l'attenzione sull'importanza dell'attenta lettura delle informative sulla privacy che i gestori delle piattaforme hanno l'obbligo di pubblicare al fine di verificare se i dati concernenti gli esami clinici eseguiti e caricati online ai fini della richiesta di interpretazione e/o diagnosi siano destinati a essere cancellati a seguito della richiesta medesima, in un momento successivo, o a essere conservati dal gestore del servizio ai fini dell'addestramento dei propri algoritmi. L'intervento umano è essenziale per prevenire rischi che potrebbero incidere direttamente sulla salute della persona (cfr. art. 14 reg. IA). La "supervisione umana qualificata", tra l'altro, deve essere garantita in tutte le fasi del ciclo di vita del sistema di IA: dallo sviluppo all'addestramento, fino ai test e alla convalida, prima della sua immissione sul mercato o nel suo utilizzo.

Il Garante ha sensibilizzato, infine, gli sviluppatori dei sistemi di IA e gli operatori del settore sanitario sui rischi derivanti dalla raccolta massiva di dati personali dal web per finalità di addestramento dei modelli di IA generativa già individuati nel documento pubblicato a maggio 2024 sul *web scraping* (doc. web n. 10020334).

5.3. *Trattamenti di dati personali per finalità di cura e amministrative correlate alla cura*

5.3.1. Screening e prevenzione

Nel 2025 il Garante è intervenuto sui trattamenti effettuati nell'ambito delle attività di screening e prevenzione. In particolare, sono stati adottati 3 pareri su versioni aggiornate dello schema di decreto concernente disposizioni per l'avvio del programma pluriennale di screening su base nazionale nella popolazione pediatrica per l'individuazione degli anticorpi del diabete di tipo 1 e della celiachia (provv.ti 30 gennaio 2025, n. 59, doc. web n. 10112237; 31 ottobre 2025, n. 657, doc. web n. 10195335; 18 dicembre 2025, n. 749, doc. web n. 10213952).

Nel parere di gennaio 2025 l'Autorità ha rilevato che lo schema di decreto teneva conto delle osservazioni formulate nell'ambito delle numerose interlocuzioni intercorse con il Ministero della salute e l'ISS concernenti in particolare: l'indicazione nei visti delle norme di cui al RGPD e al Codice nonché dei rilevanti provvedimenti del Garante anche al fine di una corretta indicazione dei compiti di rilevante interesse pubblico ivi disciplinati (art. 9, par. 2, lett. a), g), h) e j), RGPD, art. 2-*sexies* del Codice, prescrizioni e regole deontologiche); l'individuazione dei soggetti coinvolti a vario titolo nella realizzazione dello screening e la corretta attribuzione dei relativi ruoli di protezione dei dati (titolare, responsabile o autorizzato al trattamento dei dati), in considerazione delle diverse finalità istituzionali attribuite ai predetti soggetti nello svolgimento delle attività di screening (artt. 4, punti 7) e 8), 24, 28 e 29 del RGPD e 2-*quaterdecies* del Codice); la necessità di garantire che i dati anagrafici dei soggetti da sottoporre a screening siano previamente

verificati mediante l'ANA e che, nelle more della sua realizzazione, l'identificazione dell'assistito sia assicurata attraverso l'allineamento con l'elenco degli assistiti gestito dal Sistema TS, ai sensi dell'art. 50, d.l. n. 269/2003, convertito, con modificazioni, dalla l. n. 326/2003; l'ulteriore necessità che, in relazione al trattamento dei dati personali per finalità di screening, il consenso sia raccolto esclusivamente con riferimento all'indagine sulla celiachia che comporta un trattamento di dati genetici (art. 9, par. 2, lett. h) e par. 4, RGPD).

L'Autorità è tornata ad esprimersi sul testo in parola nel mese di ottobre 2025, a seguito delle esigenze manifestate dalle regioni e province autonome in sede di conferenza permanente in merito all'autonomia organizzativa e gestionale nello svolgimento dello screening, al coinvolgimento dei pediatri di libera scelta, alla possibilità di scegliere se inserire i dati direttamente sulla piattaforma nazionale oppure tramite i propri sistemi informativi in condizione di interoperabilità con la piattaforma nazionale, alla titolarità e responsabilità del trattamento dei dati da parte dei diversi soggetti coinvolti nello screening, e alla definizione della tipologia di test da effettuare e delle fasce di età da sottoporre a screening, in base alle risorse disponibili e alla programmazione dell'offerta vaccinale. Tali richieste hanno comportato la necessità di rivedere l'assetto relativo alla titolarità e alla responsabilità del trattamento dei dati personali, in funzione delle modalità di alimentazione della piattaforma nazionale, nonché l'adeguamento del disciplinare tecnico, che descrive le modalità tecniche per la raccolta dei dati, le caratteristiche della piattaforma informatica nazionale, le modalità di interoperabilità e cooperazione applicativa nonché i requisiti dei sistemi informativi regionali. Il nuovo schema di decreto ha tenuto conto delle richieste dell'Ufficio con particolare riferimento ai ruoli dei diversi soggetti che intervengono nella catena del trattamento e alle modalità di trasmissione dei dati, all'eliminazione del consenso al trattamento dei dati genetici in quanto gli screening in esame non comportano il trattamento di tale categoria di dati personali, e all'eliminazione dallo schema di decreto del riferimento alle soluzioni tecnologiche di cui all'art. 12, comma 15-*quater*, ultimo capoverso, d.l. n. 179/2012 e all'art. 13 comma 1 del decreto del Ministero della salute 7 settembre 2023 sul FSE 2.0, in quanto trattasi di soluzioni utilizzabili esclusivamente per il trattamento dei dati personali effettuato attraverso il FSE e l'EDS.

Successivamente all'adozione del parere di ottobre, il Ministero della salute ha presentato un nuovo schema di decreto con specifiche modifiche in merito alle attività di competenza dei dipartimenti di prevenzione delle aziende sanitarie nell'ambito dello screening, del personale di regioni e province autonome, dei laboratori di riferimento, dei centri clinici regionali di riferimento, dei dipartimenti di prevenzione e dei pediatri di libera scelta. Le modifiche introdotte allo schema di decreto hanno reso necessario l'adeguamento del disciplinare tecnico concernente le modalità tecniche per la raccolta dei dati, le caratteristiche della piattaforma informatica nazionale, le modalità di interoperabilità e cooperazione applicativa nonché i requisiti dei sistemi informativi regionali.

La nuova versione dello schema di decreto tiene conto delle osservazioni espresse dall'Autorità che hanno riguardato, in particolare, la necessità di individuare in maniera puntuale i soggetti che intervengono nelle operazioni di trattamento per lo svolgimento delle proprie finalità istituzionali correlate ai predetti screening. L'accesso ai dati in chiaro è consentito unicamente al personale dei centri clinici di riferimento, ai dipartimenti di prevenzione e ai pediatri di libera scelta, se coinvolti dalle regioni e province autonome limitatamente ai propri assistiti.

5.3.2. Oblio oncologico

La l. 7 dicembre 2023, n. 193, recante disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone, ha introdotto l'istituto del diritto

all'oblio oncologico, ovvero quella situazione giuridica soggettiva che riconosce alle persone pienamente guarite da una malattia oncologica, il diritto a non essere discriminati a causa di una condizione sanitaria ormai superata.

La citata legge prevede all'art. 5, comma 4 che "il Garante per la protezione dei dati personali vigila sull'applicazione delle disposizioni di cui alla presente legge". In attuazione della citata disciplina, l'Ufficio ha avviato nel 2025 un'indagine conoscitiva, mediante l'invio di richieste di informazioni volte a verificare se le strutture sanitarie destinatarie delle stesse avessero: ricevuto istanze per ottenere certificati di oblio oncologico; adottato le misure per garantire le tutele previste dalla predetta disciplina nella procedura di richiesta e di rilascio del certificato, con particolare riferimento a quelle predisposte per rispettare i termini di conservazione della suddetta istanza; in uso il modello di istanza, ivi incluso il corredato modello di informativa e di certificato allegati al predetto decreto.

A seguito dell'attività svolta è emerso il ridotto impatto delle istanze volte al rilascio del certificato di oblio oncologico presso le aziende sanitarie, a fronte dell'adozione da parte delle stesse di specifiche misure al fine di gestire correttamente le procedure di acquisizione dell'istanza, di rilascio del certificato di oblio oncologico, nonché in merito all'individuazione dei termini di conservazione indicati dalla legge.

5.3.3. Provvedimenti derivanti da data breach

Le violazioni dei dati personali (*data breach*) hanno continuato a rappresentare una delle principali criticità nel settore sanitario, con numerosi episodi di attacchi *ransomware*, accessi abusivi e perdite di dati, oggetto di specifici provvedimenti del Garante volti ad accertare le responsabilità e ad imporre le necessarie misure correttive.

Con provvedimento 13 febbraio 2025, il Garante ha concluso un procedimento nei confronti di una ASL, che aveva notificato una violazione di dati personali, a seguito di un attacco del gruppo hacker "MONTI" che aveva utilizzato un *ransomware* progettato per crittografare i dati e richiedere il pagamento in *bitcoin* per gli strumenti di decrittazione. L'attacco, originato da un'attività di *phishing*, aveva richiesto la disconnessione dell'infrastruttura da Internet, il blocco dei sistemi per una settimana e il ricorso a procedure manuali per garantire la continuità delle cure. Le verifiche, anche ispettive, avevano evidenziato carenze nelle misure di sicurezza antecedenti alla violazione, quali una rete *flat* priva di adeguata segmentazione, l'assenza di sistemi di correlazione di specifici eventi di sicurezza e di comportamenti anomali, e il *Security Operation Center* (SOC) non operativo in modalità "estesa", circostanze che non avevano consentito all'azienda di venire tempestivamente a conoscenza della violazione; è stata, altresì, rilevata una inidonea comunicazione della violazione dei dati personali agli interessati. Nei confronti dell'azienda il Garante ha adottato un provvedimento di ammonimento, considerati la cooperazione garantita in ogni fase dell'istruttoria e l'impegno del titolare nella realizzazione di misure volte a incrementare il livello di sicurezza dei trattamenti svolti (implementazione dell'autenticazione multi-fattore e potenziamento della formazione del personale) (provv. 13 febbraio 2025, n. 83, doc. web n. 10116834).

Simile dinamica ha caratterizzato l'attacco *ransomware* subito da un'azienda ospedaliera universitaria, con esfiltrazione di 650 GB di dati e pubblicazione sul *dark web* di informazioni anche sanitarie estratte da file server. A seguito della notifica di violazione da parte dell'azienda, il Garante ha avviato una istruttoria, conclusa la quale è stata accertata la mancata adozione di misure adeguate a rilevare tempestivamente la violazione dei dati e a garantire la sicurezza dei sistemi e delle reti. È stato, pertanto, adottato un provvedimento sanzionatorio che ha tenuto conto dell'impegno del titolare nell'introduzione di specifiche misure e della cooperazione con l'Autorità (provv. 10 aprile 2025, n. 205, doc. web n. 10142352).

5

Anche un centro diagnostico è stato destinatario di un provvedimento sanzionatorio. In particolare, l'istruttoria mossa da una notifica di violazione effettuata dopo aver subito un attacco informatico (con esfiltrazione di dati contenuti in 464 referti sanitari), ha evidenziato, tra gli altri, vulnerabilità derivanti da una pagina non adeguatamente protetta, dall'assenza di autenticazione multi-fattore e dalla mancata adozione di misure adeguate alla conservazione delle password degli utenti, in violazione del principio della protezione dei dati fin dalla progettazione (provv. 11 settembre 2025, n. 488, doc. web n. 10184654).

Un istituto di cura è stato destinatario del provv. 23 ottobre 2025 per la violazione degli artt. 5, par. 1, lett. f), 25 e 32 del RGPD a seguito di un attacco *ransomware* realizzato mediante compromissione delle credenziali di un collaboratore esterno, con esfiltrazione di dati relativi a circa 4.200 pazienti. L'istruttoria aveva evidenziato una serie di operazioni propedeutiche all'attacco informatico, quali accessi in orari anomali, movimenti laterali, esecuzione di codice malevolo, traffico in uscita e *upload* verso indirizzi IP appartenenti a un servizio VPN utilizzato per anonimizzare la navigazione Internet e per aggirare eventuali regole di geolocalizzazione. In sede istruttoria non era altresì emerso che l'istituto disponesse di un SIEM, né che fossero impostati e presi incarico *alert* in relazione ai predetti eventi di sicurezza riferiti alle attività dell'attaccante. Inoltre, al momento della violazione, l'istituto era risultato privo di misure adeguate a garantire la sicurezza dei sistemi di trattamento, quale la procedura di autenticazione a doppio fattore, ed era risultata inadeguata l'attività finalizzata alla sensibilizzazione del personale. Il Garante ha pertanto adottato un provvedimento sanzionatorio nei confronti dell'istituto (provv. 23 ottobre 2025, n. 616, doc. web n. 10196105).

5.3.4. Provvedimenti derivanti da reclami e segnalazioni

L'attività di vigilanza del Garante ha riguardato nel periodo di riferimento anche numerosi reclami concernenti criticità nella gestione dei trattamenti di dati personali da parte di strutture sanitarie pubbliche e private.

Con provv. 27 marzo 2025, il Garante ha sanzionato una azienda sanitaria territoriale a seguito di un reclamo a mezzo del quale la reclamante aveva lamentato di non aver ricevuto riscontro all'istanza di accesso ai dati personali ai sensi dell'art. 15 del RGPD, nonché l'avvenuta comunicazione telefonica a soggetto terzo, senza il previo proprio consenso, della necessità di sottoporsi a ulteriori accertamenti diagnostici. Il Garante ha accertato la violazione, da parte dell'azienda sanitaria, dell'art. 5, par. 1, lett. f) e degli obblighi di sicurezza di cui all'art. 32 del RGPD per l'assenza, al momento del fatto, di misure tecniche e organizzative per la gestione degli screening di II livello, oltre alla violazione dell'art. 9 del RGPD, per la comunicazione a terzi di dati relativi alla salute in assenza di presupposto giuridico legittimante, nonché la violazione dell'art. 12, in relazione all'art. 15 del RGPD, per il mancato riscontro alla richiesta di accesso (provv. 27 marzo 2025, n. 170, doc. web n. 10139489).

A seguito di altro reclamo, l'Autorità ha avviato un'istruttoria nei confronti di una agenzia di tutela della salute in relazione alla trasmissione, tramite PEC, di documentazione sanitaria al datore di lavoro del paziente. In particolare, l'agenzia aveva allegato, per mero errore materiale, una serie di documenti non pertinenti, contenenti informazioni dettagliate sullo stato di salute del reclamante. Nel corso dell'istruttoria, l'agenzia aveva rappresentato il carattere accidentale e involontario dell'episodio, l'adozione di misure tecniche e organizzative a tutela dei dati trattati nonché l'avvio di iniziative correttive quali un aggiornamento delle procedure interne e specifiche attività di richiamo e formazione del personale. All'esito del procedimento, il Garante ha ritenuto integrata la violazione dei principi di minimizzazione e di

integrità e riservatezza di cui all'art. 5, par. 1, lett. c) e f), nonché dell'art. 9 del RGPD, per avere il titolare comunicato a terzi dati relativi alla salute in assenza di base giuridica. Valutata la gravità della violazione – anche in considerazione della natura particolarmente sensibile dei dati e della operazione di trattamento (comunicazione) – e tenuto conto dei criteri di cui all'art. 83 del RGPD, l'Autorità ha ingiunto all'agenzia il pagamento di una sanzione amministrativa pecuniaria pari a euro 7.000 disponendo altresì la pubblicazione dell'ordinanza-ingiunzione sul sito istituzionale (provv. 21 maggio 2025, n. 286, doc. web n. 10143721).

Un caso diverso ha riguardato un procedimento nei confronti di un medico di medicina generale, il quale aveva registrato le conversazioni intrattenute con i pazienti durante le visite ambulatoriali in assenza di un'idonea informativa sul trattamento dei dati personali. Nel corso dell'istruttoria il professionista aveva dichiarato di aver avviato le registrazioni a fini di autotutela, a seguito di pregresse contestazioni e segnalazioni da parte di pazienti, ritenendo sufficiente un'informativa verbale e il "silenzio assenso" degli interessati. All'esito dell'istruttoria, il Garante ha ritenuto che la registrazione sistematica delle visite mediche non costituisse trattamento "necessario" per finalità di cura ai sensi dell'art. 9, par. 2, lett. h), RGPD, né potesse essere giustificata in via preventiva dall'esigenza di difesa in giudizio, in assenza di un procedimento pendente. È stata pertanto accertata la violazione degli artt. 6 e 9 del RGPD, per difetto di idonea base giuridica. È stata inoltre rilevata la violazione degli artt. 5, par. 1, lett. a), e 13 del RGPD, per inosservanza degli obblighi di trasparenza e informativi, non avendo la titolare predisposto un'informativa scritta relativa alla specifica attività di registrazione, né potendo ritenersi sufficiente la mera comunicazione orale ai pazienti. È stata infine accertata la violazione dell'art. 157 del Codice, per il mancato riscontro alla richiesta di informazioni dell'Autorità. Tenuto conto della natura dei dati trattati, della gravità delle violazioni accertate e dell'assenza di precedenti specifici, il Garante ha comminato una sanzione pecuniaria nei confronti del medico e ha inoltre prescritto al medesimo di predisporre un'idonea informativa al trattamento dei dati personali da fornire ai pazienti (provv. 10 luglio 2025, n. 388, doc. web n. 10165121).

A seguito di reclamo presentato da un paziente, l'Autorità ha avviato un'istruttoria in relazione all'erroneo invio di un referto sanitario a un indirizzo e-mail diverso da quello dell'interessato per un refuso di digitazione. La società aveva ricondotto l'episodio a un malfunzionamento temporaneo nell'interfacciamento tra il proprio software gestionale e quello del laboratorio esterno ed aveva dichiarato di aver successivamente corretto il *bug* e rafforzato le procedure interne, anche mediante formazione del personale ed introduzione di una procedura di emergenza. All'esito dell'istruttoria, il Garante ha ritenuto che la comunicazione del referto a un soggetto terzo integrasse una violazione degli artt. 5, par. 1, lett. f), 9 e 32 del RGPD, per assenza di un idoneo presupposto giuridico e per mancata adozione di misure tecniche adeguate (quali procedure di convalida degli indirizzi e-mail tramite apposita procedura di verifica online) idonee a prevenire l'errore. Tenuto conto del carattere isolato dell'episodio, dell'assenza di dolo, della collaborazione prestata e delle misure correttive adottate, la violazione è stata qualificata come "minore"; l'Autorità ha quindi dichiarato l'illiceità del trattamento e disposto l'ammonimento del titolare ai sensi dell'art. 58, par. 2, lett. b), RGPD (provv. 18 dicembre 2025, n. 753, doc. web n. 10210247).

L'Autorità ha avviato un'ulteriore istruttoria nei confronti di una struttura sanitaria, in relazione ad un caso similare a quello sopra descritto ovvero la consegna ad altra paziente, per errore, di un referto contenente dati relativi alla salute della reclamante. In particolare, a causa di un malfunzionamento informatico verificatosi al momento della dimissione, un dipendente aveva seguito una procedura alternativa di firma e stampa del

documento, nel corso della quale – anche in ragione dell'omonimia e della coincidenza di ulteriori elementi identificativi tra le due pazienti – era stato consegnato il referto della reclamante a terzi. Pertanto, l'Autorità ha ritenuto che la comunicazione dei dati sanitari in assenza di un idoneo presupposto giuridico integrasse una violazione dell'art. 9 del RGPD, nonché dei principi di integrità e riservatezza di cui all'art. 5, par. 1, lett. f), e degli obblighi di sicurezza del trattamento di cui all'art. 32 del RGPD, con particolare riferimento alla mancata adozione di misure adeguate a prevenire il rischio di divulgazioni accidentali in ipotesi di omonimia. Tenuto conto delle circostanze del caso concreto, ovvero del carattere accidentale dell'episodio, dell'assenza di dolo, della collaborazione prestata dal titolare del trattamento e dell'adozione di misure organizzative volte a richiamare il personale alla corretta identificazione degli assistiti, l'Autorità ha emesso un provvedimento di ammonimento nei confronti del titolare (provv. 30 gennaio 2025, n. 41, doc. web n. 10113102).

In un altro caso, il Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza aveva segnalato, su input del Nucleo Polizia economico-finanziaria - sezione tutela economia, che una casa di cura non aveva rinvenuto presso i propri archivi la cartella clinica di una persona ricoverata presso la stessa. Nell'ambito della relativa istruttoria era stata riscontrata, altresì, la mancata notifica di violazione ai sensi dell'art. 33 del RGPD. Anche in questo caso, considerata l'assenza di precedenti violazioni pertinenti, ed in ragione di ulteriori specifici riscontri, il Garante ha ritenuto sufficiente ammonire il titolare del trattamento (provv. 13 marzo 2025, n. 152, doc. web n. 10132289).

Sempre in tema di smarrimento, con provv. 9 ottobre 2025, il Garante ha accertato nei confronti di un centro sanitario privato violazioni degli artt. 5, par. 1, lett. f e 32 del RGPD a seguito di un reclamo della paziente che aveva subito la distruzione accidentale del campione biologico (tessuto del seno paranasale). Nel citato provvedimento, il Garante ha sottolineato che la distruzione accidentale o, comunque, non autorizzata, di un campione di tessuto prelevato durante un intervento chirurgico, che doveva essere inviato al laboratorio di anatomia patologica per l'esame istologico, associato all'identità di una paziente, aveva comportato una violazione della disciplina in materia di protezione dati, in quanto l'ospedale non aveva adottato specifiche cautele volte a garantire il rispetto del principio di integrità e riservatezza dei dati personali e degli obblighi di sicurezza. L'incidente era stato infatti determinato da un errore materiale dovuto alla mancanza di comunicazione tra chirurgo e infermiera di sala. Considerata la gravità dell'accaduto, che aveva esposto la donna a rischi concreti per la propria salute, trattandosi tra l'altro di un reperto non replicabile, il Garante ha adottato un provvedimento sanzionatorio, anche perché la società non aveva notificato il *data breach* all'Autorità ma si era limitata ad avvertire l'interessata e ad avviare la fase di *follow up* radiologico. Nello stesso provvedimento, è stata, invece, archiviata la violazione relativa allo smarrimento di un DVD contenente referto di risonanza magnetica e alla consegna errata a terzi di DVD contenente referto di altro paziente, non potendosi imputare con certezza la responsabilità della violazione (provv. 9 ottobre 2025, n. 587, doc. web n. 10184697).

Finalità estranee alla cura

Nel corso del 2025, il Garante ha adottato significativi provvedimenti sanzionatori anche nei confronti di medici che avevano utilizzato dati personali dei propri pazienti, inclusi dati relativi alla salute, per finalità estranee a quelle di cura, con particolare riferimento ad attività di propaganda elettorale, evidenziando la gravità dell'abuso della posizione professionale e la violazione dei principi di liceità, limitazione delle finalità e integrità del trattamento (provv.ti 13 febbraio 2025, n. 81, doc. web n. 10107219 e n. 82, doc. web n. 10107246).

In particolare, con ordinanza-ingiunzione 13 febbraio 2025, il Garante è intervenuto nei confronti di un medico oncologo per aver utilizzato dati relativi alla salute di pazienti oncologiche (tumore mammella) a fini di propaganda elettorale in occasione delle elezioni comunali di Sanremo 2024. I nominativi erano stati estratti dalla rubrica personale del medico, mentre gli indirizzi erano stati acquisiti dalle liste elettorali pubbliche. Il Garante ha evidenziato che i dati personali raccolti nell'ambito dell'attività di tutela della salute da parte di esercenti la professione sanitaria e di organismi sanitari non sono utilizzabili per fini di propaganda elettorale e connessa comunicazione politica. Tale finalità non è infatti riconducibile agli scopi legittimi per i quali i dati sono stati raccolti (art. 5, par. 1, lett. a) e b), RGPD), salvo che il titolare acquisisca uno specifico e informato consenso dell'interessato (art. 9, par. 1, lett. a), RGPD).

In un analogo provvedimento adottato in pari data il Garante ha sanzionato un altro medico per aver inviato e-mail di propaganda elettorale, sempre per le elezioni comunali di Sanremo 2024, a circa 500 pazienti utilizzando i loro indirizzi di posta elettronica, inseriti tra l'altro in copia conoscenza (cc) anziché in copia nascosta (ccn) e quindi rendendo visibili a tutti i destinatari gli indirizzi e-mail degli altri pazienti.

I dati erano stati raccolti nel contesto dell'assistenza medica e il consenso acquisito non copriva finalità di propaganda elettorale. In tale provvedimento è stato inoltre specificato che non era possibile considerare valido neanche il consenso acquisito dal medico per le attività indicate nell'informativa, relative a: "Attività promozionali, informazione per via telematica, newsletter"; ciò in quanto l'attività di propaganda elettorale non può essere equiparata all'invio di una newsletter riservata agli iscritti per aggiornarli sulle novità in un uno specifico settore. Del resto, ai sensi del codice di deontologia medica, "La pubblicità informativa sanitaria del medico" può avere "per oggetto esclusivamente i titoli professionali e le specializzazioni, l'attività professionale, le caratteristiche del servizio offerto e l'onorario relativo alle prestazioni" (art. 56 codice di deontologia medica del 2014 aggiornato da ultimo nel 2017).

Entrambi i provvedimenti sono stati trasmessi all'Ordine dei medici territorialmente competente.

5.4. *Esercizio dei diritti*

Cartella clinica

Il Garante, nel corso dell'anno, ha ricevuto numerosi reclami in materia di esercizio dei diritti di cui agli artt. da 15 a 22 del RGPD, con particolare riguardo al diritto di accesso ai dati relativi alla salute. Alcuni reclami hanno riguardato il mancato rilascio gratuito della prima copia dei dati contenuti nella cartella clinica, secondo quanto disposto dall'art. 15 del RGPD e, altresì, statuito dalla CGUE nell'interpretazione fornita nella causa C-307/22.

Nella trattazione di tali ultimi reclami, il Garante ha ribadito, ai titolari del trattamento, che l'interessato ha diritto di ricevere gratuitamente la prima copia dei dati personali richiesti contenuti nella cartella clinica (artt. 15, par. 3 e 12, par. 5, RGPD). Con riferimento a tali disposizioni, l'Autorità ha rammentato l'interpretazione fornita in tal senso dalla CGUE nella sentenza C-307/22 del 26 ottobre 2023, rappresentando, altresì, di essere intervenuta in materia, in linea con tale pronuncia, attraverso la pubblicazione, sul proprio sito istituzionale, di alcune "FAQ in materia di accesso alle cartelle cliniche ai sensi del RGPD" (24 dicembre 2024, doc. web n. 10086913 - cfr. Relazione 2024, p. 96), nelle quali si specifica, fra l'altro, che il titolare fornisce all'interessato, gratuitamente, la prima copia dei dati personali relativi a tale interessato contenuti nella cartella clinica.

5

Il Garante ha, poi, adottato alcuni provvedimenti, fra i quali un provvedimento sanzionatorio pecuniario nei confronti di una struttura sanitaria privata, per non aver fornito riscontro, nei termini di cui all'art. 12 del RGPD, all'istanza di accesso ai dati personali presentata dal reclamante ai sensi dell'art. 15 del medesimo RGPD. Il titolare aveva risposto alla richiesta solo a seguito dell'invito ad aderire formulato dall'Autorità nell'ambito dell'istruttoria. La società aveva ricondotto il ritardo a un problema tecnico che avrebbe impedito la tempestiva visualizzazione della PEC contenente l'istanza. L'Autorità ha, tuttavia, ritenuto che tale circostanza non integrasse un'ipotesi di errore scusabile ai sensi della l. n. 689/1981, non risultando dimostrata l'inevitabilità dell'evento neppure con l'uso dell'ordinaria diligenza, anche alla luce della mancata verifica delle comunicazioni telematiche dopo il ripristino della postazione informatica a ciò dedicata (provv. 29 aprile 2025, n. 277, doc. web n. 10139193).

Mancato riscontro

In altro caso è stata comminata una sanzione amministrativa pecuniaria nei confronti di una cooperativa operante in ambito sanitario, per non aver fornito riscontro alle istanze con cui un interessato aveva esercitato i diritti di cui agli artt. 15, 18, 19 e 20 del RGPD. Il titolare aveva risposto alle richieste solo successivamente all'invito ad adempiere formulato dall'Autorità nell'ambito dell'istruttoria avviata a seguito di reclamo, deducendo che il ritardo sarebbe stato determinato da un disguido organizzativo e da un errore umano, qualificato come evento isolato e accidentale, in presenza di procedure e misure interne adottate. L'Autorità ha ritenuto che tale circostanza non escludesse la responsabilità del titolare, richiamando le linee guida WP253 in materia di sanzioni amministrative pecuniarie, secondo cui l'errore umano costituisce espressione di negligenza. È stata pertanto accertata la violazione dell'art. 12 del RGPD, in relazione agli artt. 15, 18, 19 e 20, per tardivo riscontro alle istanze dell'interessato, e comminata una sanzione pecuniaria (provv. 10 luglio 2025, n. 414, doc. web n. 10165159).

In seguito a un reclamo presentato da un paziente nei confronti di un poliambulatorio, l'Autorità ha avviato un'istruttoria in relazione al mancato riscontro a un'istanza di accesso ai dati personali, nonché alla liceità della comunicazione di dati relativi alla salute e alla completezza dell'informativa resa agli interessati. In particolare, il reclamante aveva lamentato di non aver ricevuto tempestivo e idoneo riscontro alla richiesta di accesso volta a ottenere copia dei dati sanitari detenuti dalla struttura. Solo a seguito dell'intervento dell'Autorità, il titolare del trattamento aveva fornito riscontro all'istanza. Nel corso dell'istruttoria sono, inoltre, emerse criticità concernenti il contenuto dell'informativa privacy, risultata generica con riguardo all'indicazione dei destinatari o delle categorie di destinatari dei dati personali, nonché recante riferimenti non coerenti con i trattamenti effettivamente svolti. Ulteriori profili di illiceità hanno riguardato la comunicazione, in assenza di base giuridica, sia dei risultati di un esame diagnostico (TAC) ad altro centro medico per mezzo di un professionista sanitario operante in entrambe le strutture sanitarie sia di dati relativi alla salute attraverso la trasmissione di documentazione medica a tale altro centro medico. All'esito del procedimento, il Garante ha dichiarato l'illiceità del trattamento per violazione degli artt. 12 e 15 del RGPD, dell'art. 13, par. 1, lett. e), per carenze nell'informativa, nonché degli artt. 5, par. 1, lett. f), e 9, per l'indebita comunicazione di dati relativi alla salute, comminando una sanzione amministrativa pecuniaria (provv. 17 luglio 2025, n. 424, doc. web n. 10172163).

In relazione alla presentazione di un reclamo di un paziente nei confronti di una struttura sanitaria privata, l'Autorità ha avviato un'istruttoria con riferimento al mancato riscontro a un'istanza di accesso ai dati personali, alle carenze dell'informativa resa agli interessati ai sensi dell'art. 13 del RGPD, alla comunicazione di dati relativi

alla salute a un soggetto terzo in assenza di base giuridica; nel corso del procedimento ha, poi, avviato una parallela istruttoria per omesso riscontro a una richiesta di informazioni formulata dall'Autorità ai sensi dell'art. 157 del Codice. All'esito dei procedimenti – già unificati nell'atto di contestazione delle citate violazioni ai sensi dell'art. 10, comma 4, del reg. Garante n. 1/2019, trattandosi di fattispecie riguardanti la medesima vicenda e il medesimo titolare del trattamento – il Garante ha dichiarato l'illiceità del trattamento per violazione degli artt. 12 e 15, 13, par. 1, lett. e), 5, par. 1, lett. f), e 9 del RGPD, nonché dell'art. 157 del Codice, irrogando una sanzione amministrativa pecuniaria (provv. 17 luglio 2025, n. 425, doc. web n. 10182336).

L'Autorità è, altresì, intervenuta con un provvedimento di ammonimento nei confronti di una professionista del settore sanitario la quale non aveva fornito riscontro all'istanza di accesso ai dati personali presentata dall'interessata ai sensi dell'art. 15 del RGPD con riferimento ai dati propri e delle figlie minori. L'istanza era stata riscontrata solo a seguito dell'invito formulato dall'Autorità nell'ambito dell'istruttoria avviata a seguito di reclamo, deducendo che il mancato riscontro era dipeso da una dimenticanza determinata da periodo di particolare e intenso impegno professionale e accademico. L'Autorità ha ritenuto che tale circostanza non fosse idonea a escludere la responsabilità, richiamando le linee guida WP253 in materia di sanzioni amministrative, secondo cui la condotta colposa, ove evitabile con l'ordinaria diligenza, integra violazione. È stata pertanto accertata la violazione dell'art. 12, in relazione all'art. 15 del RGPD; tuttavia, tenuto conto di tutti gli elementi e delle circostanze del caso, il Garante ha qualificato il caso come "violazione minore" ai sensi del cons. 148 del RGPD, ritenendo sufficiente l'adozione del provvedimento di ammonimento ai sensi dell'art. 58, par. 2, lett. b), RGPD (provv. 4 dicembre 2025, n. 736, doc. web n. 10210098).

Successivamente a un reclamo presentato nei confronti di una sede provinciale dell'Associazione nazionale mutilati e invalidi civili, l'Autorità ha avviato un'istruttoria in relazione all'erronea indicazione, nell'informativa resa da tale sede provinciale, ai sensi dell'art. 14 del RGPD, dei recapiti per l'esercizio dei diritti, di cui agli artt. da 15 a 22 del RGPD, da parte degli interessati. Il reclamante, destinatario di una comunicazione relativa a una pratica di invalidità civile, aveva esercitato il diritto di accesso ai sensi dell'art. 15 del RGPD utilizzando l'indirizzo e-mail indicato nella citata informativa; tuttavia, tale recapito risultava riferito a una diversa sede provinciale, anch'essa indicata erroneamente quale punto di contatto alternativo. Ciò, ha di fatto ostacolato l'esercizio del diritto di accesso. L'Autorità ha ritenuto che l'indicazione di recapiti non corretti nel testo dell'informativa, in tal caso fornita ai sensi dell'art. 14 del RGPD, integri una violazione degli obblighi di trasparenza e di agevolazione dell'esercizio dei diritti degli interessati di cui all'art. 12, parr. 1 e 2, in relazione all'art. 14, par. 1, lett. a), RGPD. Tenuto conto del carattere isolato dell'episodio, dell'assenza di dolo, della lieve entità della colpa e delle misure correttive adottate, il Garante ha qualificato la violazione come "minore", dichiarando l'illiceità del trattamento e disponendo l'ammonimento del titolare ai sensi dell'art. 58, par. 2, lett. b), RGPD, nonché la pubblicazione del provvedimento (provv. 4 dicembre 2025, n. 735, doc. web n. 10210049).

5.5. *Rete RPD in sanità e ricerca*

L'Autorità, nel corso dell'anno, al fine di consolidare una rete di responsabili della protezione dei dati (RPD) nel settore della sanità e della ricerca scientifica, della quale ha incentivato la costituzione già a partire dal 2024, ha promosso un ciclo strutturato di eventi formativi e di confronto, rivolto ai RPD delle regioni e delle province autonome,

5

delle strutture sanitarie pubbliche e private, nonché a esperti e studiosi delle materie, dal titolo "La Privacy in Salute". In tali occasioni sono stati affrontati, tra l'altro, i temi del regolamento sui trattamenti dei dati sensibili adottato da regioni e aziende sanitarie, del FSE 2.0, dei ruoli nel trattamento, della telemedicina, dell'impiego dell'IA in sanità e nella ricerca scientifica anche alla luce della l. n. 132/2025 sull'intelligenza artificiale nonché della disciplina dei trattamenti per finalità di cura, delle metodologie predittive e dell'accesso alla cartella clinica e dell'uso secondario dei dati sanitari per scopi di ricerca scientifica. Il ciclo formativo si è concluso con un evento svoltosi presso il Ministero della salute che ha rappresentato un momento di sintesi e confronto istituzionale sui principali interventi dell'Autorità nel settore della sanità digitale e durate il quale sono stati ripercorsi i risultati del lavoro interistituzionale svolto negli ultimi anni, con particolare riferimento al FSE 2.0, all'EDS e alla PNT.

6 La ricerca scientifica

6.1. *La modifica dell'art. 110 del Codice, le comunicazioni al Garante e le nuove regole deontologiche per trattamenti per scopi statistici e di ricerca scientifica*

In relazione ai trattamenti effettuati per scopi di ricerca scientifica in campo medico, biomedico ed epidemiologico, in base alla nuova formulazione dell'art. 110 del Codice, nel 2025 sono pervenute circa 150 comunicazioni di valutazioni di impatto redatte ai sensi dell'art. 35 del RGPD.

Come noto, ai sensi del rinnovato art. 110 del Codice, laddove non sia possibile acquisire il consenso degli interessati e non vi siano altri presupposti normativi, il titolare del trattamento non è più tenuto a presentare un'istanza di consultazione preventiva al Garante, ma deve rispettare 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 altresì attuazione al novellato art. 110 del Codice (artt. 2-*quater* e 106 del Codice, provv. 9 maggio 2024, n. 298, doc. web n. 10016146).

In particolare è stato disposto che i titolari debbano accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le 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, se del caso documentando altresì i ragionevoli sforzi profusi per tentare di contattarli. Nei predetti 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.

A tale riguardo, risultano ancora pendenti talune istruttorie volte a verificare la conformità dei trattamenti effettuati per scopi di ricerca medica, biomedica ed epidemiologia al rinnovato quadro normativo, con particolare riferimento alla redazione di un'unica valutazione d'impatto avente ad oggetto tutti i trattamenti svolti per scopi di ricerca in campo medico e agli obblighi informativi (artt. 5, par. 1, lett. a), 12, 13 e 14 del RGPD). Ciò risulta peraltro conforme alle indicazioni contenute nelle linee guida in materia di valutazione d'impatto sulla protezione dei dati (cfr. documento WP248 del Gruppo Art. 29), laddove i trattamenti perseguono finalità simili, ovvero utilizzano tecnologie analoghe e quindi generano rischi simili per i diritti e le libertà delle persone fisiche, pur dovendosi assicurare che le misure di mitigazione del rischio (tecniche ed organizzative) siano adeguate a tutti i trattamenti ivi indicati.

Regole deontologiche

Nel corso dell'anno, sono proseguiti i lavori di redazione delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica (all. A5 del Codice, doc. web n. 9069637), di cui alla citata deliberazione di promovimento 9 maggio 2024, n. 298 (doc. web n. 10016146). Nello specifico sono stati costituiti tre gruppi di lavoro, cui partecipano enti e istituti di ricerca, pubbliche amministrazioni, università, istituti di ricovero o di cura a carattere scientifico, enti del terzo settore, comitati etici, nonché enti rappresentativi degli interessati (es. associazioni di malati), incaricati di redigere il testo degli articoli delle

nuove regole deontologiche, sulla base di un elenco elaborato dal Garante.

Sempre nel quadro dell'adeguamento al quadro normativo introdotto dalla novellazione dell'art. 110 del Codice, il Garante è intervenuto sulle prescrizioni relative al trattamento dei dati genetici, contenute nell'all. n. 4 al provv. 5 giugno 2019, ai sensi dell'art. 21, comma 1, d.lgs. n. 101/2018 (doc. web n. 10112364). Al riguardo ha ritenuto incompatibile con il nuovo quadro normativo il punto 4.11.3, lett. bb) delle suddette prescrizioni, nella parte in cui richiedeva, oltre al parere favorevole del comitato etico, la preventiva consultazione del Garante ai sensi dell'art. 36 del RGPD. Il provvedimento ha quindi modificato tale disposizione, sostituendo il riferimento alla consultazione preventiva con il richiamo al rispetto di quanto previsto dall'art. 110, comma 1, seconda parte, del Codice, adeguando così le prescrizioni alla disciplina vigente (provv. 13 febbraio 2025, n. 66, doc. web n. 10112364).

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

Tra gli altri provvedimenti adottati dal Garante in materia di trattamento di dati personali per scopi di ricerca scientifica, merita di essere evidenziato quello sanzionatorio e correttivo adottato nei confronti di una casa farmaceutica, a seguito di specifici accertamenti ispettivi con il quale è stato altresì ingiunto il pagamento di sanzione amministrativa pecuniaria pari a euro 21.000 e disposta la pubblicazione dell'ordinanza-ingiunzione sul sito istituzionale (provv. 21 maggio 2025, n. 287, doc. web n. 10149917).

Difatti, il Garante ha rilevato l'illiceità dei trattamenti di dati personali svolti per l'addestramento dell'algoritmo di un *tool* (basato su tecniche di *deep learning*), utilizzato nell'ambito di uno specifico progetto di ricerca scientifica, per l'analisi e la classificazione delle cellule tumorali del mieloma multiplo, per avere violato il principio di trasparenza, nonché il conseguente obbligo di rendere un'informativa esatta e completa agli interessati, i principi di limitazione della conservazione nonché di responsabilizzazione (artt. 5, par. 1, lett. a), b), e), par. 2 e 13, RGPD).

Con riferimento alla rilevata violazione del principio di limitazione della conservazione, la società aveva indicato tale periodo di conservazione (fino a venticinque anni) anche per il perseguimento di finalità eventuali e ulteriori rispetto allo scopo primario della raccolta (art. 5, par. 1, lett. e), RGPD).

In relazione al principio di trasparenza e dell'obbligo di fornire agli interessati una informativa chiara, concisa e comprensibile, a maggior ragione allorquando il trattamento di dati personali è finalizzato, come nel caso in esame, all'addestramento di strumenti di IA, l'informativa fornita ai pazienti arruolati nel progetto di ricerca era stata formulata in modo da potere ingenerare negli interessati la convinzione che gli scopi del trattamento fossero tra loro distinti e differenti (uno volto allo sviluppo di nuovi prodotti e l'altro allo sviluppo di nuovi algoritmi attraverso tecnologie di *machine learning*), senza chiarire che si trattava di due fasi di unico processo (artt. 5, par. 1, lett. a) e 13 del RGPD; parere 28/2024 "su taluni aspetti relativi alla protezione dei dati ai fini del trattamento dei dati personali nel contesto dei modelli di IA" adottato dal CEPD il 17 dicembre 2024, punto 65; cfr. anche cons. 67 reg. (UE) 2024/1689 che stabilisce norme armonizzate sull'IA). Il Garante inoltre, con riferimento all'indicazione del periodo di conservazione dei dati, avendo la società collocato tale elemento informativo nella sezione dell'informativa denominata *Retention of your data and samples and additional research projects*, ha ritenuto tale circostanza idonea a ingenerare confusione tra l'indicazione del periodo di conservazione dei dati necessario al conseguimento dello scopo della raccolta e quello,

invece, eventuale e propedeutico alla realizzazione di ulteriori progetti, confermando la violazione del principio di trasparenza e dell'obbligo di rendere informazioni idonee sul trattamento dei dati ai sensi degli artt. 5, par. 1, lett. a) e 13 del RGPD.

È stata inoltre accertata la violazione del principio di responsabilizzazione (*accountability*), con riguardo alla non adeguatezza delle misure adottate per assicurare l'effettiva applicazione dei principi di protezione dei dati personali, in particolar modo di quello di trasparenza. L'opacità delle logiche algoritmiche e il divario tra l'interessato (nei contesti sanitari spesso vulnerabile) e il titolare del trattamento possono essere infatti colmati, in primo luogo, tramite l'effettiva applicazione del principio di trasparenza così da consentire agli interessati di mantenere il governo sulle informazioni che li riguardano e formulare scelte consapevoli. Ciò contribuisce, inoltre, a creare il clima di fiducia auspicato dal Regolamento e a perseguire l'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'art. 179, par. 1, TFUE (cons. 7 e 159 del RGPD).

In un altro provvedimento, il Garante ha ammonito un'università che, per la realizzazione di un progetto di ricerca scientifica, aveva effettuato un trattamento di dati personali in maniera non conforme ai principi di liceità, correttezza e trasparenza, in assenza di un idoneo presupposto normativo, non adempiendo all'obbligo di fornire preventivamente le informazioni all'interessato, in violazione degli artt. 5, par. 1, lett. a), 9, 12 e 13 del RGPD e dell'art. 7 del regole deontologiche per trattamenti a fini statistici e di ricerca scientifica. Il Garante ha altresì rilevato la violazione dei principi di responsabilizzazione e di protezione dei dati fin dalla progettazione, non avendo garantito, attraverso indicatori misurabili, l'implementazione di idonee misure volte, da una parte, ad istruire i propri addetti, dall'altra a garantire l'effettiva applicazione dei richiamati principi di liceità e trasparenza (artt. 5, par. 2, 24, 25 e 32 del RGPD), nonché la violazione degli artt. 29 del RGPD e 2-*quaterdecies* del Codice per aver consentito ai propri incaricati di trattare dati personali sotto la propria responsabilità, in assenza di specifiche designazioni e istruzioni e per non aver vigilato sul loro operato (provv. 27 novembre 2025, n. 704, doc. web n. 10201426).

Attività consultiva - PMA

In materia di ricerca scientifica, il Garante ha reso un parere sullo schema di decreto del Ministro della salute recante modifiche al d.m. 7 ottobre 2005 istitutivo del registro nazionale delle strutture autorizzate all'applicazione delle tecniche di procreazione medicalmente assistita (PMA) e relativo disciplinare tecnico che ne costituisce parte integrante, istituito presso l'Istituto superiore di sanità, ai sensi della l. n. 40/2004.

Le modifiche riguardavano principalmente il sistema di raccolta dei dati, prevedendo il superamento dell'attuale modalità aggregata in favore della raccolta dei dati relativi al singolo ciclo di trattamento, al fine di migliorare la qualità, la completezza e l'accuratezza delle analisi epidemiologiche, nonché la valutazione dell'efficacia delle tecniche di pseudonimizzazione applicate. Ciò consente di evitare duplicazioni e di monitorare il fenomeno della mobilità delle pazienti, assicurando al contempo il rispetto dei principi di minimizzazione, di esattezza e integrità dei dati.

Il Ministero ha recepito le indicazioni fornite dall'Autorità nel corso delle numerose interlocuzioni, che hanno riguardato in particolare: la verifica della necessità e proporzionalità dei trattamenti; la corretta indicazione della natura dei dati trattati, pseudonimizzati o anonimizzati; l'indicazione dei tempi di conservazione e le misure tecniche e organizzative adottate, anche alla luce della valutazione d'impatto effettuata dall'ISS ai sensi dell'art. 35 del RGPD. In considerazione delle garanzie previste e delle modifiche introdotte, il Garante, nell'esprimere parere favorevole, ha ritenuto che lo schema di decreto e il relativo disciplinare tecnico assicurassero un adeguato livello di tutela dei diritti e delle libertà fondamentali degli interessati (provv. 27 marzo 2025, n. 163, doc. web n. 10126164).

7 La statistica

Programma statistico nazionale 2023-2025

Il Garante ha espresso parere favorevole sullo schema di Programma statistico nazionale 2023-2025 - aggiornamento 2024-2025, presentato dall'Istituto nazionale di statistica ai sensi dell'art. 58, par. 3, lett. b), RGPD e dell'art. 6-*bis*, d.lgs. n. 322/1989 nonché dell'art. 4-*bis* delle regole deontologiche per i trattamenti a fini statistici o di ricerca scientifica nell'ambito del Sistema statistico nazionale. L'aggiornamento comprende 820 lavori statistici, di cui 27 di nuova introduzione, da realizzarsi prevalentemente a cura dell'ISTAT e degli altri uffici di statistica facenti parte del SISTAN, in un contesto ancora caratterizzato dall'analisi degli effetti della pandemia, dalla crisi energetica e dalle esigenze informative connesse all'attuazione del PNRR. Nel corso dell'istruttoria, l'Autorità aveva preso atto delle modifiche apportate ai prospetti informativi dei singoli lavori statistici, rilevando un miglioramento nella descrizione delle finalità, delle categorie di dati trattati, dei tempi di conservazione, dei ruoli dei soggetti coinvolti. Era stato inoltre valorizzato il ruolo di coordinamento e formazione dei soggetti del sistema statistico nazionale da parte dell'ISTAT.

Il Garante aveva peraltro evidenziato la persistenza di taluni profili di criticità concernenti, in particolare, l'indicazione delle misure tecniche e organizzative adottate dai diversi soggetti SISTAN per garantire l'effettiva applicazione dei principi di minimizzazione e di integrità e riservatezza dei dati, nonché la perdurante assenza del decreto ministeriale previsto dall'art. 2-*octies* del Codice in materia di trattamento di dati relativi a condanne penali e reati, che incide sulla piena operatività di taluni lavori statistici.

All'esito dell'istruttoria, tenuto conto delle modifiche apportate dall'ISTAT in sostanziale conformità alle indicazioni fornite dall'Ufficio, l'Autorità ha ritenuto comprovate la necessità e la proporzionalità dei trattamenti previsti nel programma statistico in esame, esprimendo parere favorevole (provv. 27 febbraio 2025, n. 91, doc. web n. 10114317).

Il Garante ha espresso altresì parere favorevole condizionato sullo schema di Programma statistico nazionale 2023-2025 – aggiornamento 2025, presentato dall'ISTAT, ai sensi dell'art. 58, par. 3, lett. b), RGPD, art. 6-*bis*, d.lgs. n. 322/1989, nonché art. 4-*bis* delle regole deontologiche per i trattamenti statistici e di ricerca scientifica nell'ambito del SISTAN. Tale aggiornamento comprende 234 lavori, di cui 34 di nuova introduzione.

L'Autorità ha preso atto dei miglioramenti apportati dall'ISTAT, con particolare riguardo all'aggiunta di archivi, di fonti amministrative e/o di variabili alle rilevazioni statistiche contenute nel Programma, alle misure adottate al fine di garantire i diritti e le libertà degli interessati e all'aumento dei tempi di conservazione.

In particolare, il Garante ha ritenuto comprovate la necessità e proporzionalità dei trattamenti effettuati e l'adeguatezza delle misure adottate, pur ribadendo la necessità di continuare a implementare, laddove possibile, le misure di pseudonimizzazione, volte a garantire l'effettiva applicazione dei principi di minimizzazione, di integrità e riservatezza dei dati.

Il Garante ha, altresì, preso favorevolmente atto delle modifiche apportate a singoli lavori statistici, in merito ai quali, in sede di preliminari interlocuzioni con l'Istituto, aveva rilevato profili di criticità, con particolare riferimento all'utilizzo del *web scraping* per la raccolta dei dati da utilizzare nelle rilevazioni statistiche (al momento espunti) e alle misure adottate per garantire la tutela dei minori (provv. 9 ottobre 2025, n. 580, doc. web n. 10191303).

PSTN

Il Garante ha espresso parere favorevole condizionato sullo schema di Programma statistico provinciale 2025-2027 della Provincia autonoma di Trento (PSTN), ad eccezione del lavoro statistico "IND-0465 Rilevamento flussi e calcolo indicatori statistici del traffico veicolare provinciale".

Il PSTN, predisposto dall'ISPAT, individua i lavori statistici di interesse provinciale non inclusi nel Programma statistico nazionale che prevedono trattamenti di dati personali. L'istruttoria dell'Autorità ha riguardato il rispetto dei principi di liceità e trasparenza, di minimizzazione, di limitazione della finalità e di integrità e riservatezza dei dati.

Nel corso delle interlocuzioni informali, l'ISPAT ha integrato il PSTN con una parte introduttiva più chiara, tenuto conto che il Programma statistico funge anche da informativa agli interessati in caso di raccolta dei dati presso terzi (art. 14 del RGPD). Sono state inoltre migliorate le sezioni relative ai tempi di conservazione, alle tecniche di pseudonimizzazione e alla *k-anonymity*, e introdotte specifiche misure organizzative e tecniche per garantire l'effettiva applicazione del principio di integrità e riservatezza. Ciò nonostante, il Garante ha subordinato il parere favorevole a specifiche condizioni concernenti la necessità: i) di specificare, anche nelle informative fornite ai sensi dell'art. 13 del RGPD, che non è riconosciuto agli interessati il diritto di opposizione, trattandosi di trattamenti svolti in esecuzione di un compito di interesse pubblico (art. 21, par. 6, RGPD); ii) di applicare le misure tecniche di pseudonimizzazione e di *k-anonymity* all'intero ciclo del trattamento statistico; iii) di garantire che altri obiettivi perseguiti dal "progetto RMT-PAT" sarebbero stati realizzati esclusivamente attraverso dati aggregati e anonimizzati e iv) di rimuovere ogni singolarità, qualora, con qualsiasi mezzo, il titolare del trattamento ne venga a conoscenza in una fase successiva all'applicazione delle predette tecniche, tenendo traccia di tali eventi e ripetendo in tale circostanza la valutazione del rischio di re-identificazione alla luce delle cause che hanno determinato l'insorgenza di tale singolarità.

Il Garante ha, invece, ritenuto di dover sospendere il lavoro statistico "IND-0465 Rilevamento flussi e calcolo indicatori statistici del traffico veicolare provinciale" e di avviare una specifica istruttoria su di esso. Dall'esame della documentazione trasmessa è infatti emersa la persistenza di criticità relative, in particolare, alla proporzionalità dei trattamenti, alla effettiva applicazione dei principi di minimizzazione dei dati, di integrità e riservatezza e alle garanzie previste ai sensi dell'art. 89 del RGPD per gli interessati, anche in considerazione della possibile raccolta di particolari categorie di dati.

Con riferimento alle tecniche di anonimizzazione dei dati nell'ambito di tale lavoro statistico, il Garante ha rilevato la necessità di acquisire ulteriori elementi in ordine alle metriche adottate, nelle diverse fasi del trattamento (anche mediante esemplificazioni), per la stima della probabilità di re-identificazione degli interessati (provv. 13 novembre 2025, n. 666, doc. web n. 10202046).

Accertamenti ispettivi

Meritano in questa sede di essere evidenziati due provvedimenti adottati a seguito di accertamenti ispettivi svolti nei confronti degli uffici di statistica di due regioni.

Con il primo provvedimento, l'Autorità ha accertato l'illiceità dei trattamenti effettuati nell'ambito di un lavoro statistico regionale inserito nel Programma statistico nazionale. Il Garante ha in particolare rilevato la violazione dell'obbligo di adottare un accordo di contitolarità e, conseguentemente, quello di metterne il contenuto a disposizione degli interessati ai sensi dell'art. 26, parr. 1 e 2 del RGPD (artt. 5, par. 2 e 26, parr. 1 e 2 del RGPD) nonché la violazione del principio di responsabilizzazione. Con riguardo a quest'ultimo aspetto, la regione aveva omesso di implementare misure volte a prevenire il rischio di re-identificazione degli interessati in fase di diffusione, allor quando le

variabili rilevate risultavano coincidenti con una sola unità statistica, in particolare non rispettando la cd. regola del 3 (art. 5, par. 2, RGPD). Tale situazione aveva comportato altresì una diffusione di dati personali in assenza di idonea base giuridica, in violazione del principio di liceità, di cui agli artt. 5, par. 1 lett. a), par. 2, RGPD e 2-*ter* del Codice. Il provvedimento sanzionatorio adottato nei confronti della regione tiene conto delle misure correttive adottate dall'amministrazione successivamente ai rilievi dell'Autorità (provv. 29 aprile 2025, n. 275, doc. web n. 10147841).

Il secondo provvedimento ha riguardato i trattamenti effettuati nell'ambito della rilevazione statistica "Movimento dei clienti negli esercizi ricettivi – IST-00139", di titolarità di ISTAT, per la quale la Regione Lazio - ufficio di statistica opera quale responsabile del trattamento. Nel corso degli accertamenti, è emerso che la Regione non aveva designato la società *in house*, che gestisce la piattaforma con cui vengono raccolti i dati, come sub-responsabile del trattamento ed aveva omesso di informare il titolare del trattamento (ISTAT), con compromissione della piena possibilità per quest'ultimo di esercitare un controllo effettivo sulla catena dei trattamenti e sui soggetti coinvolti. Tenuto conto della natura colposa della condotta, dell'assenza di effetti negativi significativi sugli interessati, della collaborazione prestata nel corso del procedimento e dell'adozione di misure correttive (tra cui la trasmissione di uno schema contrattuale di nomina a sub-responsabile), l'Autorità nel dichiarare l'illiceità del trattamento per la violazione dell'art. 28 del RGPD ha disposto l'ammonimento nei confronti della Regione (provv. 4 giugno 2025, n. 326, doc. web n. 10164379).

8 I trattamenti in ambito giudiziario e di sicurezza

8.1. *Trattamenti in ambito giudiziario*

Trattamenti di dati relativi alla salute

Con provvedimento 16 gennaio 2025, n. 27 (doc. web n. 10132315) è stato comminato l'ammonimento a un magistrato tributario per aver trattato illecitamente dati particolari di un collega, nell'ambito della gestione delle pratiche relative agli stalli di parcheggio riservati ai magistrati in servizio presso l'ufficio giudiziario. Il reclamante aveva lamentato che il magistrato avesse illegittimamente comunicato a terzi – colleghi del reclamante interessati alla fruizione dei parcheggi riservati – la circostanza che egli fosse affetto da disabilità, in ritenuta violazione delle disposizioni sul trattamento dei dati relativi alla salute di cui all'art. 9 del RGPD e all'art. 2-*septies* del Codice. Nel provvedimento è stato rilevato, tra l'altro, che le comunicazioni erano state effettuate in violazione del principio di minimizzazione dei dati, di cui all'art. 5, comma 1, lett. c), RGPD, ai sensi del quale i dati personali oggetto di trattamento devono essere limitati a quanto necessario rispetto alle finalità per le quali sono trattati. A tale proposito, l'Autorità ha osservato che se la finalità del trattamento effettuato dal magistrato era quella di informare i potenziali terzi interessati del parziale ripristino della disponibilità dello stallo di parcheggio già in uso esclusivo del reclamante, ciò poteva essere realizzato senza dover ostendere l'informazione relativa alla parziale disponibilità dello stallo anche in favore del reclamante, in quanto persona diversamente abile.

Trattamenti effettuati da ausiliari del giudice

Diversi i casi portati all'attenzione dell'Autorità, tramite reclami o segnalazioni, riguardanti trattamenti effettuati da ausiliari del giudice, quali consulenti tecnici d'ufficio (CTU), custodi, cancellieri, ufficiali giudiziari, delegati alle vendite giudiziarie. All'esito dell'istruttoria, i relativi reclami e segnalazioni sono stati archiviati con provvedimento dirigenziale per incompetenza del Garante. Occorre infatti considerare che sia il RGPD (art. 55, par. 3), sia il Codice (art. 154, comma 7), sia l'art. 37, d.lgs. n. 51/2018, dispongono che le autorità di controllo, come il Garante, non sono competenti per la valutazione dei trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni giurisdizionali, al fine di salvaguardare l'indipendenza della magistratura nell'adempimento dei suoi compiti giurisdizionali (cons. 20, RGPD). L'incompetenza dell'Autorità si estende anche ai trattamenti di dati effettuati dagli ausiliari del giudice, alla stregua della normativa di settore che riconosce a tali figure un importante ruolo di assistenza del giudice nello svolgimento delle sue funzioni giudiziali e ne prevede l'operato sotto la direzione e il controllo dell'autorità giudiziaria (cfr. con riguardo alla figura del consulente tecnico, l'art. 61 c.p.c.; per il custode giudiziario, l'art. 65 c.p.c.; per gli altri ausiliari l'art. 68 c.p.c.; per il professionista delegato alla vendita nell'esecuzione immobiliare, l'art. 591-*bis* c.p.c. e per l'amministratore giudiziario, l'art. 592 c.p.c.).

Trattamenti in ambito forense

Con provvedimento 21 maggio 2025, n. 310 (doc. web n. 10167804), il Garante ha definito un reclamo presentato nei confronti di un avvocato per avere inviato tramite e-mail, nell'ambito di una procedura di pignoramento presso terzi, documentazione recante informazioni personali della reclamante anche ad altri dipendenti del medesimo

ufficio. Tale comunicazione di dati personali dell'interessata ad altri destinatari in assenza di una idonea base giuridica, configurando un trattamento in violazione degli artt. 5, comma 1, lett. a), e 6 del RGPD, ha condotto alla definizione del reclamo con l'ammonimento del titolare.

Con provvedimento 18 dicembre 2025, n. 767 (doc. web n. 10216406), il Garante ha ammonito un avvocato che, nella presentazione di un esposto, aveva utilizzato un link di condivisione dei dati personali dei suoi patrocinati senza adottare l'opzione restrittiva per l'accesso, per cui chiunque ne fosse stato a conoscenza avrebbe potuto avere accesso ai documenti condivisi. Ciò ha comportato la violazione dell'art. 5, par. 1, lett. f), RGPD, e dell'art. 32 del RGPD, che pone in capo al titolare del trattamento l'obbligo dell'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio. Queste misure includono, tra le altre, la pseudonimizzazione e la cifratura dei dati personali, la capacità di garantire riservatezza, integrità, disponibilità e resilienza del sistema.

Con provvedimento 23 ottobre 2025, n. 629 (doc. web n. 10199088), il Garante ha ammonito un avvocato che aveva inviato una diffida riguardante questioni personali dell'interessato utilizzando l'indirizzo di posta elettronica dell'istituzione presso cui il medesimo lavorava e non a un recapito di posta elettronica personale riferibile all'interessato o al suo indirizzo fisico, così da consentire l'ostensione di tali dati personali a terzi che non ne erano legittimi destinatari, in specie al dipendente dell'istituto addetto al controllo della casella PEC istituzionale. Inoltre, l'interessato non era un professionista e, come tale, non era destinatario di alcun obbligo legale a dotarsi di domicilio digitale che, in effetti, non era presente in elenchi pubblici. Pertanto, il Garante ha ritenuto il trattamento illecito, in quanto posto in essere in violazione degli artt. 5, par. 1, lett. a) e 6 del RGPD, per non avere il titolare trattato i dati del reclamante in modo lecito, corretto e trasparente (art. 5, cit.) e per aver effettuato il trattamento sopra descritto in assenza delle condizioni di liceità previste dal predetto art. 6.

Produzione di dati in giudizio

Nel 2025 sono stati presentati all'attenzione del Garante numerosi reclami e 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 in conformità all'art. 160-*bis* del Codice secondo cui 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.

8.2. *Trattamenti da parte di forze di polizia*

Con provvedimento 13 febbraio 2025, n. 86 (doc. web n. 10132272), è stata definita la segnalazione relativa alla diffusione, tramite la copia digitale del numero di aprile 2024 della rivista Poliziamoderna, organo ufficiale della Polizia di Stato, dei nominativi di diverse persone assoggettate a provvedimenti di polizia. All'esito dell'istruttoria è stato appurato che l'illecito era stato originato da un errore occorso durante la revisione dei testi in pubblicazione. Il titolare del trattamento, Ministero dell'interno - Dipartimento della pubblica sicurezza, a seguito dell'apertura dell'istruttoria da parte del Garante, aveva tempestivamente inibito l'accesso alle pubblicazioni in argomento e adottato misure organizzative atte a evitare il ripetersi di tali eventi; per tale motivo, anche in ragione dell'evidente assenza di dolo nella condotta, il procedimento è stato definito con l'ammonimento del titolare.

Altri reclami hanno riguardato trattamenti di dati personali effettuati da personale

delle forze di polizia impegnate nell'esercizio di funzioni di polizia giudiziaria; tali reclami, dopo attenta istruttoria, sono stati archiviati con provvedimento dirigenziale per incompetenza del Garante ai sensi dell'art. 37, comma 6, d.lgs. n. 51/2018, in quanto i trattamenti effettuati dagli organi di polizia giudiziaria afferivano allo svolgimento delle funzioni giurisdizionali , sottratte al controllo dell'autorità di protezione dati (v. par. 8.1).

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 decreti 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, del medesimo decreto n. 51/2018, il Garante, nel corso del 2025, ha espresso i seguenti pareri:

- parere 25 settembre 2025, n. 565 (doc. web n. 10219819), su uno schema di decreto del MEF, contenente le regole tecnico-operative relative alle udienze da remoto nei processi telematici instaurati innanzi alle corti di giustizia tributaria di primo e di secondo grado (cd. processo tributario telematico); il parere era stato richiesto per la necessità di adeguare tempestivamente le regole tecniche per lo svolgimento da remoto delle udienze e delle camere di consiglio, a causa dell'obsolescenza tecnologica del software in uso (Skype *for Business*), per il quale la società produttrice (Microsoft) aveva deciso di interrompere le attività di aggiornamento informatico e della sicurezza, con il rischio di rendere il sistema estremamente vulnerabile agli attacchi informatici. Il Ministero aveva ritenuto, pertanto, di utilizzare un'altra piattaforma informatica (Microsoft Teams), in sostituzione di quella obsoleta, prevista nel precedente decreto direttoriale. Sullo schema di decreto il Garante ha espresso parere favorevole;
- parere 18 dicembre 2025, n. 748 (doc. web n. 10232024), su uno schema di decreto direttoriale concernente il trattamento dei dati personali necessari all'esercizio delle competenze e al raggiungimento degli scopi connessi alla tenuta dell'elenco di cui all'art. 4 del decreto del Ministro della giustizia e dell'autorità politica delegata per le pari opportunità del 22 gennaio 2025 (cd. elenco CUAV - Centri per uomini autori o potenziali autori di violenza); esso, in particolare, era volto a disciplinare la formazione, tenuta ed aggiornamento dell'elenco degli enti e delle associazioni abilitati a organizzare percorsi di recupero destinati alle persone condannate per reati di violenza contro le donne e di violenza domestica. Lo schema sottoposto al parere del Garante costituiva una seconda bozza, nella quale erano state corrette le criticità presenti nella prima stesura ed evidenziate dall'Autorità nella fase istruttoria, riguardanti l'indicazione puntuale delle amministrazioni e le banche dati presso le quali potevano essere effettuati controlli sui dati contenuti nelle dichiarazioni sostitutive presentate dagli interessati, le modalità di verifica del possesso dei requisiti di onorabilità degli interessati e la corretta indicazione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento, in conformità alle disposizioni previste dal RGPD e dal Codice;
- parere 10 luglio 2025, n. 382 (doc. web n. 10168204), su tre schemi di decreti recanti specifiche tecniche concernenti, rispettivamente: le modalità operative per l'uso della banca dati delle aste giudiziarie (BDAG); le modalità di pubblicazione dei dati sul portale delle vendite pubbliche (PVP); le regole tecniche e operative per lo svolgimento della vendita dei beni mobili e immobili con modalità telematiche, previsti dall'art. 7, d.m. n. 99/2023, in attuazione del d.lgs. n. 149/2022 che aveva previsto l'istituzione, presso il Ministero della giustizia, di una banca dati relativa alle aste giudiziarie,

contenente i dati identificativi degli offerenti, i dati identificativi del conto bancario o postale utilizzato per versare la cauzione e il prezzo di aggiudicazione, nonché le relazioni di stima, rinviando ad un decreto ministeriale la determinazione delle modalità di acquisizione dei dati, le modalità di inserimento dei medesimi nella banca dati, nonché le modalità di esercizio del potere di vigilanza da parte del Ministero della giustizia. L'art. 7 del predetto decreto n. 99/2023, prevedeva, a sua volta, che con provvedimento del responsabile dei sistemi informativi e automatizzati del Ministero della giustizia, fossero emanate le specifiche tecniche relative all'inserimento dei dati nella banca dati e all'individuazione dei tempi di conservazione dei dati stessi, nonché le modalità di attribuzione delle utenze e di accesso alla banca dati da parte di tutti i soggetti abilitati e fossero aggiornate le specifiche tecniche previste dall'art. 161-*quater* delle disposizioni per l'attuazione del c.p.c. Il parere ha fatto seguito a quello precedente del 18 luglio 2024, n. 464 (doc. web n. 10063581, v. Relazione 2024, p. 108), reso dal Garante con riguardo a una prima versione dei provvedimenti in questione, che il Ministero aveva sottoposto ad aggiornamento e integrazione. Emerse alcune lacune di carattere prettamente tecnico, il Garante aveva rappresentato al Ministero la necessità che i primi due schemi fossero integrati prevedendo l'adozione di meccanismi per attenuare il rischio connesso all'attivazione fraudolenta di identità digitali SPID o certificati di autenticazione CNS intestati a utenti esterni (es. professionisti delegati alle vendite, curatori o liquidatori, commissionari) o a utenti interni (personale delle cancellerie degli uffici giudiziari, giudici dell'esecuzione), suscettibili di essere utilizzati per accessi abusivi e non autorizzati alla banca dati e al portale;

- parere 25 settembre 2025, n. 568 (doc. web n. 10199508), su uno schema di decreto interministeriale (interno-giustizia-MAECI) concernente il Sistema cd. *Entry/Exit,* EES istituito dal reg. UE 2017/2226 per la registrazione dei dati di ingresso e uscita e dei dati relativi al respingimento di cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto, da adottare ai sensi dell'art. 18, d.l. n. 69/2023. Quest'ultimo prevede che per l'adempimento delle disposizioni di cui all'art. 3, par. 1, punti 3), 4) e 26) del reg. (UE) 2017/2226, con uno o più decreti adottati dal Ministro dell'interno, di concerto con i Ministri degli affari esteri e della cooperazione internazionale e della giustizia, siano: a) determinate le autorità di frontiera, nonché quelle competenti in materia di immigrazione; b) designate le autorità responsabili per finalità di prevenzione, accertamento e indagine di reati di terrorismo o altri reati gravi; c) disciplinate le modalità tecniche di accesso, consultazione, inserimento, modifica e cancellazione dei dati nel sistema EES a cura dei soggetti autorizzati, di eventuale conservazione negli archivi o sistemi nazionali, nonché di comunicazione dei dati ai sensi dell'art. 41 del reg. (UE) 2017/2226. Il parere del Garante è stato frutto di interlocuzioni avutesi con il Ministero dell'interno durante l'istruttoria, nel corso delle quali sono state rese indicazioni ed osservazioni al fine di risolvere alcune criticità evidenziate e rendere lo schema pienamente in linea con i principi e le regole in materia di protezione dei dati personali. In particolare le indicazioni hanno riguardato, oltre che l'esigenza di un esaustivo coordinamento con la normativa sovranazionale di riferimento, cui il decreto dà attuazione (il citato reg. UE 2017/2226), i profili più strettamente attinenti alla protezione dei dati, come la normativa applicabile ai trattamenti effettuati in applicazione del decreto per le diverse finalità (immigrazione e *law enforcement*), la corretta indicazione dei titolari del trattamento e il riferimento ai pertinenti obblighi previsti a carico di questi ultimi (cfr. artt. 9 e 10). Lo schema trasmesso da ultimo per il parere si è conformato a gran parte delle indicazioni rese nel corso dell'istruttoria; nondimeno residuavano aspetti meritevoli di perfezionamento, sicché il Garante, preso atto della sostanziale

conformità dello schema alla normativa in materia di protezione dei dati personali, ha espresso parere favorevole sul proposto schema di decreto interministeriale, a condizione che fosse perfezionato nei termini riportati nel provvedimento.

Nel periodo considerato sono stati inoltre adottati i richiesti pareri su alcuni schemi di valutazione di impatto, e in particolare:

- parere 13 novembre 2025, n. 664 (doc. web n. 10219555), sulla valutazione di impatto presentata dal Ministero della giustizia e relativa al collegamento telematico fra la sala situazioni del dipartimento dell'amministrazione penitenziaria (DAP) del Ministero e la sala regia degli istituti penitenziari, volto a consentire la visione delle immagini riprese dai sistemi di videosorveglianza presenti negli istituti penitenziari in situazioni di criticità. L'Autorità ha ritenuto legittima la finalità del trattamento, consistente nel mantenimento dell'ordine e della sicurezza nelle strutture penitenziarie, fermo restando che il sistema non prevedeva un controllo permanente, indiscriminato o a campione e che in sede centrale non era prevista alcuna archiviazione dei dati, delle immagini di videosorveglianza ed in generale dei flussi informatici, né registrazione delle riprese audio/video;

- parere 4 dicembre 2025, n. 743 (doc. web n. 10221993), sulla valutazione di impatto relativa all'utilizzo di dispositivi *bodycam* da parte degli agenti di Polizia locale del Comune di Pescara. Il Garante ha espresso parere non favorevole anche sulla quarta versione della valutazione di impatto sulla protezione dei dati del progetto, rispetto al quale aveva segnalato al Comune la necessità di apportare diversi correttivi; nonostante ciò, anche nell'ultima versione erano rimaste numerose e rilevanti criticità, più volte segnalate al Comune. Oltre a indicazioni contraddittorie in merito alle fonti di legittimazione del trattamento, alla mancata indicazione della durata della conservazione dei file di log e all'indicazione dei motivi della presenza di SIM all'interno delle *bodycam*, permanevano ulteriori criticità in tema di sicurezza delle soluzioni tecnologiche scelte. In particolare, per la gestione dei dati il Comune intendeva avvalersi di un prodotto fornito da un'azienda statunitense, completamente in cloud. Sebbene il produttore avesse dichiarato di adoperare tecniche crittografiche sui dati a riposo e durante la trasmissione, non erano stati forniti sufficienti dettagli tecnici sul processo di gestione delle chiavi crittografiche funzionali ad escludere l'accesso ai dati del titolare in chiaro da parte del fornitore del servizio. L'eventuale accesso remoto a tali sistemi di trattamento ed ai dati ivi contenuti da parte di soggetti stabiliti al di fuori dell'Unione europea avrebbe configurato, ove non escluso, un trasferimento di dati verso paesi terzi, in violazione dell'art. 31, comma 1, lett. b), d.lgs. n. 51/2018, secondo cui, nell'ambito dei trattamenti rientranti nel capo di applicazione della direttiva 680/2016, i dati personali possono essere trasferiti ad un soggetto in un paese terzo o a un'organizzazione internazionale che sia un'autorità competente per le finalità di *law enforcement*, competenza non ascrivibile all'azienda statunitense fornitrice del sistema in cloud;

- parere favorevole al Ministero dell'interno - Dipartimento della pubblica sicurezza 4 agosto 2025, n. 455 (doc. web n. 10165349) sulla valutazione di impatto di un sistema di analisi ed elaborazione dati a supporto delle indagini patrimoniali, denominato CEREBRO in uso alla Polizia di Stato. Tale sistema è una piattaforma software centralizzata a supporto delle "indagini patrimoniali" che opera attraverso due funzionalità: l'acquisizione dei dati da fonti istituzionali "esterne", cioè di altri soggetti istituzionali, e l'elaborazione dei dati acquisiti, sia quelli provenienti da tali fonti che quelli immessi dal personale addetto al controllo per evidenziare possibili disponibilità finanziarie e patrimoniali "sproporzionate" e quindi potenzialmente riconducibili ad attività illecite. Il predetto parere favorevole dell'Autorità ha fatto seguito a diverse interlocuzioni con il Dipartimento della pubblica sicurezza, finalizzate al perfezionamento

della valutazione di impatto sulla protezione dei dati e alla sua integrazione con misure idonee a garantire l'esercizio dei diritti degli interessati, in particolare l'informativa (di cui è prevista la pubblicazione sul sito della Polizia di Stato) e i diritti di accesso, rettifica e cancellazione.

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

A seguito di reclami e segnalazioni, nel 2025 l'Autorità, nei limiti delle proprie competenze, ha assicurato il riscontro da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e di uffici periferici di polizia alle richieste degli interessati, sia di accesso e comunicazione dei dati conservati presso il CED, sia di eventuale rettifica o cancellazione degli stessi, nel rispetto delle disposizioni previste dal d.gs. n. 51/2018 e dall'art. 10, l. n. 121/1981, cui fanno rinvio gli artt. 47 e 48 del medesimo decreto.

In tale ambito, di sicuro rilievo è stato il provv. 10 aprile 2025, n. 237 (doc. web n. 10231983), adottato a conclusione di un procedimento di reclamo con cui l'interessato aveva lamentato la persistente registrazione nel CED di dati e informazioni relativi a provvedimenti giudiziari a sé riferiti e risalenti nel tempo. Con tale provvedimento, accertata l'illiceità del trattamento ai sensi dell'art. 37, comma 3, lett. d), d.lgs. n. 51/2018, l'Autorità ha ingiunto al Dipartimento della pubblica sicurezza la cancellazione dal CED dei dati relativi ad una sentenza di estinzione del reato, emessa in favore del reclamante, per decorrenza dei termini di conservazione e ha prescritto la misura correttiva dell'ammonimento (violazione artt. 3, comma 1, lett. e) e 12, comma 2, d.lgs. n. 51/2018). In esecuzione del provvedimento, il Dipartimento della pubblica sicurezza ha comunicato di aver provveduto alla cancellazione dei dati in questione, in favore dell'interessato.

Tale affare rappresenta il "caso-pilota" nella complessa materia del trattamento dei dati registrati nel CED del Dipartimento della pubblica sicurezza e, in particolare, in tema di conservazione dei dati per un tempo limitato e proporzionato ex art. 3, comma 1, lett. e), d.lgs. n. 51/2018 (principio di limitazione della conservazione) e comunque non oltre il termine stabilito dalla normativa di settore, rappresentata dal d.P.R. n. 15/2018, decorso il quale il titolare ha l'obbligo di cancellare il dato ai sensi dell'art. 12, comma 2, del medesimo d.lgs. n. 51/2018.

8.5. *Il controllo sul Sistema di informazione Schengen*

Il Sistema di informazione Schengen (SIS) permette alle autorità nazionali di polizia, di controllo delle frontiere e doganali di scambiarsi agevolmente informazioni e segnalazioni su persone verosimilmente coinvolte in reati gravi o 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.

Nel periodo considerato, in relazione alle attività di controllo riservate all'Autorità sui trattamenti effettuati sui dati personali registrati nel SIS, il Garante ha continuato a curare il monitoraggio del periodico flusso di istanze e comunicazioni provenienti dagli interessati e dalle autorità coinvolte (Dipartimento della pubblica sicurezza - Servizio informativo interforze - Divisione NSIS), al fine di verificare che l'elaborazione e l'uti-

lizzazione dei dati inseriti negli archivi SIS non leda i diritti delle persone ai sensi degli artt. 52, 53 e 54 del reg. (UE) 2018/1861, e 67 e 68 del reg. (UE) 2018/1862, in relazione alle disposizioni nazionali pertinenti del d.lgs. n. 51/2018.

Il Garante ha poi contribuito all'elaborazione del *Joint Report of Schengen Information System 2024* raccogliendo sia i dati nazionali di competenza dell'Autorità che quelli messi a disposizione dal Ministero dell'interno, in ottemperanza all'obbligo recentemente introdotto per gli Stati membri di comunicare al CEPD entro il 31 marzo di ogni anno le statistiche sull'esercizio dei diritti degli interessati relative al SIS. In particolare sono state rendicontate le richieste di accesso, rettifica e cancellazione.

Inoltre, con riguardo agli aspetti di comunicazione istituzionale di pertinenza, l'Autorità ha provveduto ad aggiornare la pagina informativa pubblicata sul sito del Garante recante indicazioni sul funzionamento del SIS e sulle corrette modalità di esercizio, da parte degli interessati, dei diritti di accesso, rettifica e cancellazione sui dati personali registrati nel SIS, ai sensi dei citati regolamenti. L'Autorità ha pubblicato sul sito anche la modulistica da utilizzare per l'esercizio di tali diritti, redatta – in linea con le indicazioni rese a livello europeo – in stretta collaborazione con il Ministero dell'interno - Dipartimento della pubblica sicurezza - Divisione NSIS che è l'autorità centrale competente sulla sezione nazionale del SIS, cui devono essere indirizzate le richieste in questione.

9 L'attività giornalistica

L'Autorità ha continuato a riservare particolare attenzione ai temi legati alla libertà di espressione, svolgendo un costante lavoro di bilanciamento tra il diritto all'informazione, da un lato, e la tutela dell'identità personale e dei dati personali, dall'altro. Tale attività si è concretizzata nell'analisi di un numero significativo di reclami e segnalazioni riguardanti presunte violazioni connesse alla diffusione di notizie online e sui social media da parte degli organi di informazione.

9.1. *Profili generali*

Le istanze pervenute all'Autorità in questo ambito sono risultate sostanzialmente equivalenti, per numero, tra segnalazioni e reclami. In alcuni casi è stato necessario richiedere la loro regolarizzazione, a causa della mancanza dei requisiti formali e sostanziali previsti dalla normativa, in particolare per l'assenza dell'interpello preventivo richiesto quando l'interessato intende esercitare i diritti previsti dagli artt. 15-22 del RGPD.

Un numero rilevante di segnalazioni, a seguito di una valutazione preliminare, ha dato luogo all'avvio di istruttorie, laddove sono stati individuati elementi idonei a configurare possibili violazioni della normativa.

Sono inoltre pervenute istanze di natura mista, quali diffide e interpelli preventivi indirizzati direttamente ai titolari del trattamento e trasmessi per conoscenza all'Autorità, nonché segnalazioni provenienti dall'autorità giudiziaria relative a ipotesi di reato con possibili implicazioni in materia di protezione dei dati personali.

Una parte consistente dei reclami definiti nel 2025 ha riguardato richieste rivolte ai gestori dei motori di ricerca, soprattutto Google, per numero e rilevanza dei casi, finalizzate alla deindicizzazione di contenuti associati al nominativo degli interessati (*delisting*). Non sono mancate, tuttavia, istanze relative ad altri motori di ricerca, tra cui Microsoft Corporation e Verizon Media Emea Limited, titolare del motore Yahoo!.

Un'altra quota significativa di reclami ha avuto come destinatari gli organi di informazione (testate giornalistiche, blog, siti web informativi, ecc.). In tali circostanze, le doglianze hanno riguardato principalmente la pubblicazione di articoli contenenti dati personali ritenuti eccedenti rispetto al principio di essenzialità dell'informazione, nonché la diffusione di informazioni in violazione di specifici limiti, come nel caso di dati sanitari o relativi a minori. Ulteriori interventi hanno riguardato la pubblicazione di fotografie, commenti e video, anche sui social network, in assenza del consenso dell'interessato o di un'adeguata base giuridica.

Per quanto concerne l'esercizio dei diritti previsti dagli artt. 15-22 del RGPD, si è registrata in diversi casi la collaborazione dei titolari del trattamento, che hanno accolto le richieste dei reclamanti a seguito dell'intervento dell'Autorità in fase istruttoria. Ciò ha consentito, nella maggior parte delle situazioni, di definire i reclami senza necessità di adottare provvedimenti collegiali.

Nei casi in cui si è reso necessario l'intervento del Collegio dell'Autorità, quest'ultimo

ha operato un attento bilanciamento tra le esigenze individuali e l'interesse pubblico alla diffusione delle informazioni, ricorrendo, ove opportuno, ai poteri correttivi previsti dal RGPD.

Infine, nelle situazioni caratterizzate da violazioni particolarmente gravi, il Garante ha applicato anche sanzioni pecuniarie, tenendo conto delle specificità connesse all'esercizio di tali poteri in un ambito particolarmente delicato come quello della libertà di espressione.

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

9.2.1. Dati giudiziari

Nel corso del periodo di riferimento l'Autorità si è dedicata al tema del trattamento dei dati giudiziari da parte di testate giornalistiche e siti di informazione, attraverso un proporzionato e corretto giudizio di bilanciamento tra il trattamento dei dati giudiziari e la salvaguardia delle esigenze informative connesse a fatti di cronaca di pubblico interesse.

In un caso, l'Autorità ha preso atto dell'aggiornamento effettuato dal titolare nel titolo dell'articolo e financo nell'intestazione del relativo URL e, con riferimento alla richiesta di deindicizzazione, ha valutato che non vi fossero i presupposti per procedere in tal senso, ritenendo il reclamo infondato in ragione dell'attualità della vicenda giudiziaria ancora in corso e dell'interesse pubblico alla notizia stante gli incarichi istituzionali ricoperti dal reclamante (provv. 29 aprile 2025, n. 254, doc. web n. 10146249).

In un'altra fattispecie, l'Autorità – nel prendere atto dell'adesione manifestata dal titolare alla richiesta di deindicizzazione dell'interessato – ha ritenuto proporzionata la misura dell'ammonimento per aver lo stesso diffuso, a corredo visivo di uno degli articoli pubblicati su una testata giornalistica, una foto raffigurante l'ingresso in carcere del reclamante, sottoposto all'uso di manette ai polsi, benché non direttamente inquadrate; tale immagine è risultata idonea a far ritenere il soggetto in essa ritratto inequivocabilmente sottoposto a misura restrittiva della libertà, ledendone la dignità (provv. 18 dicembre 2025, n. 786, doc. web n. 10234245).

In diverse ipotesi, inoltre, l'Autorità ha ritenuto infondate le richieste di esercizio del diritto all'oblio e di deindicizzazione avanzate nei confronti di editori, in considerazione della pendenza del procedimento penale a carico dell'interessato e dell'attinenza dell'attività professionale svolta dal medesimo rispetto ai presunti reati oggetto del procedimento (provv.ti 27 marzo 2025, n. 180, doc. web n. 10144955 e n. 181, doc. web n. 10145219. Entrambi i provvedimenti sono oggetto di impugnazione)

Avverso il diniego a una richiesta di deindicizzazione di un articolo rivolta a un editore, l'Autorità non ha accolto il relativo reclamo valutando, nel caso di specie, sproporzionata la misura richiesta all'editore, l'accoglimento della quale avrebbe determinato la rimozione totale di articoli di rilevante e perdurante interesse pubblico riguardanti una pluralità di soggetti oltre ai reclamanti e non solo la loro irreperibilità in associazione al nome e cognome dei reclamanti stessi - come invece sarebbe stato il caso ove una richiesta analoga fosse stata rivolta a un motore di ricerca. Il Garante ha tuttavia aggiunto che nelle circostanze della fattispecie resta salvo il diritto all'aggiornamento della notizia (provv. 27 novembre 2025, n. 711, doc. web n. 10211757).

9.2.2. Dati relativi a minori

La tutela dei minori è stata una priorità anche nel corso del 2025, con particolare riguardo al rispetto delle garanzie previste dalle regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica pubblicate ai sensi

dell'art. 20, comma 4, d.lgs. 10 agosto 2018 (art. 7) e dalla Carta di Treviso al fine di tutelare la dignità, la personalità e il diritto alla riservatezza del minore. In tale contesto, si collocano due reclami con i quali è stata lamentata la pubblicazione, sul sito Internet nonché sui canali social di un'associazione e di una federazione sportiva, della versione integrale di una decisione disciplinare adottata dal competente tribunale federale, contenente i dati personali di una minore (nome, cognome e numero di tesseramento). L'Autorità, nel comminare una sanzione amministrativa pecuniaria ai titolari coinvolti nella vicenda, ha ritenuto opportuno ingiungere agli stessi di adottare ogni misura idonea a garantire la conformità ai principi di liceità e correttezza, di limitazione delle finalità e di minimizzazione dei dati dei trattamenti dei dati personali relativi a soggetti minorenni, al fine di impedirne l'identificazione, anche in relazione ad un'eventuale diffusione in rete (provv.ti 17 luglio 2025, n. 446, doc. web n. 10172305 e n. 447, doc. web n. 10172356).

È altresì pervenuto all'Autorità un reclamo avente ad oggetto la pubblicazione sui social network di terzi di fotografie ritraenti la figlia minore della reclamante, nonostante i ripetuti inviti a cancellare le immagini postate. L'Autorità ha ritenuto illecito il descritto trattamento in quanto la pubblicazione delle fotografie oggetto di doglianza era stata effettuata in assenza del consenso dei genitori della minore ritratta. È stato, dunque, disposto il divieto di ulteriore trattamento, ivi compresa la contestata pubblicazione delle immagini della minore precedentemente postate sui predetti profili social ed è stato, altresì, rivolto un ammonimento ai titolari ingiungendo loro di provvedere alla cancellazione delle foto della minore attualmente pubblicate sui propri social network in assenza della base giuridica del consenso (provv. 10 luglio 2025, n. 394, doc. web n. 10181642).

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

Nel periodo di riferimento l'esame di reclami e segnalazioni riguardanti vicende di cronaca ha costituito occasione per un intervento dell'Autorità teso a ribadire i principi fondamentali della disciplina relativa alla protezione dei dati personali in ambito giornalistico. Tra questi, assume rilievo il principio 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, in particolare, il limite della essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137 del Codice). Tale parametro – espressione del principio generale di minimizzazione dei dati formalizzato dal RGPD (art. 5, par. 1, lett. c) – viene richiamato anche nelle regole deontologiche in materia (artt. 6, 8, 10 e 11) e costituisce un requisito fondamentale della professione giornalistica per un'informazione corretta e rispettosa dei diritti della persona.

In applicazione di tale principio l'Autorità ha accolto le richieste, formulate da una persona di una certa notorietà, di disporre il divieto di ulteriore trattamento di alcuni dati concernenti una rapina subìta mentre era in macchina nella propria zona di residenza e contenuti in alcuni articoli pubblicati da due quotidiani. Il reclamante aveva contestato la non essenzialità del proprio nome e cognome, evidenziando come la diffusione del dato identificativo, unitamente all'indicazione della tipologia del bene oggetto di furto e della zona in cui ciò era avvenuto, avrebbe ulteriormente esposto sé e la propria famiglia al rischio di reiterazione della condotta illecita. L'Autorità, nel condividere le eccezioni sollevate dal reclamante, ha convenuto che nel caso di specie era stato violato il principio di essenzialità dell'informazione – con riguardo al nominativo, ma non con riferimento al bene sottratto e alla zona in cui il fatto si era verificato – non

potendosi ravvisare un interesse pubblico specifico collegato alla conoscibilità dell'identità del medesimo ed ha pertanto disposto il divieto di ulteriore trattamento del dato nonché ammonito gli editori per le violazioni riscontrate (provv. 10 aprile 2025, n. 214, doc. web n. 10144227).

Il principio di essenzialità è stato rilevante anche nella valutazione di ulteriori reclami tramite i quali era stata contestata l'indebita pubblicazione di immagini di alcune persone. In un caso, in particolare, erano stati pubblicati i dati identificativi e le immagini di una persona deceduta in circostanze singolari, la ricostruzione delle quali era stata oggetto di un libro curato da un noto criminologo, consulente tecnico di parte nell'ambito del relativo procedimento penale. Le interessate, congiunte della persona defunta, avevano contestato tale utilizzo di dati ed informazioni, ivi comprese immagini del corpo senza vita del *de cuius*, tratte da atti e documenti di cui l'autore aveva avuto disponibilità in ragione dell'incarico di consulenza conferito nonché la violazione delle specifiche finalità a quest'ultimo sottese e il principio di essenzialità dell'informazione. L'Autorità ha ritenuto che, nel caso specifico, non vi fossero ragioni di interesse pubblico collegate alla conoscibilità dei dati identificativi delle interessate e del *de cuius*, tenuto conto che si era trattato di una vicenda risalente e priva (anche all'epoca dei fatti) di risonanza mediatica, e che pertanto il bilanciamento era da effettuarsi tra il diritto alla protezione dei dati personali ed il diritto alla rievocazione storiografica tenuto conto dei criteri enunciati dalle sezioni unite della Corte di cassazione (Cass. civ. sez. unite n. 19681/2019). L'Autorità ha confermato la ritenuta violazione ed ha vietato l'ulteriore trattamento dei dati contestati (provv. 23 ottobre 2025, n. 701, doc. web n. 10218967).

Medesimo principio è stato applicato in un caso concernente la pubblicazione di immagini relative a una vicenda di rilevanza pubblica che tuttavia aveva riguardato una persona diversa dalla reclamante, pur se a quest'ultima legata da un rapporto di tipo familiare che si è dunque trovata suo malgrado esposta all'attenzione mediatica attraverso la diffusione di contenuti afferenti la sua vita personale che non avevano alcun legame con la più ampia vicenda in riferimento alla quale la pubblicazione era avvenuta (provv. 23 ottobre 2025, n. 656, doc. web n. 10218807).

Una valutazione diversa è stata invece svolta in merito ad un trattamento effettuato da alcune testate giornalistiche riguardante la pubblicazione di immagini relative ad attività svolte nella vita quotidiana direttamente dalla persona con la quale la reclamante del provvedimento aveva rapporti di tipo familiare; in tal caso infatti, tenuto conto della rilevanza pubblica della vicenda, il Garante ha ritenuto la diffusione di informazioni relative alla reclamante, sia pure afferente a situazioni di vita personale, conforme alla normativa di settore e, in particolare, al principio di essenzialità dell'informazione (provv. 23 ottobre 2025, n. 620, doc. web n. 10219450).

In un altro caso, il reclamante – noto avvocato ed esponente politico – aveva lamentato la pubblicazione su una testata giornalistica online di diversi articoli relativi ad un'indagine in materia di corruzione a proprio carico nell'ambito della quale sarebbero stati divulgati anche video di incontri sessuali intrattenuti dallo stesso presso gli uffici comunali (estratti da intercettazioni ambientali). L'Autorità, nel prendere atto dell'avvenuta rimozione e della deindicizzazione degli articoli oggetto del reclamo, ha disposto la misura dell'ammonimento per l'inosservanza delle disposizioni in materia di protezione dei dati personali nell'esercizio dell'attività giornalistica, con particolare riguardo alle notizie che investono la sfera sessuale delle parti coinvolte (provv. 30 gennaio 2025, n. 43, doc. web n. 1011356).

La differente valutazione resa in casi similari, evidenzia che il giudizio di bilanciamento tra il diritto alla protezione dei dati personali ed il diritto di manifestazione del pensiero deve sempre essere effettuato in concreto.

9

Parimenti, nel febbraio 2025 il Garante ha adottato una serie di provvedimenti nei confronti di editori di testate giornalistiche che, nel riportare gli sviluppi delle indagini e del procedimento pendente a carico di alcuni giovani indagati – e poi imputati – per il reato di violenza sessuale nei confronti di una loro coetanea, avevano diffuso alcuni dati idonei a consentirne l'identificazione unitamente a una pluralità di informazioni – anche particolareggiate – attinenti alla sua vita personale nonché alla violenza denunciata. L'Autorità ha rilevato nelle condotte delle testate una violazione dei principi di liceità e minimizzazione del trattamento (art. 5, par. 1, lett. a) e c), RGPD), nonché una violazione del principio di essenzialità dell'informazione. L'Autorità ha ritenuto nella stessa sede di stigmatizzare la generale condotta dei media i quali, nell'occuparsi del caso, erano andati ben oltre l'esercizio del diritto e dovere di cronaca, mostrando un accanimento informativo su dettagli non essenziali e comunque lesivi della dignità della persona interessata, a prescindere dalla sua identificazione da parte della generalità della collettività ovvero dal più circoscritto ambito sociale di riferimento della stessa. In ragione della gravità della condotta ha ritenuto di comminare ai titolari destinatari dei provvedimenti anche una sanzione pecuniaria (provv.ti 27 febbraio 2025, da n. 119 a n. 126, doc. web nn., 10160373, 10162891, 10160396, 10160593, 10160732, 10160755, 10160782, 10160799; i provv.ti nn. 121, 124 e 126 sono stati oggetto di impugnazione).

La tutela dell'anonimato e della riservatezza delle persone che denunciano atti di violenza sessuale è altresì alla base di un provvedimento di divieto del trattamento adottato dal Garante nei confronti di un'emittente televisiva in relazione ad un servizio giornalistico che aveva reso visibili i nominativi di due donne che avevano denunciato violenze sessuali in un centro olistico (provv. 27 febbraio 2025, n. 127, doc. web n. 10138907, oggetto di impugnazione).

Nel giugno 2025, l'Autorità ha adottato un provvedimento relativo a un reclamo avente ad oggetto la richiesta di limitazione definitiva del trattamento di dati personali idonei a rendere identificabile l'interessata, riportati in alcuni articoli giornalistici relativi ad una violenza sessuale della quale la stessa era risultata vittima. In tale circostanza, l'Autorità ha dichiarato il reclamo infondato in quanto i contenuti editoriali lamentati risultavano essere stati narrati nel rispetto del principio dell'essenzialità dell'informazione. Invero, negli articoli in argomento non sono stati rinvenuti elementi idonei a consentire l'identificazione diretta della reclamante, in linea con il richiamo dell'Autorità ai mezzi di informazione di astenersi dal riportare dettagli che possano creare ulteriore danno alle vittime di violenza e abusi (cfr. "Violenza sessuale: il Garante privacy richiama i media al rispetto delle vittime" - 31 marzo 2009, doc. web n. 1602527) (provv. 23 giugno 2025, n. 366, doc. web n. 10161332).

Con riferimento a tre reclami aventi ad oggetto la diffusione di una quantità eccessiva e ultronea di dati personali degli interessati (tra cui, anche dati relativi allo stato di salute) all'interno di articoli pubblicati su un sito di informazione online, l'Autorità, all'esito di una lunga e articolata istruttoria, ha impartito al titolare una sanzione amministrativa pecuniaria e disposto il divieto di ulteriore trattamento, nonché la cancellazione di tali contenuti editoriali (provv. 4 agosto 2025, n. 458, doc. web n. 10166287).

Nel periodo di riferimento, l'Autorità è intervenuta in merito alla diffusione, nell'ambito di una serie televisiva distribuita su una piattaforma di streaming, di registrazioni audio relative a conversazioni telefoniche e messaggi vocali intercettati durante la fase delle indagini preliminari nell'ambito di un noto caso di cronaca giudiziaria risalente al 2010, concernente l'omicidio di una tredicenne, conclusosi con una condanna definitiva nell'ottobre 2018.

I genitori della vittima avevano lamentato la pubblicazione – nei primi episodi della serie – di numerosi file audio contenenti conversazioni telefoniche e messaggi vocali scambiati

nell'immediatezza della scomparsa della figlia, tra cui un messaggio lasciato dalla madre nella segreteria telefonica della giovane. Secondo i reclamanti, tali registrazioni, mai utilizzate nel corso del processo, erano state diffuse senza alcuna attinenza con le indagini e con finalità meramente sensazionalistiche, in violazione della loro sfera privata.

Nel caso di specie, l'Autorità ha ritenuto che la diffusione delle registrazioni – contenenti espressioni intime e particolarmente dolorose dei genitori della vittima nelle fasi più drammatiche della vicenda – non fosse giustificata da esigenze informative essenziali e integrasse una scelta editoriale di rilevante impatto sulla sfera privata degli interessati, idonea a rinnovare una forte sofferenza.

Il Garante ha pertanto dichiarato illecita la pubblicazione delle registrazioni, ritenendola in violazione dei principi di liceità, correttezza e minimizzazione del trattamento (art. 5 del RGPD) nonché in violazione delle disposizioni applicabili ai trattamenti effettuati per finalità giornalistiche e ha pertanto disposto il divieto di ulteriore diffusione degli audio, consentendone esclusivamente la conservazione per eventuali esigenze giudiziarie (provv. 13 novembre 2025, n. 695, doc. web n. 10199522; il provvedimento è stato oggetto di impugnazione).

Parimenti illecita, quale violazione dei principi suindicati, è stata ritenuta la pubblicazione – all'interno della medesima serie televisiva – della fotografia di un uomo (autore di un reclamo al Garante), sottoposto alle indagini quale persona dal cui DNA si era risaliti al supposto responsabile dell'omicidio della giovane. Il Garante ha ritenuto che la conoscenza e la rievocazione – a distanza di anni – delle "fattezze" di quest'uomo non fosse sostenuta da alcuna attualità di interesse e necessaria completezza informativa, alla luce del rilievo marginale e transitorio nell'ambito delle indagini della persona ritratta. È stato quindi disposto il divieto di trattamento delle fotografie ritraenti il reclamante (provv. 13 novembre 2025, n. 697, doc. web n. 10212597; il provvedimento è stato oggetto di impugnazione).

Sempre in relazione a fatti di cronaca di forte impatto mediatico, deve citarsi il provvedimento d'urgenza adottato dal Garante nel mese di luglio 2025 in relazione ad alcune immagini dell'autopsia della ventiseienne vittima di omicidio nel 2007 rese disponibili su un canale YouTube, nell'ambito di "masterclass" a pagamento. Il Garante ha al riguardo rilevato una grave lesione della dignità della vittima e una violazione dei diritti dei suoi familiari e ha vietato l'ulteriore trattamento delle immagini, nonché formulato un avvertimento a chiunque fosse entrato nella disponibilità delle immagini in ordine all'illiceità della loro eventuale ulteriore diffusione (provv. 11 luglio 2025, n. 411, doc. web n. 10149350).

Il Garante ha avuto anche modo di pronunciarsi sul rispetto del principio di essenzialità dell'informazione in relazione a forme di manifestazione del pensiero realizzate tramite social network. In tal senso, il Garante ha accolto un reclamo con cui era stata lamentata la pubblicazione di un post corredato da stralci di atti giudiziari e intercettazioni – afferenti a un procedimento penale che aveva coinvolto il titolare del trattamento e rispetto al quale quest'ultimo era stato poi prosciolto – contenenti frammenti di conversazioni del reclamante (estraneo al suddetto procedimento) nell'ambito delle quali erano state attribuite al titolare del trattamento circostanze rivelatesi infondate in sede processuale. In particolare, l'Autorità ha reputato la pubblicazione di stralci di intercettazioni eccedente e non essenziale rispetto alla dichiarata finalità del titolare di voler riqualificare la propria figura a seguito dell'ottenuto proscioglimento (provv. 29 aprile 2025, n. 253, doc. web n. 10146266).

In un'altra occasione, l'Autorità ha ritenuto che anche l'attività svolta da agenzie fotogiornalistiche possa, in taluni casi, rientrare nell'ambito dei trattamenti di dati personali effettuati per finalità giornalistiche e nell'esercizio della libera manifestazione

del pensiero. In particolare, il Garante ha esaminato un reclamo relativo alla raccolta e alla messa a disposizione, da parte di un'agenzia fotogiornalistica, di immagini raffiguranti un personaggio pubblico ripreso nel corso di convegni ed eventi pubblici nell'ambito dei quali era intervenuto in qualità di relatore. L'Autorità ha ritenuto che il trattamento di tali immagini, realizzate in occasione di eventi aperti ai media e destinate alla pubblicazione a corredo di articoli, fosse riconducibile alla disciplina di cui agli artt. 85 del RGPD e 136 ss. del Codice, se funzionale alla diffusione al pubblico di informazioni e alla documentazione di fatti di interesse per la collettività (provv. 27 marzo 2025, n. 179, doc. web n. 10148557).

9.2.4. Giornalismo d'inchiesta e modalità di acquisizione delle informazioni

L'Autorità ha avuto modo di interrogarsi sui presupposti in presenza dei quali possa ritenersi lecita una raccolta di dati effettuata avvalendosi della deroga di cui all'art. 2, comma 1, delle regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica – che esonera il giornalista dall'obbligo di rendere nota la propria identità e professione, laddove ciò possa pregiudicare l'esercizio della funzione informativa – con particolare riguardo al trattamento di dati effettuato nell'ambito del cd. giornalismo di inchiesta che gode, quale *species* più rilevante della attività di informazione, di ampia tutela sia nell'ordinamento interno che internazionale.

In tale contesto l'Autorità ha, in particolare, valutato le modalità di acquisizione dei dati personali confluiti in un servizio di inchiesta riferito a comportamenti ritenuti censurabili posti in essere da giovani appartenenti a un movimento politico giovanile ed emersi in vari contesti, tra i quali un evento svoltosi all'interno di un casale. Nel caso di specie il Garante – considerata l'avvenuta anonimizzazione dei dati dei partecipanti, ad esclusione di quelli delle persone che rivestivano una posizione apicale nel movimento – ha ritenuto che la raccolta fosse avvenuta lecitamente in quanto la giornalista responsabile dell'inchiesta non aveva utilizzato artifici o raggiri per introdursi nella struttura ma era intervenuta su invito e nella sua qualità professionale, limitandosi a modificare in modo minimale il proprio nominativo ed omettendo le finalità della raccolta delle informazioni allo scopo di potere svolgere la propria attività.

L'Autorità ha inoltre escluso, nel caso di specie, la configurazione di una violazione di domicilio – pure prospettata dagli interessati – ritenendo che il luogo in questione, per le sue caratteristiche, non poteva ritenersi assimilabile ad un domicilio privato, trattandosi di una struttura ricettiva data in uso agli organizzatori dell'evento al quale aveva partecipato un consistente numero di persone (provv. 25 settembre 2025, n. 567, doc. web n. 10188249; il provvedimento oggetto di impugnazione).

Sono state altresì ritenute lecite la raccolta e la diffusione – nell'ambito di una nota trasmissione televisiva – dei dati e del volto di un notaio, raggiunto nel proprio studio dagli operatori tecnici i quali, rendendo palese la propria identità e la presenza di una telecamera, avevano chiesto informazioni in merito a un atto di compravendita rogato dallo stesso pubblico ufficiale; ciò era avvenuto nel contesto di una vicenda, più volte trattata dalla medesima trasmissione, relativa agli effetti pregiudizievoli subìti da alcune persone per effetto dell'usucapione di cui anche il notaio (reclamante) aveva validato l'operatività. L'Autorità ha ritenuto che l'identificazione del notaio non si ponesse in contrasto con il principio di essenzialità dell'informazione alla luce del fatto che egli era stato notaio rogante di analogo atto di compravendita coinvolgente lo stesso beneficiario (e persone della sua cerchia parentale) e aveva potuto ampiamente giustificare, nell'ambito del servizio oggetto di reclamo, la correttezza del proprio operato e la validità giuridica dell'atto (provv. 4 giugno 2025, n. 334, doc. web n. 10163554).

9.2.5. Essenzialità dell'informazione e personaggi noti

Con riferimento alla pubblicazione di contenuti afferenti a personaggi noti, l'Autorità ha in più occasioni chiarito che coloro che sono, per qualsiasi motivo, noti al pubblico, godono di un'aspettativa di riservatezza più limitata, sussistendo per questi ultimi più ampi margini nella diffusione di informazioni che possono riguardare, entro certi limiti, anche notizie attinenti alla vita privata. In merito, si deve precisare che "persona nota" non è solo il soggetto che ricopre un pubblico incarico, ma anche colui che, a vario titolo, per l'attività svolta o per specifiche circostanze della vita, si trova esposto al pubblico e alla valutazione collettiva, rientrando certamente in tale categoria anche i personaggi dello spettacolo.

In tale contesto, il compito dell'Autorità è quello di valutare quando l'interesse pubblico alla conoscenza di determinate notizie possa sacrificare la pretesa all'oblio del personaggio noto che si ritenga leso nella sua riservatezza.

In tale quadro l'Autorità, nell'esaminare un reclamo, ha ritenuto che la notorietà di una persona e della sua relazione con un noto esponente politico non potevano considerarsi condizioni sufficienti a legittimare qualsiasi forma di raccolta e di utilizzo di dati e immagini, dovendosi invece caso per caso valutare la sussistenza dei presupposti idonei a legittimare il trattamento. Nel caso di specie l'Autorità ha ritenuto illecita la diffusione di immagini ritraenti alcune nudità della reclamante mentre si trovava sulla propria barca, al largo, corredate da allusioni ad uno "spogliarello" per il compagno distratto, a nulla valendo la circostanza di essere un servizio inserito all'interno di un prodotto giornalistico "leggero" destinato a lettori «che, specie d'estate, gradiscono storie che si occupino delle relazioni sentimentali del loro beniamini» (provv. 25 settembre 2025, n. 572, doc. web n. 10231924).

Analogo bilanciamento è stato svolto dall'Autorità con riferimento al reclamo proposto da un noto attore italiano concernente la divulgazione in rete di un file audio estratto da una conversazione privata e originariamente pubblicato, in assenza di consenso, sul canale YouTube riconducibile ad un altro noto personaggio televisivo, titolare del trattamento, e poi ulteriormente ripreso su varie piattaforme social. L'Autorità – tenuto conto della viralità raggiunta dall'audio lamentato, della facilità di condivisione nei social network, nonché del parametro di essenzialità dell'informazione, applicabile a informazioni che riguardano persone note ove le notizie o i dati non rivestano alcun rilievo in rapporto al loro ruolo o alla loro vita pubblica – ha rivolto un avvertimento a tutti gli utenti della rete, evidenziando che l'eventuale ulteriore diffusione dell'audio avrebbe potuto configurare una violazione delle disposizioni del RGPD e del Codice (artt. 137 del Codice e 6 delle regole deontologiche) (provv. 4 agosto 2025, n. 467, doc. web n. 10155769).

L'Autorità ha successivamente accertato l'inottemperanza da parte del titolare a quanto prescritto attraverso il suddetto provvedimento, non avendo lo stesso adottato alcuna misura diretta a mitigare gli effetti della diffusione dell'audio riguardante il reclamante. Pertanto, l'Autorità, riservandosi ogni altra determinazione all'esito della definizione dell'istruttoria già avviata, ha disposto, in via d'urgenza, la limitazione provvisoria del trattamento, da ritenersi riferita all'ulteriore diffusione online del file audio o dei contenuti estratti dalla conversazione privata intercorsa tra l'interessato e un soggetto terzo ed ha altresì rivolto un avvertimento sulla possibile irrogazione di una sanzione amministrativa pecuniaria, in caso di reiterata inottemperanza (provv. 20 agosto 2025, n. 479, doc. web n. 10159435).

Analogamente, in data 16 agosto 2025, l'Autorità ha adottato un provvedimento d'urgenza avente ad oggetto la lamentata divulgazione in rete di filmati – ritraenti un noto presentatore italiano e la propria compagna in momenti di intimità – estratti ille-

citamente dal sistema di videosorveglianza installato presso l'abitazione degli stessi. L'Autorità ha al riguardo imposto a tutti gli utenti della rete la limitazione definitiva del trattamento e, dunque, del filmato e/o delle immagini lamentate, disponendo, altresì, l'avvertimento che l'eventuale ulteriore diffusione avrebbe potuto configurare una violazione della normativa di settore e comportare l'adozione dei conseguenti provvedimenti, anche di carattere sanzionatorio (provv. 16 agosto 2025, n. 477, doc. web n. 10158795).

9.3. *Trattamento dei dati personali da parte dei motori di ricerca*

I reclami proposti nei confronti dei gestori di motori di ricerca hanno costituito, nel periodo di riferimento, una parte rilevante delle doglianze complessivamente pervenute all'Autorità con riferimento al settore della libertà di informazione.

La maggior parte delle richieste di deindicizzazione pervenute ha riguardato trattamenti posti in essere tramite il motore di ricerca gestito da Google LLC, cui ha fatto seguito l'attivazione di altrettanti procedimenti. Al riguardo, occorre rilevare che, in taluni casi, le predette richieste sono state soddisfatte a seguito di un'adesione spontanea del titolare del trattamento dopo l'intervento dell'Autorità, mentre nei restanti casi è stato necessario un provvedimento collegiale.

La maggior parte delle richieste di rimozione, anche inerenti a istanze di *delisting* globale, concernevano articoli di stampa recanti informazioni attinenti a vicende giudiziarie, più o meno recenti, riguardo alle quali gli interessati avevano invocato l'esercizio del diritto all'oblio in ragione del tempo decorso dall'accadimento dei fatti, della tenuità dei reati commessi, del ruolo professionale rivestito dagli interessati e della narrazione aggiornata all'attuale realtà processuale. Non sono mancate anche ipotesi nelle quali l'esercizio del diritto all'oblio è stato invocato in ragione della non veridicità, sostenuta e opportunamente documentata dal reclamante, dei fatti e delle circostanze riportate all'interno di pagine web (provv. 4 giugno 2025, n. 337, doc. web n. 10152780).

In un certo numero di casi, l'Autorità ha tuttavia ritenuto che le argomentazioni addotte dagli interessati a fondamento delle loro richieste non fossero tali da determinare un accoglimento dell'istanza di deindicizzazione (provv.ti 13 febbraio 2025, n. 72, doc. web 10119733; 13 marzo 2025, n. 161, doc. web n. 10132518; 4 giugno 2025, n. 333, doc. web n. 10149987; 9 ottobre 2025, n. 599, doc. web n. 10191470; 9 ottobre 2025, n. 600, doc. web n. 10192843; 13 novembre 2025, n. 672, doc. web n. 10200607; 4 dicembre 2025, n. 740, doc. web n. 10212707). Ciò è quanto si è verificato, ad esempio, anche in un caso in cui era stata chiesta la deindicizzazione di articoli relativi ad una vicenda giudiziaria che aveva coinvolto il reclamante come imputato "per ipotesi di reato contro il patrimonio nonché sottoposto a misura cautelare", poi revocata. L'Autorità ha ritenuto che il mancato aggiornamento della notizia in ordine alla revoca della misura cautelare non giustificasse l'invocata deindicizzazione, posto che un giudizio cautelare, per definizione, è volto ad evitare il rischio che determinate circostanze vanifichino le esigenze procedimentali, qualificandosi come strettamente servente rispetto al più ampio procedimento penale da cui promana (provv. 13 novembre 2025, n. 696, doc. web n. 10213539).

In un altro caso, il Garante non ha ritenuto fondata la richiesta di deindicizzazione motivata dal mancato aggiornamento di alcuni recenti articoli di stampa che – nel riportare una vicenda giudiziaria relativa alla condanna di un medico di base per aver raggirato diversi pazienti – non avevano dato conto della diminuzione di pena comminata alla reclamante in sede di appello. L'Autorità ha infatti ritenuto di non poter accogliere

la richiesta tenuto conto della natura e della gravità della condotta, dell'esiguo tempo trascorso dai fatti e dalla pubblicazione degli articoli, della colpevolezza della reclamante confermata anche in appello, della non ancora intervenuta estinzione del reato e, inoltre, della professione medica che l'interessata continuava a svolgere (provv. 10 luglio 2025, n. 395, doc. web n. 10171733).

Sempre in tema di reperibilità in rete di articoli di cronaca giudiziaria, il Garante ha ricordato che l'espiazione della pena non determina un'automatica prevalenza del diritto all'oblio, costituendo piuttosto uno dei possibili fattori di cui tenere conto ai fini dell'accoglimento di un'istanza di deindicizzazione. Tale valutazione è stata seguita dall'Autorità nel ritenere infondato un reclamo diretto a escludere la reperibilità in rete di alcuni articoli riguardanti un grave episodio di corruzione che aveva coinvolto l'interessata. Nonostante quest'ultima avesse espiato la propria pena in tempi assai recenti a seguito di patteggiamento, l'Autorità ha infatti ritenuto essere ancora sussistente l'interesse pubblico alla conoscenza delle informazioni riportate negli articoli, tenuto conto del mancato riconoscimento del beneficio della non menzione e dell'entità del sistema corruttivo portato alla luce dall'inchiesta giudiziaria, nonché del ruolo di primo piano rivestito dalla reclamante in tale sistema (provv. 23 ottobre 2025, n. 619, doc. web n. 10197507).

Non sono mancati casi in cui l'Autorità, in considerazione del differente contenuto degli articoli oggetto di reclamo, ha ritenuto parzialmente accoglibili le istanze di deindicizzazione. È quanto si è verificato, ad esempio, con riguardo a un reclamo, presentato dall'interessato in proprio e in qualità di erede del nonno defunto, rispetto ad articoli relativi a vicende giudiziarie che avevano coinvolto, rispettivamente, il *de cuius* per i suoi collegamenti con organizzazioni della criminalità organizzata e il reclamante in relazione alla confisca-sequestro di beni ritenuti proventi di tali legami. In particolare, l'Autorità non ha accolto la richiesta di deindicizzazione avanzata dal reclamante rispetto a taluni articoli contenenti informazioni recenti sull'attività professionale svolta dallo stesso; viceversa, ha ritenuto prevalente, rispetto ai restanti articoli, il diritto alla riservatezza del singolo, posto che dalla vicenda giudiziaria non era emersa alcuna attribuzione di responsabilità in capo al reclamante e che la posizione di quest'ultimo si era definita da tempo con la revoca del sequestro dei beni aziendali di sua titolarità. L'Autorità, inoltre, con riguardo alle istanze avanzate per conto del *de cuius*, ha ritenuto il reclamo fondato limitatamente agli articoli contenenti notizie aggiornate sull'evoluzione della vicenda giudiziaria che aveva coinvolto il *de cuius* (provv. 18 dicembre 2025, n. 765, doc. web n. 10213507).

Il Garante ha ritenuto parzialmente infondata la richiesta di deindicizzazione di pagine rinvianti ad articoli attinenti ad una vicenda giudiziaria relativamente recente (2020) conclusasi con un patteggiamento, in ragione della perdurante attualità dell'interesse alla reperibilità degli articoli – comunque aggiornati – alla luce della natura economica dei reati contestati al reclamante, connessi alla sua attività imprenditoriale, nonché del ruolo rivestito dal medesimo (provv. 29 aprile 2025, n. 252, doc. web n. 10145853).

In altra occasione, l'Autorità ha ritenuto di estendere la tutela dell'interessato ai risultati della ricerca rinvenibili dall'associazione del nominativo con ulteriori termini qualificativi della persona e della relativa attività professionale, ricordando che, in base alla nota sentenza Costeja della CGUE, interpretata alla luce della definizione di "dato personale" di cui all'art. 4 del RGPD, il ruolo professionale, annoverandosi tra gli "elementi caratteristici dell'identità culturale e sociale" dell'individuo, presenta una stretta attinenza alla dimensione personale dell'interessato (provv. 13 febbraio 2025, n. 71, doc. web n. 10119716).

9

9.4. *Gestione di istanze di esercizio dei diritti degli interessati nei trattamenti di dati per finalità giornalistiche*

Nell'ambito delle istanze di esercizio dei diritti degli interessati rivolte a titolari di testate giornalistiche l'Autorità, pur ritenendo talvolta infondate le richieste di deindicizzazione avanzate, reputando persistente l'interesse pubblico a conoscere le notizie pubblicate (provv. 4 giugno 2025, n. 335, doc. web n. 10149947), ha comunque sottolineato la necessità che i titolari forniscano riscontro alle istanze preventive presentate dagli interessati (provv. 4 giugno 2025, n. 336, doc. web n. 10149964). L'Autorità ha inoltre evidenziato l'importanza di soddisfare tali richieste in ragione della delicata natura dei dati coinvolti, relativi nella maggior parte dei casi a notizie afferenti a vicende giudiziarie spesso non aggiornate, la cui persistente reperibilità in rete appare idonea a determinare un concreto pregiudizio per i protagonisti dei fatti narrati.

Muovendo da tale assunto, con riferimento ad un reclamo, l'Autorità, nel prendere atto dell'adesione del titolare del trattamento alla richiesta di deindicizzazione del reclamante, ha inflitto una sanzione amministrativa pecuniaria per il mancato riscontro alla richiesta di informazioni del Garante e all'istanza di esercizio dei diritti dell'interessato nel previsto termine di trenta giorni dalla ricezione della stessa, nonché in ragione dell'assenza di una privacy policy nel sito Internet del titolare. È stato inoltre ingiunto al titolare di adottare misure tecniche e organizzative adeguate a facilitare l'esercizio dei diritti previsti dalla normativa in materia di protezione dei dati personali e di soddisfare, senza ingiustificato ritardo, le relative istanze (provv.ti 10 aprile 2025, n. 213, doc. web n. 10145256; 23 ottobre 2025, n. 638, doc. web n. 10199198).

10 Cyberbullismo e *revenge porn*

Cyberbullismo

Nel corso del 2025, l'Autorità ha proseguito il proprio impegno nell'attività di prevenzione, sensibilizzazione e contrasto alle condotte di cyberbullismo. Ciò è avvenuto sia attraverso la partecipazione ai lavori del tavolo interistituzionale per la prevenzione e il contrasto al bullismo e al cyberbullismo, costituito dal Dipartimento per le politiche della famiglia della Presidenza del Consiglio dei ministri, in conformità a quanto disposto dalla l. n. 71/2017 (i cui lavori sono ancora *in itinere*), sia attraverso la trattazione delle segnalazioni dei casi. Queste ultime – presentate dai minori o dagli esercenti la potestà genitoriale – hanno riguardato, in via principale, la pubblicazione di post denigratori e diffamatori, nonché la creazione di falsi profili all'interno di social network o ancora la richiesta di rimozione di account hackerati, i cui contenuti sono stati utilizzati da terzi a scopo denigratorio. In taluni casi i segnalanti hanno 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, sono state fornite anche indicazioni riguardo alla specifica procedura prevista.

L'intervento che la l. n. 71/2017 affida all'Autorità in tale ambito è volto, infatti, a ottenere "l'oscuramento, la rimozione o il blocco" di un contenuto lesivo ai danni di un minore "diffuso nella rete Internet" (art. 2). Le istanze di tal genere sono state trattate mediante l'invio di apposite richieste di intervento al gestore della piattaforma di volta in volta coinvolto. Tuttavia, le segnalazioni hanno denunciato spesso condotte consumate non in rete, ma attraverso l'uso di chat private, in un contesto "amicale" o di classe nelle quali hanno altresì espresso il disagio vissuto e una richiesta di aiuto. In tali casi l'Autorità ha fornito un riscontro al segnalante (e mantenuto un contatto con quest'ultimo) indicando gli strumenti e le figure utili all'individuazione della misura di tutela più idonea al caso.

Revenge porn

Nel corso dell'anno è inoltre proseguita l'attività finalizzata a contrastare il fenomeno della diffusione non consensuale di materiale a contenuto sessualmente esplicito, tramite l'attivazione della tutela di tipo preventivo prevista ai sensi dell'art. 144-*bis* del Codice.

Il numero di segnalazioni in materia di *revenge porn* è risultato considerevole anche nel 2025, raggiungendo il numero di 854, trasmesse al Garante attraverso l'apposita procedura online resa disponibile sul sito istituzionale dell'Autorità.

La principale tipologia di istanze pervenute all'Autorità è stata quella attraverso cui i segnalanti hanno manifestato il timore della diffusione di proprio materiale intimo, dopo avere ricevuto minacce in tal senso da parte di terzi non identificabili, in caso di mancato pagamento di una somma di denaro o di rifiuto di invio di ulteriore materiale (cd. *sextortion*). Più circoscritti sono risultati, invece, i casi di temuta diffusione di materiale intimo per finalità vendicative, al termine di una relazione sentimentale intrattenuta dal segnalante (cd. *revenge porn*).

Laddove le segnalazioni sono risultate carenti degli elementi indispensabili ai fini della relativa trattazione, l'Autorità ha chiesto agli interessati di fornire le integrazioni

10

necessarie, domandando altresì, in taluni casi, di trasmettere il materiale a contenuto sessualmente esplicito la cui acquisizione è prevista dall'art. 144-*bis* del Codice. Non sono mancati i casi in cui il materiale inviato dai segnalanti è risultato privo di contenuti sessualmente espliciti o non è risultato idoneo (come nel caso di screenshot di videochiamate o di chat), in quanto non corrispondente all'immagine originale in possesso della persona malintenzionata e di cui era lamentata la temuta diffusione.

La trattazione delle segnalazioni perfezionate ha portato all'adozione in via d'urgenza di un consistente numero di determinazioni dirigenziali (nel complesso 523), successivamente ratificate dal Collegio e dirette ai gestori delle piattaforme coinvolte per ottenere l'intervento di blocco preventivo del materiale a contenuto sessualmente esplicito oggetto della temuta attività di diffusione.

Il Garante ha inoltre proseguito le interlocuzioni con la Procura della Repubblica di Roma, anche attraverso la comunicazione, in taluni casi, delle possibili notizie di reato che risulterebbero emergere dalla trattazione dalle segnalazioni pervenute all'Autorità ai sensi dell'art. 144-*bis* del Codice.

11 Marketing e trattamento di dati personali

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

Nel corso del 2025, in continuità con gli anni precedenti, l'Autorità ha svolto un'attività di contrasto al fenomeno del telemarketing non richiesto, mediante un'ampia e sistematica azione di verifica e controllo nei confronti di operatori attivi in diversi settori merceologici, distribuiti sull'intero territorio nazionale e coinvolti, a vario titolo, nelle diverse fasi della filiera del trattamento che, a partire dal contatto, conduce alla conclusione del contratto.

Si conferma nel periodo di riferimento il costante incremento del numero di reclami e segnalazioni relativi alla ricezione di comunicazioni indesiderate, veicolate tramite chiamate telefoniche, SMS ed e-mail nonché quelli concernenti lo svolgimento di attività promozionali mediante il ricorso ad Internet e ai social.

L'azione di contrasto intrapresa si è sviluppata principalmente lungo tre direttrici fondamentali. In primo luogo, l'Autorità ha promosso una concreta attività di cooperazione con le altre autorità di regolazione (in particolare AGCOM), nonché con i diversi soggetti coinvolti, a vario titolo, nelle iniziative di contrasto al telemarketing indesiderato, quali le associazioni di consumatori e l'Organismo di monitoraggio del codice di condotta per le attività di telemarketing e *teleselling* promosso da associazioni di committenti, call center, *teleseller*, *list provider* e associazioni di consumatori (adottato con provv. 9 marzo 2023, n. 70, doc. web n. 9868813 - cfr. Relazione 2023, p. 123; cfr. anche Relazione 2024, p. 120 per una sintetica descrizione delle prescrizioni contenute nel codice di condotta).

Nell'ambito della seconda linea direttrice, l'Autorità ha assicurato un impegno continuo e quotidiano volto a fornire, già al termine della fase istruttoria preliminare, riscontri, chiarimenti e indicazioni operative alle migliaia di segnalazioni e lamentele presentate dagli interessati.

Con riferimento al terzo ordine di obiettivi, partendo dall'esame delle segnalazioni e dei reclami, sono state svolte approfondite attività istruttorie, anche mediante iniziative ispettive, che hanno condotto all'adozione di numerosi provvedimenti correttivi e sanzionatori, spesso caratterizzati da una rilevanza interpretativa di carattere generale.

In tale ambito continua a riscontrarsi il diffuso ricorso a numerazioni VoIP fittizie, utilizzate per mascherare l'effettiva linea telefonica chiamante (cd. *spoofing*), nonché l'effettuazione di contatti da parte di operatori non iscritti nel registro degli operatori della comunicazione e postali (ROC).

Complessivamente, nella quasi totalità delle istruttorie, l'attività condotta ha evidenziato, come per gli anni precedenti, la carente assimilazione degli obblighi gravanti sul titolare del trattamento in applicazione del principio di *accountability*, l'assenza di un adeguato controllo lungo l'intera filiera del trattamento, la mancata predisposizione di idonee

misure tecniche e organizzative, nonché l'utilizzo di liste di contatto acquisite da soggetti terzi in mancanza dei presupposti richiesti dalla normativa vigente con particolare riferimento alla correttezza dell'informativa resa agli interessati e alla validità dei consensi da questi prestati.

11.1.1. Il telemarketing illegale nel settore delle agenzie immobiliari

Il Garante ha intensificato la propria attività di vigilanza nel settore delle agenzie immobiliari, concentrandosi in particolare sulle pratiche di telemarketing e sull'invio di comunicazioni promozionali indesiderate. A seguito di numerose segnalazioni e reclami pervenuti già nel 2024 e degli accertamenti condotti anche mediante ispezioni presso le sedi dei titolari coinvolti, il Garante ha verificato le modalità di trattamento dei dati, rilevando, con frequenza significativa, il mancato svolgimento, da parte dei titolari, di verifiche adeguate in merito alla liceità delle liste di contatti acquisite da terzi. Analogamente, sono state riscontrate criticità relativamente alla completezza delle informazioni fornite agli interessati e alla validità dei consensi raccolti per la comunicazione dei dati a ulteriori titolari del trattamento. Tali riscontri hanno evidenziato una diffusa necessità di rafforzamento delle procedure interne di controllo e di verifica della conformità ai principi di trasparenza, liceità e responsabilizzazione previsti dalla normativa in materia di protezione dei dati personali.

Le istruttorie hanno altresì mostrato carenze organizzative significative, con riferimento sia al controllo sull'intera filiera del trattamento e sui soggetti nella stessa coinvolti, sia all'adozione di misure tecniche e organizzative idonee a garantire la sicurezza dei dati e il corretto esercizio dei diritti da parte degli interessati. In diversi casi, le società coinvolte hanno intrapreso iniziative correttive solo a seguito dell'intervento dell'Autorità, le quali, pur valutate positivamente sotto il profilo dell'indirizzo complessivo, non sono state ritenute sufficienti a sanare le violazioni già consumate.

In particolare, l'Autorità, a conclusione di un'articolata istruttoria, ha adottato un provvedimento che ha dichiarato l'illiceità dei trattamenti svolti da una società operante nella commercializzazione di dati per finalità di marketing, disposto il divieto di ulteriori trattamenti in assenza di idonea base giuridica, adottato misure correttive nonché irrogato una sanzione amministrativa pecuniaria pari a euro 100.000. Il Garante ha in particolare riscontrato la sussistenza di diffuse criticità soprattutto con riferimento alla liceità dei trattamenti, alla corretta individuazione dei ruoli soggettivi e all'effettiva osservanza del principio di responsabilizzazione di cui all'art. 5, par. 2, RGPD. È anche emerso l'utilizzo sistematico di liste di contatto acquisite da soggetti terzi in assenza di adeguate verifiche in ordine alla provenienza dei dati, alla completezza delle informative rese agli interessati e alla validità dei consensi raccolti per la comunicazione dei dati a ulteriori titolari per finalità promozionali. L'attività istruttoria ha inoltre evidenziato l'insufficienza delle misure tecniche e organizzative adottate dalla società, con specifico riguardo ai presidi di sicurezza, alla gestione degli accessi ai sistemi informativi e al controllo sulle operazioni di trattamento effettuate dai soggetti coinvolti nella filiera, nonché rilevanti carenze nella gestione delle istanze di esercizio dei diritti da parte degli interessati (provv. 16 gennaio 2025, n. 11, doc. web n. 10110241).

Criticità similari sono emerse in relazione a due procedimenti riguardanti ulteriori società operanti nel medesimo settore, all'esito dei quali, unitamente ai profili già sopra menzionati, è emerso un quadro di insufficiente controllo sull'intera filiera tale da indurre l'Autorità a dichiarare l'illiceità dei trattamenti in esame, l'ingiunzione del divieto di trattare i dati raccolti e la cancellazione degli stessi, l'imposizione di talune prescrizioni correttive e sanzioni amministrative pecuniarie, nonché la disposizione della pubblicazione dei provvedimenti stessi, anche in funzione dissuasiva e di

orientamento interpretativo per l'intero settore (provv.ti 13 marzo 2025, n. 138, doc. web n. 10120366 e n. 157, doc. web n. 10120517).

In un altro caso, il Garante ha affermato che l'affidamento su mere assicurazioni contrattuali del *list provider*, senza autonome e documentate verifiche sulla liceità dei dati, costituisce violazione degli obblighi del titolare, con conseguente mancata acquisizione di un consenso valido. In particolare, è emersa l'assenza di riscontri da parte di un titolare circa la preventiva acquisizione di un consenso valido e informato, la mancata consultazione del RPO e l'inadeguata gestione delle istanze di esercizio dei diritti degli interessati, subordinate a un non tempestivo confronto con il fornitore dei dati. Il quadro istruttorio ha altresì restituito una carente organizzazione complessiva dei trattamenti, sotto il profilo dell'*accountability* e del controllo dell'intera filiera, con ricadute sia sul rispetto dei principi di liceità e trasparenza, sia sull'adozione di misure tecniche e organizzative idonee a prevenire trattamenti illeciti (provv. 10 aprile 2025, n. 210, doc. web n. 10135041).

In relazione ad uno specifico procedimento, è stato ribadito che l'obbligo di cooperazione con l'Autorità di cui all'art. 157 del Codice costituisce un dovere autonomo e inderogabile del titolare, che permane anche in presenza di dichiarazioni di estraneità rispetto ai fatti contestati e non può ritenersi assolto mediante iniziative informali o il mero coinvolgimento di soggetti terzi (provv. 10 aprile 2025, n. 211, doc. web n. 10134986).

Il Garante ha inoltre continuato ad occuparsi dei trattamenti di dati personali effettuati da agenzie immobiliari attraverso telefonate indesiderate o invio di messaggi WhatsApp promozionali. Accertato in sede istruttoria che alcuni titolari del trattamento non avevano verificato né documentato la liceità delle liste utilizzate, né fornito agli interessati un'informativa completa e trasparente funzionale anche all'esercizio dei diritti di opposizione previsti dal RGPD, il Garante ha imposto l'adozione di misure organizzative e tecniche, il divieto di ulteriori trattamenti illeciti, la cancellazione dei dati raccolti illecitamente, l'adozione di misure organizzative e tecniche per assicurare l'esercizio dei diritti degli interessati e l'irrogazione di sanzioni amministrative pecuniarie proporzionate alla gravità delle condotte e al numero di soggetti coinvolti (provv.ti 10 aprile 2025, n. 212, doc. web n. 10134918; 29 aprile 2025, n. 247, doc. web n. 10134847; 29 aprile 2025, n. 278, doc. web n. 10134791).

Da ultimo, l'Autorità ha confermato il proprio orientamento in merito al ruolo di titolare del trattamento dei dati personali ricoperto dai cd. *list provider* nell'ambito di trattamenti in cui gli stessi abbiano determinato, di fatto, le finalità e i mezzi, cioè le modalità, dello stesso trattamento, e ciò indipendentemente da eventuali diverse previsioni inserite nelle privacy policy e nelle condizioni di servizio. In tale contesto, l'Autorità ha continuato ad occuparsi delle diverse doglianze ricevute, nel periodo compreso tra maggio 2022 e aprile 2024, concernenti l'avvenuta ricezione di telefonate indesiderate da parte di diverse agenzie immobiliari che avevano riferito di aver acquisito i dati da una società terza, già sanzionata nell'ambito di un autonomo procedimento (cfr. provv. 16 gennaio 2025, n. 11, doc. web n. 10110241, cit.). Partendo da tali accertamenti, è stato possibile risalire ad una delle origini delle liste e definire il procedimento avviato nei confronti della società destinataria del provvedimento in esame in relazione ai trattamenti di dati personali posti in essere attraverso il proprio sito Internet. L'Autorità ha accertato la responsabilità della società in ordine alla violazione degli artt. 5, par. 1, lett. a) e 24 del RGPD per avere effettuato trattamenti di dati personali con finalità promozionali senza la previa corretta individuazione del ruolo soggettivo ricoperto e di conseguenza in violazione dei doveri che derivano da tale ruolo, degli artt. 5, par. 1, lett. d) e par. 2, 6, par. 1, lett. a), 7, 13 e 14 del RGPD per aver effettuato trattamenti di dati inesatti e non aggiornati, degli artt. 5, par. 2, 12, parr. 1 e 2, 21, par.

2, 24 e 25 del RGPD per l'omesso riscontro alle istanze di esercizio dei diritti presentate dagli interessati, degli artt. 5, par. 1, lett. a), 6, par. 1, lett. a), 7 e 13 del RGPD per l'omessa trasparenza sui trattamenti effettuati per il tramite del proprio sito Internet nonché per l'errata individuazione della base giuridica dei trattamenti realizzati con la compilazione dei form online, degli artt. 5, par. 1, lett. b) e f), 25 e 32 del RGPD per la predisposizione di misure non idonee a garantire un accesso limitato ai dati, anche attraverso l'adozione di procedure di segregazione. Accertata l'illiceità delle condotte della società, l'Autorità ha irrogato una sanzione amministrativa pecuniaria pari a euro 5.000 e imposto alla società il divieto di ogni ulteriore trattamento dei dati in assenza di un consenso libero, specifico e informato, nonché il divieto di trattamento dei dati personali raccolti anche mediante i siti Internet della società senza la necessaria acquisizione di un preventivo idoneo consenso degli interessati in relazione a ciascuna delle attività effettuate dalla società, nonché anche la cancellazione di tali dati (provv. 9 ottobre 2025, n. 593, doc. web n. 10193723).

11.1.2. Il telemarketing illegale nel settore energetico

Anche nel 2025 l'Autorità ha proseguito l'attività istruttoria e sanzionatoria finalizzata al contrasto del cd. telemarketing selvaggio nel campo dei servizi energetici.

L'attività complessivamente posta in essere nell'ambito di tale settore ha consentito di accertare che, accanto alle metodologie tradizionali caratterizzanti il telemarketing selvaggio, si sta assistendo anche alla sempre maggiore preponderanza di tecniche basate sul cd. *digital advertising* inteso in senso ampio.

Più in particolare, sotto il primo profilo, continuano a verificarsi con sempre maggiore frequenza acquisizioni illecite di liste sovente non aggiornate, utilizzate per effettuare contatti promozionali nell'ambito dei quali gli operatori, già a conoscenza dei dati anagrafici e di fornitura, paventando problemi tecnici o bonus di fantasia, cercano di indurre l'utente alla sottoscrizione di un nuovo contratto. Nei casi più gravi, le medesime informazioni vengono utilizzate per l'attivazione non richiesta di servizi di fornitura, dei quali l'utente si avvede solamente al momento della ricezione di sproporzionate richieste di pagamento da parte dell'operatore.

Accanto a tali insidiose tecniche di ingaggio, nel 2025 si è altresì assistito con una certa frequenza anche ad attività di telemarketing e *teleselling* realizzate sulla base di anagrafiche acquisite mediante form presenti su siti web di comparazione o portali riguardanti concorsi a premi e social network riconducibili a società aventi sede all'estero o a siti web non navigabili, che utilizzano informative generiche e poco trasparenti non idonee a verificare l'identità del soggetto che conferisce i dati e l'esattezza delle informazioni acquisite. In mancanza di adeguate misure, tali portali possono essere sfruttati al fine di conferire una parvenza di liceità ad anagrafiche acquisite *aliunde* ed illecitamente, nonché allo scopo di precostituire un presunto consenso conferito successivamente all'avvenuta iscrizione al RPO.

Dinanzi a tali complessi fenomeni, è apparso indispensabile indirizzare l'azione dell'Autorità sia nei confronti degli operatori energetici, che delle agenzie e dei *list provider* a vario titolo coinvolti nella filiera del trattamento.

Così in primo luogo sono proseguiti i proficui incontri con le altre autorità amministrative indipendenti e con l'Organismo di monitoraggio del codice di condotta per le attività di telemarketing e *teleselling*, finalizzati alla collaborazione e al confronto sulle tematiche di comune interesse. Contestualmente, sono state condotte attività ispettive e istruttorie puntuali o cumulative nei confronti dei singoli operatori economici.

Più in particolare, l'Autorità ha irrogato la sanzione amministrativa pecuniaria di

euro 300.000 per avere svolto attività promozionali realizzate sulla base di consensi raccolti mediante form online che non avevano garantito il conferimento di una valida manifestazione di volontà da parte dei soggetti interessati. In tale occasione, l'Autorità ha dichiarato l'invalidità dei cd. consensi omnibus, intendendo per tali quelle manifestazioni di volontà espresse sulla base di form e informative estremamente generiche che, nelle intenzioni degli utilizzatori, avrebbero avuto l'effetto di legittimare il trasferimento dei dati personali ad una moltitudine indistinta di terzi e società attive nel campo del marketing nonché il successivo utilizzo per proprie finalità promozionali. Nelle motivazioni del provvedimento, è stato chiarito che questa tipologia di consenso non può essere considerata valida, in quanto carente dei requisiti previsti dal RGPD, giacché non consente di esprimere una volontà libera, specifica e granulare, né l'adeguato esercizio dei diritti riconosciuti ai soggetti interessati (provv. 27 febbraio 2025, n. 114, doc. web n. 10114967).

In tale ambito, l'Autorità ha irrogato una sanzione pari a euro 3.850.000 nei confronti di uno dei principali fornitori nazionali di energia e di diverse agenzie ad esso connesse per avere realizzato, attraverso modalità fraudolente, attività di telemarketing e *teleselling* in assenza di un'idonea base giuridica, utilizzando liste illecite in mancanza dei dovuti controlli presso la propria rete di vendita. I relativi due provvedimenti avevano tratto origine da una complessa attività istruttoria caratterizzata da ispezioni simultanee nelle diverse sedi delle società coinvolte. Più in particolare, partendo dalla denuncia di un collaboratore della trasmissione televisiva "Striscia la notizia", l'Autorità ha potuto verificare la sussistenza di attività di call center abusivi (perché operanti in assenza di formale incarico da parte dei committenti, non censiti presso il registro degli operatori di comunicazioni – ROC, obbligo previsto per tutti gli operatori di call center) in possesso di liste anagrafiche di soggetti da contattare telefonicamente per proporre l'attivazione di forniture di servizi energetici (gas e luce). Nello specifico, partendo dalle informazioni ricevute da un ex operatore di uno dei call center coinvolti, nell'esposto erano state denunciate le pratiche scorrette per il procacciamento di contratti in favore di un primario fornitore di energia nazionale da parte di un call center, non formalmente inserito nella filiera delle agenzie del titolare del trattamento, dietro fornitura di liste illecite di contatto provenienti da una terza società. Le chiamate venivano effettuate nei confronti di soggetti che avevano da poco richiesto il passaggio ad altro operatore nel mercato libero dell'energia e del gas, prospettando inesistenti disguidi tecnici e di fatturazione nella migrazione dal gestore "uscente" al gestore "entrante". Parallelamente alle attività di competenza dell'Autorità, vista la possibile rilevanza, anche sotto il profilo penale, delle condotte oggetto di valutazione, è stata trasmessa – già in corso di istruttoria – una nota informativa alla Procura della Repubblica competente.

Dalle attività svolte nei confronti delle agenzie e sub-agenzie è emerso che il call center, sfruttando il canale formale costituito dal contratto di agenzia di tipo "porta a porta" tra il fornitore e un prestanome, era riuscito a caricare un elevato numero di contratti nei sistemi del primo il quale, anche per la carenza di adeguate misure tecniche ed organizzative, non era riuscito ad intercettare l'attività illecita indicata. Inoltre, gli operatori del call center avevano avuto la possibilità di entrare nei sistemi del fornitore adoperando tutti le credenziali collegate ad un unico soggetto censito dalla stessa società fornitrice. Da parte sua il call center aveva ricevuto le liste di *switch-out* da parte di una terza società che, a sua volta, le aveva reperite da dipendenti ed ex dipendenti di società di distribuzione nazionale, senza che fossero stati adottati i necessari presidi a tutela dei dati degli interessati. In considerazione del ruolo di "porta d'ingresso" del telemarketing selvaggio che si è potuto attribuire al titolare del

trattamento, è stato possibile configurare un quadro di responsabilità a carico della compagnia energetica per non aver predisposto misure organizzative e di sicurezza idonee a salvaguardare i dati personali degli interessati coinvolti nei relativi trattamenti illeciti (provv.ti 10 aprile 2025, n. 228, doc. web n. 10127930 e n. 229, doc. web n. 10127964).

Nell'ambito della medesima istruttoria cumulativa scaturita dalle numerose doglianze presentate dai soggetti interessati e dalle risultanze ottenute dal cosiddetto metodo della "settimana campione", l'Autorità ha irrogato rispettivamente una sanzione pari a euro 100.000 nei confronti del titolare del trattamento e una sanzione pari a euro 10.000 nei confronti del responsabile del trattamento, per la realizzazione di attività di telemarketing e *teleselling*, in assenza di un'idonea base giuridica, nonché senza la previa e corretta individuazione dei ruoli soggettivi ricoperti e conseguentemente senza pienamente aderire ai doveri derivanti dai medesimi ruoli (provv.ti 29 aprile 2025, n. 248, doc. web n. 10145986 e n. 249, doc. web n. 10146517).

L'Autorità ha anche rivolto un ammonimento nei confronti di una delle maggiori società operanti nel settore energetico, in relazione all'errata individuazione della base giuridica del trattamento per l'inoltro di comunicazioni finalizzate a saggiare il livello di soddisfazione dei clienti e a indurli alla pubblicazione di una recensione online. In base alle valutazioni dell'Autorità, infatti, la base giuridica del trattamento nel caso di specie doveva essere individuata nell'interesse legittimo, anche in attuazione delle indicazioni contenute nelle linee guida del CEPD 1/2024 sul trattamento dei dati personali effettuato sulla base dell'art. 6, par. 1, lett. f), RGPD (provv. 17 luglio 2025, n. 437, doc. web n. 10176077).

Nello stesso ambito l'Autorità ha irrogato:

- una sanzione pecuniaria pari a euro 25.000 e talune misure correttive, per la realizzazione di trattamenti di dati personali senza la previa e corretta individuazione dei ruoli soggettivi e utilizzando dati personali raccolti mediante *landing page* – proprie o di terzi – che non avevano consentito agli utenti di esprimere un consenso libero, specifico e granulare (provv. 17 luglio 2025, n. 435, doc. web n. 10182814);

- una sanzione pecuniaria pari a euro 35.000 e talune misure correttive, in relazione alla realizzazione di chiamate promozionali al di fuori dei presupposti di legittimità previsti dalla vigente normativa, alla carenza di controlli in merito alla selezione dei *list provider* ed alla legittimità delle liste acquistate (es. verifica anche a campione dei consensi e delle informative, della provenienza dei dati personali ecc.) (provv. 25 settembre 2025, n. 539, doc. web n. 10187997);

- una sanzione pecuniaria pari a euro 5.000 e talune misure correttive in relazione all'inoltro di e-mail promozionali recanti informazioni e accorgimenti grafici manifestamente contraddittori e fuorvianti, tali da rendere difficoltoso l'esercizio dei diritti degli interessati nonché veicolate sulla base di consensi che non potevano ritenersi validi giacché carenti sotto il profilo della previa informazione, della libertà e della specificità (provv. 9 ottobre 2025, n. 592, doc. web n. 10197144);

- una sanzione pecuniaria pari a euro 300.000 e talune misure correttive, in quanto ai fini della registrazione all'area riservata del sito aziendale, utile alla consultazione delle bollette e dello storico dei consumi, la società non aveva svolto alcuna verifica in merito alla identità del soggetto che effettuava la registrazione, né alla e-mail utilizzata. Inoltre, all'esito di un accesso al sito effettuato dall'Ufficio in data successiva alla ricezione della segnalazione, era emerso che in calce al form utile alla registrazione all'area riservata erano presenti tre moduli per il conferimento del consenso, già pre-flaggati sul "si" (provv. 27 novembre 2025, n. 709, doc. web n. 10202135 - Newsletter 17 dicembre 2025, n. 541).

Infine, l'Autorità ha rivolto un ammonimento nei confronti di una importante società nel settore, in ordine alla violazione delle disposizioni vigenti in materia di esercizio dei diritti degli interessati di cui agli artt. 12, da 15 a 22 del RGPD (provv. 18 dicembre 2025, n. 764, doc. web n. 10210454).

11.1.3. Il telemarketing illegale in altri settori commerciali

Piattaforme di messaggistica istantanea

L'Autorità nel corso dell'anno è più volte intervenuta sull'utilizzo improprio delle piattaforme di messaggistica istantanea per finalità promozionali, con particolare riferimento alla creazione di gruppi chat senza l'oscuramento dei dati di contatto dei partecipanti. In un caso specifico, originato da un reclamo, è stato accertato che una società operante nel commercio elettronico aveva inserito il numero di cellulare di un cliente, acquisito tramite una piattaforma di *marketplace* terza, all'interno di un gruppo WhatsApp denominato con il marchio aziendale, unitamente ad altre 46 utenze. Tale operazione, finalizzata all'invio di messaggi promozionali e sconti, aveva reso visibile il numero di telefono di ciascun partecipante a tutti gli altri membri del gruppo. Nel provvedimento adottato, l'Autorità ha ribadito che l'uso di gruppi WhatsApp non è legittimo per finalità commerciali in assenza di uno specifico consenso e al di fuori delle attività a carattere esclusivamente personale o domestico. È stato chiarito che la funzionalità di *opt-out* offerta dalla piattaforma non può surrogare il consenso preventivo, libero e informato necessario per l'inclusione in gruppi promozionali, trattamento che per sua natura comporta la comunicazione di dati personali (il numero di telefono) a terzi. Alla società è stata pertanto comminata una sanzione amministrativa pecuniaria pari a euro 10.000 (provv. 16 gennaio 2025, n. 12, doc. web n. 10112726).

Comunicazioni promozionali tramite posta cartacea

L'Autorità è poi intervenuta nuovamente sul tema delle basi giuridiche per l'invio di comunicazioni promozionali tramite posta cartacea, censurando l'erroneo ricorso al legittimo interesse in assenza di una relazione pertinente tra titolare e interessati. La vicenda ha riguardato una società che aveva inviato circa 15.000 missive cartacee ad azionisti di un istituto bancario per promuovere servizi di assistenza stragiudiziale, utilizzando un elenco fornito da un altro azionista. L'Autorità ha rilevato che il legittimo interesse non poteva costituire una valida base giuridica, mancando i requisiti di concretezza e attualità, nonché una preesistente relazione appropriata con gli interessati tale da rendere ragionevole l'aspettativa del trattamento. È stato altresì ribadito che il legittimo interesse non può surrogare il consenso qualora questo costituisca la condizione di liceità ordinariamente prevista e che, per dati non acquisiti da elenchi pubblici, è necessario il consenso specifico. Nel comminare una sanzione pari a euro 15.000, il Garante ha valorizzato la condotta proattiva della società che aveva interrotto l'invio delle missive e implementato nuove procedure di compliance (provv. 13 febbraio 2025, n. 73, doc. web n. 10119750).

SMS promozionali

L'Autorità si è pronunciata nei confronti di una società impegnata nella consegna di piante e fiori a seguito della ricezione di una doglianza in cui l'interessato aveva lamentato la ricezione di numerosi SMS promozionali senza essere riuscito ad opporsi. In sede istruttoria, inoltre, era emerso che nel portale e-commerce della società era obbligatorio conferire i propri dati e il numero di cellulare per completare l'acquisto, in assenza di una specifica informativa sul successivo utilizzo di tali dati per scopi promozionali ed anche della relativa richiesta di consenso. Preso atto della contestazione, il titolare aveva tempestivamente provveduto a modificare le proprie procedure aziendali attraverso l'acquisizione di uno specifico consenso per l'invio di messaggi promozionali e la cancellazione dei dati del reclamante e di tutte le persone per le quali non era in grado di documentare un idoneo consenso. Per tali ragioni, non si è ritenuto necessario imporre alcuna misura correttiva ed è stata comminata, quale misura proporzionata e

dissuasiva, una sanzione amministrativa pari a euro 40.000 (provv. 13 marzo 2025, n. 155, doc. web n. 10138948).

Il Garante si è poi occupato di alcune palestre appartenenti al medesimo circuito, a seguito di un reclamo concernente diverse comunicazioni promozionali indesiderate, ricevute via SMS e WhatsApp anche dopo che l'interessato aveva manifestato l'opposizione al trattamento. Dall'istruttoria era emerso un quadro di totale disinteresse per i diritti degli interessati che ha reso necessario imporre il divieto di trattare ulteriormente i dati raccolti oltre a predisporre un'ordinanza-ingiunzione per l'applicazione di una sanzione amministrativa pecuniaria pari a euro 6.000 per ciascuna società coinvolta nel procedimento (provv. 27 marzo 2025, n. 174, doc. web n. 10140216).

In un diverso procedimento, l'Autorità ha esaminato il caso di una struttura alberghiera che aveva inviato per diversi anni SMS promozionali a un cliente utilizzando dati raccolti nel 2015 in occasione di un soggiorno, senza aver acquisito uno specifico consenso e senza aver correttamente recepito le reiterate richieste di opposizione. In particolare, il trattamento per finalità promozionali si era protratto per circa nove anni, interrompendosi solo a seguito dell'intervento del Garante. L'Autorità ha richiamato il principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e), RGPD, ribadendo che i dati devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati e che un utilizzo prolungato nel tempo, specie in assenza di un consenso valido e attuale, non rientra nelle legittime aspettative dell'interessato. Pur tenendo conto delle misure correttive adottate, il Garante ha irrogato una sanzione amministrativa pecuniaria pari a 6.000 euro (provv. 23 ottobre 2025, n. 637, doc. web n. 10199166).

A seguito di un reclamo concernente la ricezione di numerosi SMS promozionali inviati da parte di un'università e il tardivo e inadeguato riscontro alla richiesta di esercizio dei diritti, nonché di ulteriori segnalazioni avverso il medesimo titolare, è emerso che quest'ultimo utilizzava, per fini promozionali e anche a distanza di molti anni, i dati che gli interessati avevano rilasciato, al telefono o tramite la compilazione di un form online, unicamente con l'intento di chiedere informazioni in merito ai servizi offerti. Tutti i tentativi di opporsi direttamente nel corso della chiamata sarebbero risultati vani.

Al riguardo il Garante già nel 2023 aveva adottato un provvedimento prescrittivo, inibitorio e sanzionatorio, che viste le più recenti doglianze pervenute è risultato non essere stato integralmente ottemperato dal titolare (provv. 18 luglio 2023, n. 393, doc. web n. 9939507). Per tali ragioni, si è ritenuto necessario adottare alcune misure correttive, indicando al titolare di adeguare i tempi di conservazione dei dati e imponendo nuovamente il divieto di utilizzare, per finalità di marketing, banche dati realizzate senza un idoneo consenso degli interessati. Inoltre, in ragione delle violazioni rilevate, si è ritenuto necessario, quale misura proporzionata e dissuasiva, comminare una sanzione amministrativa pecuniaria pari a euro 60.000 (provv. 9 ottobre 2025, n. 590, doc. web n. 10201409).

Un ulteriore intervento si è reso necessario nei confronti di un rivenditore di franchising di arredamento a seguito di un reclamo concernente la ricezione di numerosi SMS promozionali, nonostante le numerose richieste di cancellazione presentate.

In corso di istruttoria la società ha dichiarato di non aver recepito immediatamente la richiesta del reclamante per mero errore ma di aver provveduto a cancellare i dati interrompendo l'invio di SMS. La società ha altresì rappresentato di aver raccolto i dati del reclamante nel 2012 in occasione di un acquisto da questi effettuato nel negozio.

Nonostante tali assicurazioni fornite dal titolare, l'Autorità ha ritenuto necessario

adottare alcune misure correttive, indicando al titolare di adeguare i tempi di conservazione dei dati e di rivedere le procedure in essere per il recepimento delle richieste degli interessati nonché comminare una sanzione amministrativa pecuniaria pari a euro 6.000 (provv. 23 ottobre 2025, n. 636, doc. web n. 10244075).

In relazione ad un caso, originato dalla presentazione di un reclamo, con il quale, l'interessato aveva lamentato la ricezione numerose e-mail promozionali indesiderate aventi ad oggetto la promozione di un sito web in assenza di un valido consenso, il Garante è intervenuto sulle modalità con le quali il titolare del trattamento possa adeguatamente comprovare di aver acquisito il consenso degli interessati, con particolare riguardo al meccanismo del cosiddetto *double opt-in*. L'Autorità ha infatti osservato che tra i requisiti di liceità del consenso di cui all'art. 7 del RGPD, si configura l'obbligo per il titolare di dimostrare che l'interessato ha prestato il proprio consenso. In tale contesto si deve innanzitutto tenere conto del fatto che il Regolamento non prevede espressamente specifici obblighi normativi per singole fattispecie ma impone il rispetto di generali principi da adattare al contesto, ai potenziali rischi e alle aspettative degli interessati. Partendo da tale presupposto, il Garante ha più volte fornito orientamenti su casi specifici ricordando che la documentazione del consenso in modalità *double opt-in* offre maggiori garanzie e può considerarsi, allo stato dell'arte, una misura minima di protezione per l'interessato ma anche per lo stesso titolare, tenuto a comprovare la liceità del trattamento; analoghe modalità di documentazione del consenso sono indicate anche all'interno del codice di condotta in materia di telemarketing e *teleselling* (provv. 7 marzo 2024, n. 148, doc. web n. 9993808, cfr. Relazione 2024, p. 120). Pertanto, tale misura (o qualsiasi altra che possa offrire un pari livello di garanzia) rientra perfettamente nel quadro normativo, in ragione del combinato disposto dell'art. 7, par. 1 e dell'art. 24, par. 1, RGPD poiché il titolare, tenuto conto del contesto e dei potenziali rischi, deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento e che l'interessato ha prestato il proprio consenso. Per tali ragioni è stata comminata, quale misura proporzionata e dissuasiva, una sanzione amministrativa pari a euro 45.000 (provv. 4 giugno 2025, n. 330, doc. web n. 10143278).

Il Garante ha rilevato l'illecito trattamento dei dati da parte di una società che gestisce una piattaforma online per la vendita di prodotti altoatesini. In particolare, ha ritenuto sussistente la violazione dell'art. 13, par. 1, lett. c) e d), RGPD perché il titolare non aveva reso all'interessato informazioni idonee sul trattamento dei suoi dati personali per finalità di sondaggi somministrati tramite posta elettronica da parte di una società terza (provv. 23 giugno 2025, n. 365, doc. web n. 10161428).

Con riferimento ai tempi di conservazione dei dati personali, il Garante si è occupato di un reclamo, con il quale l'interessato aveva lamentato la ricezione di un'e-mail promozionale da parte di una concessionaria di auto e la richiesta di cancellazione dei propri dati alla medesima società senza ottenere alcun riscontro. In corso di istruttoria, il titolare aveva dichiarato di aver acquisto l'indirizzo e-mail del reclamante in occasione della vendita di un'autovettura nel 2013; il reclamante aveva, tuttavia, replicato che l'indirizzo e-mail in oggetto era piuttosto recente e che, in occasione della predetta vendita, era stato fornito un altro indirizzo. Alla società è stato quindi contestato l'invio di comunicazioni promozionali senza consenso, dal momento che non era stata in grado di documentare l'acquisizione di un idoneo consenso *ab origine* anche per conservare e trattare per finalità promozionali i dati dell'interessato dopo oltre dieci anni. Il titolare aveva comunque provveduto ad adottare diverse misure correttive, con una revisione totale sia dei sistemi aziendali, che delle procedure. Per tali ragioni l'Autorità non ha ritenuto necessario imporre misure correttive; per le violazioni pregresse, invece, ha

adottato un'ordinanza-ingiunzione per l'irrogazione della sanzione amministrativa pecuniaria pari a euro 45.000 (provv. 11 settembre 2025, n. 522, doc. web n. 10181812).

In riferimento al mancato rispetto dei diritti dell'interessato, l'Autorità ha adottato un provvedimento nei confronti di una società per il mancato riscontro alla richiesta di esercizio dei diritti da quest'ultimo avanzata a seguito della ricezione di due e-mail promozionali. La società, già destinataria di un provvedimento correttivo per una condotta analoga, non aveva fornito adeguate giustificazioni alla sua condotta omissiva ma aveva assicurato di aver cancellato i dati del reclamante. Per tali ragioni, si è ritenuto necessario, quale misura proporzionata e dissuasiva, comminare una sanzione amministrativa pecuniaria il cui importo, tenuto conto della natura di microimpresa della società, è stato quantificato in euro 10.000 (provv. 25 settembre 2025, n. 537, doc. web n. 10184761).

A seguito di un'istruttoria avviata su impulso di un reclamo e di una segnalazione relativi alla ricezione di e-mail promozionali indesiderate, nonostante la richiesta di opposizione formulata nei confronti del titolare e asseritamente recepita da quest'ultimo, il Garante ha adottato un provvedimento di ammonimento nei confronti di una società che effettua, per conto di committenti, campagne promozionali tramite e-mail e chiamate automatizzate.

In particolare, la società era stata destinataria di un prudente avviso formulato nel 2023 ai sensi dell'art. 11, comma 1, lett. d) del reg. del Garante n. 1/2019. La ricezione di nuove istanze aveva dunque reso necessario effettuare un accertamento ispettivo *in loco*, all'esito del quale erano emerse alcune criticità relative all'effettiva applicazione delle misure di garanzia per gli interessati, pur sussistendo un'impostazione *privacy oriented* e procedure formalmente adeguate. Tali misure inoltre erano risultate in fase di revisione nell'ottica di adeguarle agli standard imposti dal codice di condotta in materia di telemarketing e *teleselling*.

La società inoltre aveva garantito di aver corretto tutte le difformità rilevate e di aver altresì adottato delle ulteriori misure a garanzia degli interessati quali l'inserimento in *black list* di tutti i dati acquisiti dal *list provider* prima che questi raggiungesse la conformità attesa. Considerato che la società ha prontamente adottato adeguate misure correttive, l'Autorità non ha ritenuto necessario un ulteriore intervento in tal senso, limitandosi a formulare un ammonimento (provv. 25 settembre 2025, n. 576, doc. web n. 10191282).

La duplice *ratio* del provvedimento da ultimo esaminato attiene alla necessità di acquistare liste di dati che documentino in maniera inequivocabile il consenso degli interessati all'utilizzo dei propri dati per finalità promozionali nonché al favore accordato agli operatori del mercato che si adoperano per ottenere quel controllo della filiera auspicato dal codice di condotta.

Nel medesimo ambito, l'Autorità ha accertato gravi carenze nella gestione delle richieste di esercizio dei diritti da parte di una società operante nel settore dell'e-mail marketing. A fronte di numerose segnalazioni relative alla ricezione di messaggi promozionali indesiderati, è emerso che le istanze di accesso, cancellazione e opposizione non erano state tempestivamente trattate, anche perché recapitate nelle caselle spam e prive di adeguate procedure di gestione, in violazione degli artt. 12, 15, 17, 21 e 24 del RGPD. Nel medesimo contesto erano state rilevate criticità nell'acquisizione e nell'utilizzo di liste di contatto provenienti da fornitori terzi, prive di un idoneo consenso. Il Garante ha quindi ingiunto l'adozione di misure organizzative idonee e ha irrogato una sanzione amministrativa pecuniaria pari a 30.000 euro (provv. 23 ottobre 2025, n. 654, doc. web n. 10200530).

A seguito di un reclamo relativo all'invio di una e-mail promozionale non sollecitata e

al mancato riscontro a una richiesta di accesso ai dati personali, l'Autorità ha accertato l'illiceità dei trattamenti di dati personali di una società attiva nel settore della fornitura di software. Nel corso dell'istruttoria, la società aveva dichiarato di non essere in grado di ricostruire l'origine del dato dell'interessato, né di saper individuare una valida base giuridica del trattamento, limitandosi a riferire di aver adottato misure correttive successive. Era emerso, inoltre, che la richiesta di esercizio dei diritti dell'interessato non aveva ricevuto alcun riscontro e che la comunicazione commerciale inviata era carente delle informazioni minime previste dalla normativa. L'Autorità ha pertanto accertato la violazione degli artt. 5, 6, 12, 15 e 24 del RGPD, nonché dell'art. 130, comma 4, del Codice, rilevando l'assenza di una base giuridica del trattamento, il mancato rispetto del principio di *accountability* e l'inadeguatezza delle misure organizzative adottate. Tenuto conto del carattere isolato della condotta e dell'assenza di precedenti, il Garante ha ingiunto alla società di conformare i trattamenti alla normativa vigente e ha applicato una sanzione amministrativa pecuniaria pari a euro 5.000 (provv. 27 novembre 2025, n. 706, doc. web n. 10210014).

Da ultimo, l'Autorità ha esaminato il caso dell'invio di una e-mail promozionale a un professionista il cui indirizzo era stato desunto dal canale YouTube dell'interessato. Il Garante ha escluso che la comunicazione potesse qualificarsi come mero tentativo di contatto professionale, rilevandone invece la natura promozionale e ribadendo che anche in tali ipotesi trova applicazione l'art. 130, comma 1 e 2, del Codice. L'Autorità ha disposto un ammonimento (provv. 18 dicembre 2025, n. 763, doc. web n. 10209904).

Revoca del consenso e periodo di conservazione

L'Autorità si è inoltre pronunciata sul diritto dell'interessato di revocare il consenso alla pubblicazione della propria immagine e di dati personali diffusi a fini promozionali, chiarendo l'inefficacia di eventuali pattuizioni contrattuali volte a limitare tale diritto. La vicenda ha riguardato il reclamo di una professionista che, dopo aver partecipato volontariamente a video-interviste promozionali (casi studio) per una società di consulenza, aveva revocato il consenso e richiesto la rimozione dei contenuti. La società titolare si era opposta alla cancellazione, sostenendo che il consenso fosse stato prestato senza limiti temporali e che la revoca avrebbe causato un danno economico non indennizzato. Il Garante ha ribadito che il consenso è revocabile in qualsiasi momento con la stessa facilità con cui è accordato (art. 7 RGPD) e che tale revoca comporta l'obbligo per il titolare di cancellare i dati senza ingiustificato ritardo, salvo sussista altra base giuridica. È stato al riguardo altresì chiarito che la pretesa di un risarcimento del danno per la revoca del consenso non può costituire una condizione ostativa all'esercizio del diritto alla cancellazione, né legittimare la prosecuzione del trattamento. Avendo la società provveduto spontaneamente alla rimozione dei contenuti prima della conclusione del procedimento, l'Autorità ha ritenuto sufficiente rivolgere un ammonimento al titolare (provv. 10 luglio 2025, n. 415, doc. web n. 10166250).

In un ulteriore procedimento, l'Autorità ha esaminato il caso di una società che, pur avendo acquisito in origine il consenso per finalità promozionali, aveva continuato a trattare i dati dell'interessato anche dopo la revoca manifestata nel 2019, in ragione di una non corretta registrazione dell'opposizione. Dall'istruttoria era altresì emerso che, all'epoca dei fatti, l'informativa privacy aveva indicato quali tempi di conservazione una formulazione piuttosto generica (fino a revoca del consenso), senza alcun riferimento temporale certo, con la conseguenza che il trattamento per finalità promozionali si sarebbe potuto protrarre indefinitamente. Il Garante, ribadito che la definizione preventiva e la chiara indicazione dei termini di conservazione costituiscono requisito essenziale ai sensi degli artt. 5, par. 1, lett. e) e 13, par. 2, lett. a), RGPD, ha rivolto al titolare un ammonimento ed ha ingiunto l'adozione di misure idonee a rendere conformi i trattamenti (provv. 25 settembre 2025, n. 538, doc. web n. 10184782).

L'Autorità è intervenuta su un caso di recensioni online e di diffusione dei dati in rete nei confronti di un'impresa turistica a seguito di un reclamo con il quale l'interessato aveva lamentato la diffusione del proprio indirizzo di residenza da parte del titolare. In particolare, nel dare riscontro ad una recensione rilasciata dall'interessata, il titolare aveva inserito nel corpo del testo l'indirizzo della reclamante senza che lo stesso risultasse necessario e comunque utile al riscontro. Nel corso dell'istruttoria era emerso che il titolare aveva trattato l'informazione per motivi precontrattuali e contrattuali quindi, in particolare, per la compilazione di preventivi e per l'offerta dei servizi di accoglienza della struttura. Pertanto, si è rilevata la carenza sia di idonea base giuridica del trattamento, sia di effettiva finalità che potesse giustificare il trattamento medesimo (in particolare la diffusione dei dati in rete). La condotta collaborativa del titolare nei confronti dell'Autorità, la pronta cancellazione dell'informazione in questione, unitamente alla mancata evidenza circa i danni subiti dall'interessato nonché l'assenza di precedenti violazioni della stessa natura, ha portato il Garante a formulare un ammonimento circa il trattamento illecito rilevato (provv. 9 ottobre 2025, n. 591, doc. web n. 10191645).

L'Autorità ha accertato l'illiceità di un trattamento di dati personali effettuato da un Google partner in relazione a una chiamata telefonica a contenuto promozionale. Il procedimento è scaturito dal reclamo di un interessato iscritto al RPO. Dall'istruttoria, e in particolare dalla trascrizione della telefonata, è emerso che la chiamata non era limitata alla verifica dei dati presenti su Google Maps, finalità dichiarata dal partner, ma conteneva una proposta di consulenza commerciale autonoma della società. L'Autorità ha ritenuto insussistente una valida base giuridica del trattamento e ha accertato la violazione degli artt. 5, par. 1, lett. a) e 6 del RGPD, nonché dell'art. 130 del Codice, anche per la mancata verifica dell'iscrizione nel RPO. Tenuto conto della singolarità della condotta, della breve durata del trattamento dei dati personali e dell'assenza di precedenti ulteriori nei confronti del titolare, l'Autorità ha adottato nei confronti della società un ammonimento e un divieto di ulteriori trattamenti analoghi, senza irrogare sanzioni pecuniarie (provv. 13 novembre 2025, n. 671, doc. web n. 10209743).

In un ulteriore caso, l'Autorità ha esaminato un reclamo avente ad oggetto l'invio di due e-mail promozionali in assenza di consenso, a seguito di un contatto ricostruito dal titolare mediante una ricerca manuale su LinkedIn e la successiva generazione dell'indirizzo di posta elettronica secondo una struttura standardizzata. Il Garante ha ribadito che l'art. 130, comma 2, del Codice impone l'acquisizione del preventivo consenso per l'invio di comunicazioni promozionali via e-mail, a prescindere dalle modalità di reperimento o generazione dell'indirizzo e dal fatto che le informazioni siano pubblicamente accessibili online. Con particolare riguardo all'utilizzo dei dati pubblicati online o sui social network, il Garante ha più volte ricordato che essi non sono liberamente utilizzabili per finalità promozionali, poiché deve essere sempre rispettata la finalità per la quale i dati sono stati originariamente raccolti in accordo con le legittime aspettative degli interessati. Pur ravvisando la violazione degli artt. 6, par. 1, lett. a), RGPD e 130, comma 2, del Codice, l'Autorità ha qualificato l'episodio come violazione minore, in considerazione del carattere isolato della condotta, del tempestivo riscontro all'opposizione dell'interessato e della natura di piccola impresa del titolare, disponendo un ammonimento nei confronti di questi (provv. 18 dicembre 2025, n. 762, doc. web n. 10209888).

11.1.4. Attivazione illecita di schede telefoniche

Nell'ambito del contrasto al fenomeno delle attivazioni non richieste di servizi di comunicazione elettronica, l'Autorità ha adottato provvedimenti sanzionatori nei confronti di *dealer* e intermediari che hanno agito in violazione delle istruzioni dei gestori telefonici, assumendo la qualifica di titolari autonomi del trattamento.

In un primo caso, è stata sanzionata un'impresa individuale per aver attivato indebitamente un contratto di rete fissa. In sede istruttoria era emerso che l'impresa aveva intercettato la richiesta di contratto sottoposta da un utente e non andata a buon fine sul canale web ufficiale del gestore e che, contattando l'interessato tramite WhatsApp, aveva acquisito copia del documento d'identità per finalizzare un'attivazione diversa da quella richiesta, simulando una vendita in presenza. Tale condotta, posta in essere in violazione delle procedure contrattuali di identificazione e al di fuori del canale di vendita autorizzato, ha comportato l'applicazione di una sanzione pari a euro 15.000 (provv. 13 marzo 2025, n. 154, doc. web n. 10137409).

A seguito di reclamo concernente la ricezione di SMS promozionali da parte di una società di *shopping outlet* specializzata nel segmento della vista, nonostante il reclamante si fosse opposto al trattamento dei suoi dati per finalità promozionali, l'Ufficio ha accertato che il titolare: non aveva acquisito un consenso valido, in quanto era stato accorpato alla richiesta di consenso richiesto per altre finalità, inclusa quella "negoziale" per la fornitura del servizio; non aveva comunicato il termine di conservazione dei dati; aveva inviato comunicazioni commerciali senza tener conto dell'esercizio dei diritti del reclamante. Rilevata quindi la violazione degli artt. 5; 6; 7; 12; 13; 15; 17; 21; 24 e 25 del RGPD, nonché dell'art. 130, comma 2, del Codice il Garante ha adottato un provvedimento prescrittivo e sanzionatorio, in cui è stato disposto il divieto di trattamento per finalità promozionali dei dati degli interessati eventualmente ancora presenti nella banca dati del titolare, e irrogato una sanzione amministrativa pecuniaria pari a euro 15.000 (provv. 10 luglio 2025, n. 392, doc. web n. 10164395).

In un altro caso, l'Autorità ha sanzionato una società che aveva effettuato una procedura di portabilità (MNP - *Mobile Number Portability*) all'insaputa dell'interessata, utilizzando una copia fotostatica di un documento d'identità già presente nei propri archivi a seguito di un'interazione commerciale avvenuta anni prima. La società aveva inizialmente attribuito l'accaduto a un errore materiale, fornendo tuttavia nel corso del procedimento versioni contraddittorie e scarsamente collaborative, sostenendo infine una presunta presenza fisica della cliente smentita dagli atti. Il Garante ha innanzitutto confermato che il *dealer*, operando al di fuori delle direttive del gestore telefonico (in particolare riguardo all'identificazione del cliente), agisce come titolare autonomo. In ragione della gravità della condotta, finalizzata all'ottenimento di vantaggi commerciali mediante l'uso illecito di dati personali, e della scarsa collaborazione istruttoria, è stata irrogata una sanzione pari a euro 30.000 (provv. 27 novembre 2025, n. 707, doc. web n. 10209961).

È stato inoltre adottato un provvedimento nei confronti di una nota società produttrice di dispositivi antifurto in relazione ai trattamenti di dati personali di clienti/ex clienti e di potenziali clienti per finalità di *telebooking*, *teleselling* e marketing. In particolare, nei confronti dei potenziali clienti, è stata accertata l'assenza di un consenso informato, specifico e granulare per l'ulteriore trattamento per finalità di marketing poiché la società aveva svolto tre distinti trattamenti (*telebooking*, *teleselling* e marketing) sulla base dello stesso presupposto, ossia la fornitura del numero di telefono per ottenere il preventivo (*telebooking*). Con riferimento agli ex clienti, invece, la società aveva acquisito il consenso senza fornire alcuna indicazione sui tempi di conservazione dei dati. Su tali basi l'Autorità ha adottato un provvedimento sanzionatorio e prescrittivo, irrogando una sanzione amministrativa pecuniaria pari a euro 400.000, imponendo il divieto di ogni ulteriore trattamento per finalità di marketing dei dati dei potenziali clienti acquisiti in assenza di un valido consenso e la relativa cancellazione, e ingiungendo di conformare i trattamenti alle disposizioni del Regolamento con riferimento all'informativa breve contenuta nel box per l'acquisizione del numero di telefono e alla corretta e completa informazione relativa al trattamento di *teleselling* (provv. 27 novembre 2025, n. 708, doc. web n. 10201989).

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

Nel corso del 2025, il numero di notifiche ricevute dall'Autorità 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. n. 83/2012, come sostituito dall'art. 1, comma 243, l. n. 232/2016, è risultato essere pressoché analogo a quello rilevato nell'anno precedente.

11.1.6. 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. Segnatamente, a seguito di alcuni reclami e numerose segnalazioni aventi a oggetto la ricezione di diverse comunicazioni promozionali via e-mail con impossibilità per gli interessati di ottenere risposta alle richieste di cancellazione dei propri dati, l'Autorità ha accertato che, in un caso, le comunicazioni indesiderate – riguardanti la promozione di corsi di formazione erogati dal titolare – erano state inviate dal responsabile del trattamento, almeno a partire dal 2021, a professionisti iscritti a vari ordini professionali.

In sede istruttoria, il responsabile si era attribuito ogni responsabilità dichiarando che il titolare non era a conoscenza della modalità operativa adottata e aveva altresì dichiarato di aver utilizzato dati di contatto estratti da pubblici registri, confermando pertanto l'assenza di un idoneo consenso degli interessati.

Pur tenendo conto delle dichiarazioni rese, si è ritenuto che la società committente non potesse essere considerata del tutto esente da responsabilità dal punto di vista organizzativo, per non aver predisposto alcun tipo di controllo sul fornitore esterno sia in fase di selezione, che durante il lungo periodo di svolgimento dell'attività. Per tali ragioni, oltre ad alcune misure correttive, è stata predisposta un'ordinanza-ingiunzione e irrogata una sanzione pecuniaria pari a euro 15.000 per il titolare del trattamento ed euro 5.000 per il responsabile (provv. 11 settembre 2025, n. 494, doc. web n. 10224441).

L'Autorità ha inoltre esaminato il reclamo di un professionista che aveva ricevuto, in assenza di consenso, una comunicazione promozionale relativa a corsi di formazione accreditati presso gli ordini professionali. La società, accreditata presso il Consiglio nazionale forense, aveva ritenuto di poter contattare gli iscritti sulla base del legittimo interesse, valorizzando l'interesse dei professionisti a conoscere le opportunità formative utili all'ottenimento dei crediti obbligatori. In particolare, il Garante ha ribadito che, se la finalità delle comunicazioni è promozionale e se il canale utilizzato è un mezzo di comunicazione elettronica, la norma applicabile è l'art. 130 del Codice, in quanto *lex specialis* rispetto al Regolamento. In tale contesto, la base giuridica del legittimo interesse non è mai applicabile non essendo contemplata nell'art. 13 della direttiva 2002/58/CE che l'art. 130 del Codice recepisce nell'ordinamento italiano. Tale impostazione non è suscettibile di interpretazione, trattandosi di disciplina di carattere speciale. Pur accertando la violazione degli artt. 6, par. 1, lett. a), RGPD e 130, comma 2, del Codice, l'Autorità, tenendo conto delle numerose circostanze attenuanti, relative all'assenza di un danno per l'interessato, al tempestivo recepimento dell'opposizione, alla natura di piccola impresa del titolare e alle dichiarazioni rese in sede difensiva riguardo alle misure correttive già implementate, ha qualificato il caso come violazione minore, disponendo un ammonimento (provv. 23 ottobre 2025, n. 634, doc. web n. 10197559).

A seguito di un reclamo, l'Autorità ha esaminato il caso dell'invio di e-mail promozionali a professionisti iscritti all'albo degli avvocati, i cui recapiti erano stati estratti dal relativo elenco pubblico. Nel corso dell'istruttoria era emerso che i messaggi, aventi ad oggetto la promozione di servizi formativi, erano stati inviati in assenza di un idoneo presupposto

di liceità. Il Garante ha ribadito che la pubblicità della fonte (ad esempio, la presenza dei dati personali in elenchi pubblici o in fonti liberamente accessibili) non legittima l'utilizzo dei dati per finalità di marketing senza il consenso degli interessati. È stata inoltre affermata la responsabilità della società preponente per avere incaricato l'agente, nell'ambito della propria rete di vendita, senza impartire adeguate istruzioni né effettuare controlli sul trattamento dei dati personali (provv. 23 ottobre 2025, n. 635, doc. web n. 10197577).

In un altro caso, l'Autorità ha esaminato un reclamo relativo alla ricezione di diverse e-mail inviate da una società operante nel settore della mediazione civile e della formazione in materia di risoluzione alternativa delle controversie (ADR), nonché al mancato riscontro a una richiesta di accesso ai dati. Il titolare aveva qualificato le comunicazioni come meramente informative e divulgative, sostenendo che esse non integrassero attività promozionale e che potessero fondarsi sul legittimo interesse, anche in ragione del ruolo professionale dei destinatari. Dall'esame del contenuto dei messaggi, tuttavia, era emerso che essi erano finalizzati a far conoscere i servizi offerti dalla società, invitando i destinatari a interagire tramite appositi link per l'eventuale conclusione di un contratto, con conseguente qualificazione degli stessi come materiale pubblicitario e comunicazioni commerciali ai sensi dell'art. 130 del Codice. Il Garante ha ribadito che, in presenza di finalità promozionali veicolate tramite posta elettronica, trova applicazione la disciplina speciale di cui all'art. 130 del Codice, che non consente il ricorso al legittimo interesse quale base giuridica e richiede il preventivo consenso. Pur qualificando la vicenda come violazione minore in considerazione delle circostanze attenuanti e della natura di microimpresa del titolare, l'Autorità ha adottato un ammonimento e ha imposto il divieto di utilizzare per finalità promozionali ulteriori dati di contatto di professionisti di cui non sia comprovabile l'acquisizione di uno specifico consenso (provv. 4 dicembre 2025, n. 739, doc. web n. 10213792).

Con ulteriore provvedimento, l'Autorità ha esaminato più reclami, presentati da professionisti appartenenti al medesimo studio legale, concernenti la ricezione di e-mail promozionali in assenza di consenso, nonché il mancato riscontro a richieste di informazioni. In sede istruttoria la società aveva dichiarato di aver inviato una sola comunicazione per errore; tuttavia, era emersa la ricezione di ulteriori messaggi promozionali anche dopo l'opposizione degli interessati. È stata pertanto contestata la violazione dell'art. 130 del Codice per l'invio di comunicazioni commerciali senza consenso ad indirizzi di posta elettronica desunti da pubblici registri (quali ad esempio, gli albi professionali), nonché l'omesso riscontro a richieste formulate ai sensi dell'art. 157 del Codice. Pur ravvisando le violazioni, l'Autorità ha ritenuto di poter qualificare il caso come di minore gravità, disponendo un ammonimento. Nella valutazione complessiva della vicenda si è tenuto conto anche delle modalità con cui un reclamante aveva prospettato richieste risarcitorie prima di adire l'Autorità, evidenziando la necessità di preservare il ruolo del Garante quale presidio dell'interesse pubblico, scoraggiando possibili strumentalizzazioni a fini meramente privatistici (provv. 18 dicembre 2025, n. 761, doc. web n. 10222804).

12 Servizi di comunicazioni elettroniche e Internet

12.1. Cookie wall *e altri strumenti di tracciamento dei dati personali*

Consultazione pubblica
Pay or ok

L'Autorità ha avviato una consultazione pubblica volta a valutare la liceità del consenso per trattamenti di profilazione da parte di diversi titolari, e innanzitutto dagli editori di giornali, attraverso l'adozione del cd. modello *pay or ok* (anche denominato *pay or consent* o *consent paywall*). Tale modello impone agli utenti, per accedere ai contenuti, ai servizi o alle funzionalità offerte online, di scegliere se sottoscrivere un abbonamento a pagamento oppure acconsentire al trattamento dei propri dati personali, attraverso cookie e strumenti di tracciamento, ai fini di profilazione commerciale. In mancanza di una delle due opzioni, l'accesso ai siti è bloccato.

L'iniziativa si inserisce nel quadro delle istruttorie già avviate dal Garante nei confronti di numerosi editori di giornali che utilizzano tale modalità di business ritenuta controversa sul piano della normativa privacy, anche dal CEPD, in particolare quanto alla possibilità di considerare libero il consenso eventualmente prestato dall'utente (cfr. parere 8/2024 sul consenso valido nel contesto dei modelli consenso o pagamento attuati dalle piattaforme online di grandi dimensioni del 17 aprile 2024 - cfr. Relazione 2024, p. 207). La maggior parte degli interessati, infatti, pur di accedere gratuitamente ai contenuti o alle funzionalità e ai servizi offerti, acconsente al trattamento dei propri dati, spesso neppure comprendendo appieno gli effetti delle proprie scelte. Allo stesso tempo, l'iniziativa vuole evitare un approccio meramente sanzionatorio da parte dell'Autorità, che rischierebbe di compromettere l'attuale modello di mercato degli editori e degli altri titolari coinvolti senza offrire una valida alternativa in grado di bilanciare adeguatamente le esigenze economiche dei settori interessati, la libera circolazione dell'informazione e il diritto fondamentale alla protezione dei dati personali.

Nell'ambito della consultazione rivolta a tutti i portatori di interessi, sono stati raccolti contributi utili a individuare soluzioni tecniche e operative – come modelli alternativi di accesso ai contenuti – in grado di garantire agli utenti il rispetto dei principi di libertà, specificità e consapevolezza del consenso.

In particolare, sono pervenuti 105 contributi, da parte di diverse tipologie di soggetti, dalla cui analisi comparata è emerso un quadro fortemente polarizzato. Segnatamente, i soggetti favorevoli, numericamente limitati, hanno interpretato il modello *pay or ok* come uno strumento di mercato idoneo a valorizzare economicamente i dati personali, garantire la sostenibilità dei servizi digitali basati sulla pubblicità e preservare la libertà di scelta dell'utente fondata sull'alternativa tra pagamento monetario e consenso al trattamento dei dati, richiamando in particolare la libertà di iniziativa economica. Al contrario, la maggior parte dei contributi ha espresso una posizione critica, evidenziando come tale modello comprometta la libertà e la validità

del consenso, in ragione dello squilibrio di potere tra piattaforme e utenti e dell'assenza di una reale terza opzione, in contrasto con i principi del RGPD, con l'orientamento del Comitato e con i diritti e le libertà fondamentali degli interessati.

Nell'ambito dell'attività di collaborazione instaurata tra il Corpo della Guardia di finanza ed il Garante, nel corso del 2025 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 (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 diverse istruttorie è emerso che nonostante l'avvenuta predisposizione di un banner utile al conferimento del consenso, i siti oggetto di accertamento avevano utilizzato soltanto cookie di natura prettamente tecnica. In altri casi ancora è stato riscontrato che il titolare aveva mantenuto settaggi risalenti, che avevano reso di fatto obbligatorio il conferimento del consenso ai fini della navigazione e/o non avevano consentito di esprimere un consenso differenziato rispetto alle diverse tipologie di cookie utilizzate (cd. principio di granularità e specificità). In un numero ridotto di casi i siti web sono apparsi totalmente carenti degli accorgimenti richiesti dalla normativa in materia di protezione dei dati personali, stante la totale assenza di banner e informativa (cfr. provv.ti 27 febbraio 2025, n. 98, doc. web n. 10118222; 27 febbraio 2025, n. 99, doc. web n. 10118246; 27 marzo 2025, n. 175, doc. web n. 10148519; 27 marzo 2025, n. 176, doc. web n. 10147883; 27 marzo 2025, n. 177, doc. web n. 10148493; 27 marzo 2025, n. 178, doc. web n. 10140251; 29 aprile 2025, n. 246, doc. web n. 10139147; 4 giugno 2025, n. 327, doc. web n. 10152729; 4 giugno 2025, n. 328 doc. web n. 10171713; 4 giugno 2025, n. 329, doc. web n. 10152755; 10 luglio 2025, n. 391, doc. web n. 10162286; 17 luglio 2025, n. 436, doc. web n. 10174517; 23 ottobre 2025, n. 618, doc. web n. 10197361; 4 dicembre 2025, n. 738, doc. web n. 10217124; 18 dicembre 2025, n. 760, doc. web n. 10211780).

Il Garante ha inoltre adottato un provvedimento di ammonimento nei confronti di una web agency italiana specializzata in *digital marketing* avendo rilevato trattamenti di dati personali eccedenti e non necessari rispetto alle finalità dichiarate nonché un'informativa agli utenti non aggiornata e non rappresentativa dei trattamenti effettivamente svolti (provv. 9 ottobre 2025, n. 594, doc. web n. 10193871).

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

L'Autorità ha proseguito l'attività istruttoria/decisoria e di cooperazione a livello europeo (cfr. *infra*) in merito al trattamento dei dati personali sotteso al funzionamento dei servizi di IA generativa.

L'Autorità ha adottato un provvedimento di limitazione definitiva dei trattamenti nei confronti delle società cinesi, titolari di un noto servizio di IA generativa sia su piattaforma web che via app con riferimento alle attività di trattamento dei dati personali di interessati che si trovano nel territorio. La limitazione è stata disposta con

effetto immediato a decorrere dalla notificazione del provvedimento.

Trattandosi di titolari stabiliti in Cina, la notifica del provvedimento è avvenuta in virtù di una collaborazione con l'ambasciata d'Italia a Pechino, alla quale il Garante si è rivolto come da istruzioni fornite dal MAE - Direzione generale per gli italiani all'estero e le politiche migratorie, nella guida alla notifica all'estero di atti amministrativi. La richiesta di collaborazione è stata positivamente riscontrata dall'ambasciata italiana, che ha comunicato all'Autorità di aver trasmesso al locale ministero degli esteri il provvedimento, evidenziando, tuttavia, l'impossibilità di garantire la collaborazione da parte delle autorità cinesi sia ai fini della trasmissione dell'atto amministrativo e della relata di notifica, sia di un riscontro.

Le società che gestiscono il servizio di IA in questione hanno, peraltro, dimostrato per *facta concludentia* di aver ricevuto in notifica il provvedimento *de qua*, interagendo con l'Autorità, in particolare adempiendo parzialmente all'ordine di limitazione mediante rimozione dell'app del servizio dagli app store italiani e sostenendo l'impossibilità tecnica di aderire alla richiesta dell'Autorità di bloccare l'accesso al servizio fornito dall'Italia (provv. 30 gennaio 2025, n. 33, doc. web n. 10098477).

L'istruttoria nazionale avviata nei confronti dei titolari fornitori del servizio fornito dalle società cinesi ha avuto eco anche a livello europeo. In particolare, sono state aperte istruttorie nei confronti dei medesimi titolari anche dalle autorità di controllo della Grecia, dell'Austria e della Francia e la discussione relativa ai trattamenti effettuati da tali titolari prosegue nell'ambito della task force *Generative AI Enforcement* (GAIE) (v. *infra*).

L'Autorità ha concluso l'istruttoria avviata nel corso del 2023, a seguito di un provvedimento d'urgenza di limitazione provvisoria (provv. 2 febbraio 2023, n. 392, doc. web n. 9852214) e successiva sospensione dello stesso (provv. 22 giugno 2023, n. 280, doc. web n. 10013893) nei confronti di una società statunitense, in relazione ad un noto servizio di IA relazionale in grado di simulare ed elaborare conversazioni umane basato su un sistema di IA generativa.

Il provvedimento ha riguardato le violazioni consumate sino al 2 febbraio 2023 (data del provvedimento di urgenza sopra menzionato), segnatamente la violazione degli artt. 5, par. 1, lett. a), 6; art. 5, par. 1, lett. a), 12, 13, 5, par. 1, lett. c), 24 e 25, par. 1, RGPD. In relazione a tali violazioni l'Autorità ha ingiunto alla società, ai sensi dell'art. 58, par. 2, lett. d), RGPD, di conformare, entro trenta giorni dalla notifica del provvedimento, i trattamenti alle disposizioni del Regolamento (nello specifico, conformare la privacy policy agli artt. 5, par. 1, lett. a), 12 e 13 del RGPD ed il sistema di verifica dell'età agli artt. 5, par. 1, lett. c), 24 e 25 del RGPD, ponendo rimedio alle lacune accertate).

Sotto il profilo procedurale, il provvedimento è di particolare interesse in quanto è stata valutata e ritenuta sussistente la giurisdizione euro-unitaria, ai sensi dell'art. 3, par. 2, lett. a), RGPD, atteso che il titolare offre il servizio *de quo* in Italia e la competenza è stata radicata in capo al Garante conformemente al principio per cui, laddove un titolare non disponga di uno stabilimento nell'Unione europea, trova applicazione la regola generale di cui all'art. 55, par. 1, RGPD secondo cui "ogni Autorità di controllo è compente ad eseguire i compiti assegnati ed a esercitare i poteri ad essa conferiti a norma del (…) regolamento nel territorio del rispettivo Stato membro".

Sotto il profilo sostanziale, l'Autorità ha posto enfasi sul rispetto degli obblighi informativi che gravano sul titolare del trattamento, sia con riferimento agli utenti del servizio che ai non utenti, puntualizzando, tra l'altro, come in quest'ultimo caso, attesa l'assenza di una relazione diretta con il titolare del trattamento, sia *a fortiori* da escludere una ragionevole aspettativa degli interessati in merito al trattamento dei loro dati personali. A tal fine, infatti, l'Autorità, in ragione dell'ambito circoscritto ed iperspecializzato in cui aveva operato inizialmente il titolare, ha considerato irrilevanti ai fini del soddisfacimento

degli obblighi di trasparenza i documenti di ricerca, le pubblicazioni, gli articoli e le comunicazioni recanti le informazioni sul trattamento dei dati personali che il titolare aveva pubblicato prima di avviare le attività di trattamento dei dati.

Con riferimento agli obblighi di trasparenza l'Autorità ha altresì colto l'occasione per chiarire, nel solco dell'interpretazione fornita dal CEPD nella decisione vincolante 1/2021, la differenza tra gli obblighi specifici di trasparenza (di cui agli artt. 12-14 del RGPD) e il principio espresso nell'art. 5, par. 1, lett. a), RGPD in quanto, sebbene tali obblighi siano una concretizzazione del principio generale, quest'ultimo ha una portata più ampia e la sua violazione può considerarsi integrata solo nella misura in cui sia connotata da elementi di gravità e sistematicità.

Il provvedimento ha altresì affermato il principio secondo cui il ricorso alla base giuridica contrattuale di cui all'art. 6, par. 1, lett. b), RGPD impone al titolare di dimostrare l'esistenza e la validità del contratto, oltre che l'oggettiva necessità del trattamento ai fini dell'esecuzione dello stesso, e che, pertanto, l'omessa previsione da parte della società in questione di verifiche idonee ad impedire l'accesso al servizio ad interessati minorenni ed a garantire il coinvolgimento del titolare della responsabilità genitoriale nel processo di iscrizione al servizio, come richiesto dalle condizioni contrattuali, comportava la violazione degli artt. 24 e 25, par. 1, RGPD (provv. 10 aprile 2025, n. 232, doc. web n. 10130115). Avverso il provvedimento è stato proposto ricorso ai sensi dell'art. 78 del RGPD e dell'art. 152 del Codice, con contestuale istanza di sospensione cautelare).

L'Autorità è stata coinvolta dall'autorità irlandese (*Data Protection Commission* o anche DPC) in un intenso lavoro di cooperazione, unitamente alle altre autorità europee, in merito al progetto di una nota società statunitense di utilizzare i dati contenuti nei post pubblici degli utenti europei maggiorenni (post, commenti, didascalie, foto, ecc.) e quelli derivanti dall'utilizzo dei servizi di IA generativa offerti dal titolare sui due principali social network del titolare (cd. *first party data*) ai fini dell'addestramento dei modelli proprietari di IA generativa in Europa sulla base del legittimo interesse di cui all'art. 6, par.1, lett. f), RGPD (cfr. par. 21.1). Tale progetto era stato inizialmente lanciato dal titolare nel 2024 e successivamente sospeso a seguito delle prime interlocuzioni con le autorità di controllo europee che avevano riscontrato diverse lacune sotto il profilo della trasparenza e del corretto esercizio del diritto di opposizione, anche da parte dei non utenti dei due servizi coinvolti.

L'attività svolta dall'Autorità nel 2025, alla riproposizione del progetto, in esito alla revisione dello stesso, anche alla luce del parere del Comitato 28/2024 su "taluni aspetti relativi alla protezione dei dati ai fini del trattamento dei dati personali nel contesto dei modelli di AI", è consistita nell'esame della copiosa documentazione inviata dal titolare del trattamento alla DPC e delle analisi preliminari di quest'ultima, nonché nella predisposizione di proposte di modifiche ed integrazioni e commenti, sia per iscritto che attraverso la partecipazione a numerosi web meeting.

In esito a tale lavoro, il Garante ha pubblicato un comunicato stampa informativo sulla tematica e sulle modalità per l'esercizio del diritto di opposizione da parte degli interessati (29 aprile 2025, doc. web n. 10125702).

Analoga attività in cooperazione con le altre autorità europee è stata svolta con riguardo all'esame ed allo studio della documentazione fornita in *accountability* da un'altra nota società statunitense, stabilita in Irlanda, che offre un social network ampiamente utilizzato in Europa. Attesa la localizzazione dello stabilimento del titolare, l'attività di cooperazione è stata condotta dalla autorità irlandese in qualità di *Lead Supervisory Authority* (LSA). Nello specifico, l'iniziativa del titolare riguardava il trattamento dei dati personali degli utenti europei maggiorenni del social network,

per addestrare i propri sistemi di IA generativa a partire dal 3 novembre 2025 sulla base del legittimo interesse di cui all'art. 6, par.1, lett. f), RGPD. Vista l'individuazione di tale base giuridica del trattamento, e in considerazione del conseguente obbligo del titolare di garantire agli utenti un efficace esercizio del diritto di opposizione, l'Autorità ha valutato il corretto funzionamento del sistema di *opt-out* predisposto dal titolare, vale a dire il *toggle switch* (per gli utenti) ed il modulo di *opt-out* (per gli utenti ed i non utenti), e ha fornito un tempestivo riscontro alle richieste della DPC sul punto.

A completamento della propria attività, l'Autorità ha pubblicato sul proprio sito web una scheda informativa volta ad informare gli utenti relativamente al trattamento dei loro dati per finalità di addestramento di IA generativa da parte del titolare in questione. La scheda informativa, pubblicata il 28 ottobre 2025 (doc. web n. 10183938), è strutturata in tre parti: nella prima parte sono indicati nel dettaglio i dati personali che il titolare ha annunciato di voler utilizzare per addestrare i suoi sistemi di IA generativa, ovverosia i dati di tutti gli utenti maggiorenni del suo servizio nell'area SEE, con l'esclusione dei dati rispetto ai quali gli interessati nutrono un'aspettativa di riservatezza, tra cui messaggi privati, credenziali di accesso, dati relativi a metodi di pagamento e carte di credito, dati sulla retribuzione forniti dagli utenti e dati relativi alle candidature attribuibili ad un utente specifico. La seconda parte del documento è invece dedicata alle modalità attraverso cui il titolare ha fornito agli utenti ed ai non utenti le informazioni in ordine al trattamento in argomento ed alla base giuridica del legittimo interesse su cui lo stesso si basa. In collegamento con quest'ultima indicazione, nella terza parte, è resa nota la possibilità di esercizio del diritto di opposizione di cui all'art. 21 del RGPD, e sono inseriti gli *hyperlink* che indirizzano ai due strumenti utili a tal fine.

Nell'ambito di un'attività istruttoria svolta *ex officio,* l'Autorità ha riscontrato la presenza sul mercato di numerosi servizi che consentono agli utenti di utilizzare la voce e/o le immagini anche di terze persone, per la generazione di contenuti audio, fotografici e/o audiovisivi basati su tali voci o immagini.

Di conseguenza l'Autorità ha adottato un provvedimento di avvertimento. Segnatamente, tenuto conto che la tecnologia sulla quale si basano tali servizi si avvale dell'IA per la generazione di contenuti multimediali digitali, audio o video idonei a manipolare la realtà (deepfake), e che la stessa sottende dei trattamenti di dati di natura personale, che potrebbero essere riferiti a soggetti terzi rispetto all'utilizzatore dei servizi medesimi, l'Autorità ha avvertito tutte le persone fisiche o giuridiche che utilizzano, in qualità di titolari o di responsabili del trattamento, servizi di generazione di contenuti basati sull'IA partendo da voci o immagini reali di terze persone, che tale trattamento dei dati personali, qualora effettuato in assenza di un'idonea condizione di liceità e senza la preliminare fornitura di informazioni corrette e trasparenti agli interessati, può, verosimilmente, violare le disposizioni del RGPD, in particolare gli artt. 5, par. 1, lett. a), 6 e 9, RGPD, con tutte le conseguenze, anche di carattere sanzionatorio, previste dalla disciplina in materia di protezione dei dati personali (provv. 18 dicembre 2025, n. 789, doc. web n. 10207132).

Nell'ambito dei servizi di deepfake il Garante ha affrontato altresì il tema dei servizi di cd. *deep nude* ossia quel particolare servizio, offerto anche a titolo oneroso, che, partendo da una foto raffigurante una persona vestita, consente di restituirne una (o un video) ritraente il medesimo soggetto senza indumenti, oltre che di realizzare altre alterazioni sessualmente esplicite, o finanche pornografiche, delle immagini. L'allarme scattato intorno al proliferare di siti e applicazioni online che offrono tale tipologia di servizi in assenza di adeguate misure atte a garantire la liceità dei trattamenti di dati

personali effettuati è, inoltre, stato accresciuto dalla denuncia su articoli di stampa di numerosi interessati, soprattutto donne, anche appartenenti al mondo dello spettacolo, della politica o a soggetti minori di età.

In tale contesto l'Autorità ha disposto un provvedimento di limitazione provvisoria dei trattamenti di dati personali svolti tramite un servizio di *deep nude* afferente ad una società con sede nelle British Virgin Islands (provv. 1° ottobre 2025, n. 574, doc. web n. 10174164).

L'Autorità ha inoltre proseguito l'attività di cooperazione con le altre autorità di controllo su tematiche relative all'IA, nell'ambito della specifica task force costituita in seno al CEPD.

GAIE TF

Il 19 febbraio 2025, il Comitato ha deliberato l'ampliamento del mandato della task force ChatGPT (costituita nell'aprile 2023) e la modifica del suo nome (ora *Generative AI Enforcement* TF, ossia GAIE TF), disponendo che si occupi di promuovere la cooperazione e lo scambio di informazioni sulle possibili azioni di contrasto condotte dalle autorità di protezione dei dati sui casi di IA generativa che non ricadono nel meccanismo dello sportello unico mediante la celere condivisione di informazioni, l'agevolazione di comunicazioni esterne comuni e condivise, l'eventuale redazione di un report che delinei la posizione comune delle autorità sulla materia in argomento.

Le tematiche discusse nell'ambito della task force hanno riguardato principalmente aggiornamenti delle autorità di controllo in relazione ad istruttorie nazionali avviate nei confronti di titolari stabiliti al di fuori dell'Unione europea in relazione ai quali, nei casi in cui sussista la giurisdizione euro-unitaria ai sensi dell'art. 3, par. 2, RGPD, ogni autorità di controllo mantiene la propria competenza esclusiva ad eseguire i compiti di cui all'art. 57 del RGPD ed esercitare i poteri di cui all'art. 58 del RGPD, nonché la valutazione di alcune potenziali azioni collettive nei confronti dei medesimi soggetti. Sono infine state esaminate alcune ipotesi di possibile interazione tra RGPD e DSA nella gestione di casi estranei al meccanismo di sportello unico e si è tenuta una tavola rotonda sullo stato sull'implementazione nazionale del reg. IA.

12.3. *Attività di collaborazione con le altre autorità amministrative indipendenti*

Il Garante ha ricevuto una richiesta di chiarimenti da parte dell'AGCM, volta ad acquisire informazioni in merito al ruolo di Apple nel sistema di autorizzazione al tracciamento *App Tracking Transparency* (ATT) nonché alla conformità dello stesso alle norme in materia di protezione dei dati personali, con riguardo al procedimento avviato dalla stessa AGCM nei confronti delle società Apple Inc., Apple Distribution International Limited e Apple Italia S.r.l., per l'asserita violazione dell'art. 102 del TFUE.

In particolare, l'AGCM ha chiesto chiarimenti su alcuni punti – correlati alla propria decisione di estendere l'oggetto del procedimento ad un presunto abuso di sfruttamento (art. 102, lett. a), TFUE) – sui quali si erano espressi i Garanti francese e tedesco interpellati dalle relative autorità nazionali di concorrenza in relazione a casi nazionali aventi il medesimo oggetto.

È stato pertanto adottato un provvedimento che ha esplicitato con maggior dettaglio i profili oggetto di interesse anche alla luce delle predette pronunce delle autorità di controllo francese e tedesca, nel merito coerenti con le posizioni assunte dal Garante (provv. 4 agosto 2025, n. 456, doc. web n. 10223356).

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

13.1. *Trattamenti di dati personali nell'ambito del rapporto di lavoro privato*

Nell'anno di riferimento l'Autorità ha adottato molteplici provvedimenti relativi al trattamento dei dati nel contesto lavorativo privato, anche relativamente alla fase successiva alla cessazione del rapporto di lavoro. In tale contesto sono stati presi in considerazione, tra l'altro, trattamenti effettuati mediante strumenti tecnologici ai quali si fa ricorso, anche in ambito lavorativo, con sempre maggiore frequenza; ciò comporta una crescente pervasività del controllo del datore di lavoro sull'attività del lavoratore, e conseguentemente un'accresciuta esigenza di garantire l'effettività della tutela del diritto alla protezione dei dati personali.

Più in particolare le questioni trattate hanno riguardato il trattamento di account di posta elettronica aziendale, anche a seguito della cessazione del rapporto di lavoro, la geolocalizzazione del lavoratore, un sistema di valutazione di guida dei conducenti, l'esercizio dei diritti ovvero il diritto di accesso e la cancellazione dei dati, la gestione delle assenze dal lavoro tramite affissione in bacheca aziendale dei relativi nominativi e motivazioni, la formulazione di un modulo per il colloquio di rientro al lavoro a seguito di assenza, il trattamento di dati tratti da social network e da un sistema di messaggistica e quello relativo alla posta elettronica e alla navigazione in Internet.

Si segnala, inoltre, che in data 26 marzo 2025 è stato rinnovato il Protocollo d'intesa tra l'Autorità e l'Ispettorato nazionale del lavoro al fine di proseguire la collaborazione strategica tra le istituzioni firmatarie. In tale contesto, nell'anno di riferimento, sono state avviate sessioni di formazione reciproca tra le due istituzioni in materia di trattamento dati e controlli a distanza dell'attività lavorativa.

Procedimenti disciplinari e dati tratti da social network

Una lavoratrice si è rivolta al Garante dopo che una società le aveva inviato due contestazioni disciplinari, riferite anche al contenuto di comunicazioni effettuate attraverso il suo profilo Facebook e i canali di messaggistica Messenger e WhatsApp. L'Autorità ha stabilito che tali comunicazioni, inviate al datore di lavoro da terzi, sono state raccolte (verificandone anche l'attendibilità e la veridicità) e ulteriormente trattate mediante l'utilizzo nel procedimento disciplinare, in assenza delle condizioni di liceità previste dall'ordinamento.

In proposito è emerso che i commenti della lavoratrice utilizzati dalla società nel procedimento disciplinare erano stati condivisi in un gruppo chiuso di Facebook, circostanza che ha comportato una legittima aspettativa di riservatezza della reclamante.

Il Garante ha altresì ribadito che i dati personali pubblicati sui social network o, più in generale, disponibili in rete, non possono essere utilizzati a ogni fine, solo perché accessibili a un numero più o meno esteso di persone, considerato che tali contenuti, anche quelli presenti nella sezione del profilo accessibile a chiunque, sono messi a disposizione dagli interessati per finalità di comunicazione interpersonale o di libera

manifestazione del pensiero (v. artt. 21 Cost. e 1, l. n. 300/1970, che ne costituisce l'applicazione in ambito lavorativo).

Inoltre la società ha utilizzato anche i contenuti di conversazioni effettuate dalla reclamante con un terzo e con alcuni colleghi, tramite i propri account privati su Messenger e su WhatsApp, al fine di elevare le contestazioni disciplinari nei suoi confronti.

L'Autorità ha ribadito che la corrispondenza e ogni altra forma di comunicazione riferita a "ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza" – e che pertanto ricomprende, allo stato delle tecnologie disponibili, anche lo scambio di messaggi elettronici quali e-mail, WhatsApp, SMS "e simili" (v. Corte Cost. n. 170/2023) – sono tutelate dall'ordinamento anche a livello costituzionale (art. 15 Cost.). Ciò premesso, il trattamento dei messaggi scambiati dalla reclamante, effettuato dalla società, è avvenuto in assenza di base giuridica (artt. 5, par. 1, lett. a) e 6 del RGPD), nonché in violazione dei principi di liceità, finalità e minimizzazione di cui all'artt. 5, par. 1, lett. a), b) e c) e 6 del RGPD, vista anche l'inutilizzabilità dei dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali (v. art. 2-*decies* del Codice), posto che una volta venuta a conoscenza che i dati trasmessi riguardavano comunicazioni private e commenti sul profilo Facebook chiuso, la società avrebbe dovuto astenersi dall'utilizzarli.

Il Garante ha anche accertato che i commenti e le comunicazioni utilizzate per elevare la contestazione disciplinare contenevano opinioni e commenti della reclamante non attinenti allo svolgimento dell'attività lavorativa o all'attitudine professionale, anche alla luce della mansione svolta da quest'ultima. Considerato che in base al principio generale di liceità del trattamento (art. 5, par. 1, lett. a), RGPD) devono essere applicate le disposizioni nazionali più specifiche e di maggior tutela nell'ambito dei rapporti di lavoro (art. 88 del RGPD) e tra queste norme rientra l'art. 113 del Codice, che richiama quanto stabilito dall'art. 8, l. n. 300/1970 e dall'art. 10, d.lgs. n. 276/2003, norme che per l'appunto vietano al datore di lavoro di effettuare indagini e di raccogliere e trattare ulteriormente informazioni su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore, i trattamenti effettuati dalla società nei termini sopra descritti sono avvenuti in violazione delle norme sopra richiamate (provv. 21 maggio 2025, n. 288, doc. web n. 10143261; il provvedimento è stato impugnato davanti al giudice competente per la parte relativa all'ordinanza-ingiunzione).

Posta elettronica aziendale e Internet

Un ex dipendente ha presentato un reclamo all'Autorità lamentando che, pur avendo rifiutato di firmare un modulo di riconsegna delle dotazioni aziendali che conteneva una richiesta di autorizzazione all'accesso alla casella di posta elettronica aziendale, aveva poi appreso che l'accesso alle e-mail era stato comunque effettuato dall'azienda.

Nel corso dell'attività istruttoria, il Garante ha accertato che la società, in base a quanto disposto da regolamenti interni, effettuava, in modo sistematico, la registrazione e la conservazione delle comunicazioni elettroniche e dei log di navigazione in Internet dei dipendenti, anche dopo la cessazione del rapporto di lavoro, riservandosi di potervi accedere per una pluralità di finalità, comprese attività di controllo (sicurezza del sistema, motivi tecnici e/o manutentivi, controllo dell'osservanza delle regole per l'uso dei pc e verifica del rispetto delle regole interne all'uso della rete Internet).

Il Garante ha pertanto accertato che, operando nei termini sopra descritti, la società, in violazione del principio di liceità del trattamento (art. 5, par. 1, lett. a), RGPD), aveva potuto ricostruire ed effettuare un controllo sull'attività dei propri dipendenti, in assenza delle garanzie stabilite, nell'ambito del rapporto di lavoro, ai sensi dell'art. 88 del RGPD, da norme nazionali più specifiche (v. art. 4, l. n. 300/1970, in materia di controlli a

distanza, richiamato dall'art. 114 del Codice come condizione di liceità del trattamento).

Inoltre l'Autorità ha stabilito che attraverso il sistematico tracciamento sopra descritto il titolare del trattamento/datore di lavoro poteva accedere a informazioni relative a fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore, in violazione dell'art. 113 del Codice (che richiama l'art. 8, l. n. 300/1970 e l'art. 10, d.lgs. n. 276/2003).

Alla luce del predetto quadro normativo il Garante ha anche ritenuto che l'individuazione, da parte della società, in sostanziale assenza di una congrua motivazione, di un periodo di conservazione dei log della posta elettronica dei lavoratori pari a sei mesi ovvero un termine ampiamente superiore a quello di 21 giorni quale periodo (in termini generali) indicato dall'Autorità allo scopo di assicurare il funzionamento delle infrastrutture del sistema della posta elettronica (v. documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" - provv. 6 giugno 2024, n. 364, doc. web n. 10026277), si poneva in violazione di quanto stabilito dall'ordinamento in materia di controlli a distanza, la cui effettuazione attraverso l'impiego di strumenti tecnologici è consentita solo al ricorrere di finalità tassativamente individuate dalla norma tra le quali non rientra la verifica dell'osservanza di regole aziendali interne (v. artt. 5, par. 1, lett. a) e 88 del RGPD in relazione all'art. 114 del Codice, che richiama l'art. 4, comma 1, l. n. 300/1970).

Infine, il Garante ha ricordato che il datore di lavoro può, invece, conservare le e-mail contenute nell'account di posta elettronica se l'accesso è riservato esclusivamente all'intestatario dell'account, sempre che, in applicazione dei principi di liceità e minimizzazione, si adottino misure di tipo organizzativo e tecnologico volte ad impedire l'accesso all'archivio a soggetti diversi dall'intestatario, salva la richiesta di quest'ultimo per finalità di assistenza (v. anche provv. 1° febbraio 2018, n. 53, doc. web n. 8159221). Nel caso in cui invece sia possibile per il titolare accedere alle e-mail per finalità consentite dall'ordinamento e in applicazione dei principi di protezione dei dati, dovranno essere previamente esperite le procedure di garanzia in materia di controlli a distanza (provv. 9 ottobre 2025, n. 613, doc. web n. 10185435).

Assenze dal luogo di lavoro

Il Garante, a seguito di una segnalazione, ha adottato un provvedimento nei confronti di una società per avere trattato, in violazione della disciplina di protezione dei dati personali, le informazioni dei propri dipendenti tramite la compilazione, da parte di un responsabile (di varie versioni succedutesi nel tempo) di un modulo attestante il contenuto dei colloqui di rientro al lavoro dopo un'assenza per malattia, infortunio o ricovero.

Ciò è avvenuto in assenza di una adeguata informativa di cui all'art. 13 del RGPD e di un'idonea condizione di liceità del trattamento.

Con riferimento a tale ultimo aspetto è stato accertato che, tramite i predetti moduli, la società aveva trattato, oltre a dati cd. comuni, anche dati appartenenti a categorie particolari ed in particolare quelli relativi alla salute. La condotta dunque aveva violato sia l'art. 6 sia l'art. 9 del RGPD. In proposito, l'Autorità non ha riscontrato l'asserito carattere di volontarietà che, secondo quanto rappresentato dalla società, avrebbe caratterizzato la compilazione del modulo: la formulazione utilizzata in almeno due delle tre versioni era incompatibile con la volontarietà della compilazione dello stesso. Inoltre, è stato ricordato che nell'ambito del rapporto di lavoro, di regola, il consenso (art. 6 par. 1 lett. a), RGPD) non può costituire idonea condizione di liceità del trattamento per quanto riguarda i dati cd. comuni dei lavoratori vista la strutturale asimmetria che caratterizza il rapporto di lavoro e la conseguente impossibilità (salvo limitati casi da accertare volta per volta) di riconoscere al consenso del lavoratore il carattere di libertà. Inoltre, è stato osservato, che, in conformità all'art. 9 par. 2 lett. b), RGPD, per il trattamento dei dati cd. particolari dei lavoratori, non possono costituire

idonea base giuridica né il consenso né il legittimo interesse.

Tra l'altro, l'Autorità ha precisato che, in base a quanto disposto dal d.lgs. n. 81/2008, il medico competente è l'unico soggetto legittimato a trattare, in piena autonomia e competenza tecnica, i dati personali di natura sanitaria indispensabili per lo svolgimento della funzione di protezione della salute e sicurezza dei luoghi di lavoro.

Il Garante ha accertato altresì che la condotta della società aveva violato il principio di minimizzazione poiché i dati così raccolti sono risultati non pertinenti rispetto all'attività che il datore di lavoro avrebbe dovuto effettuare, nel caso di assenza del lavoratore, anche alla luce di quanto previsto dall'art. 2087 c.c., nonché in ragione della ricordata attribuzione dell'attività di sorveglianza sanitaria al medico competente, in base a quanto disposto dal d.lgs. n. 81/2008. Peraltro, alcune delle informazioni di cui si era chiesto l'inserimento nel questionario erano già (legittimamente) conosciute dall'ufficio del personale e ciò aveva comportato una inutile duplicazione dell'acquisizione di dati.

Il Garante ha inoltre accertato la violazione del principio di limitazione della conservazione nonché l'effettuazione di un trattamento di dati non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore, in violazione, quindi dell'art. 113 del Codice che richiama gli artt. 8 della l. n. 300/1970 e 10 del d.lgs. n. 276/2003, nonché, dunque, dell'art. 88 del RGPD.

L'Autorità ha pertanto disposto il divieto del trattamento dei dati raccolti illecitamente, la loro cancellazione e l'irrogazione di una sanzione amministrativa pecuniaria di euro 50.000 (provv. 10 luglio 2025, n. 390, doc. web n. 10154148).

L'Autorità ha deciso su un reclamo presentato da una sigla sindacale, su mandato di alcuni dipendenti di una società di trasporto locale, in merito all'affissione delle tabelle dei turni di servizio sulle bacheche aziendali unitamente alle cause di assenza dal servizio.

Le informazioni relative ai motivi delle assenze, indicate mediante sigle sintetiche ma facilmente decifrabili ("MAL" in luogo di malattia, "104" in luogo di "permesso assistenza disabili, l. n. 104/1992", ecc,) venivano rese disponibili a tutti i dipendenti mediante affissione sulle bacheche aziendali, posizionate presso i depositi aziendali dei mezzi di trasporto utilizzati per la gestione del servizio, nonché tramite l'invio di una e-mail ai dipendenti dell'azienda.

In via generale, l'Autorità ha ricordato che, in base alla disciplina in materia di protezione dei dati personali, il datore di lavoro può trattare i dati personali dei propri dipendenti, anche relativi a categorie particolari di dati (tra cui sono ricompresi i dati relativi alla salute e quelli relativi all'appartenenza sindacale, art. 9, par. 1, RGPD), se il trattamento è necessario per la gestione del rapporto di lavoro e per adempiere a specifici obblighi o compiti previsti da leggi, dalla normativa comunitaria, da regolamenti o da contratti collettivi (artt. 6, par. 1, lett. c), 9, par. 2, lett. b) e 4 e 88 del RGPD).

In base agli elementi acquisiti nel corso dell'istruttoria, è stato accertato che la pubblicazione dei dati personali e particolari contenuti nelle tabelle recanti i turni di servizio aveva determinato una "comunicazione" illecita di dati personali ai sensi dell'art. 2, comma 4, del Codice. I dati personali dei dipendenti non possono, infatti, essere messi a conoscenza di soggetti diversi da coloro che sono parte del rapporto contrattuale né trattati da coloro che, in ragione delle mansioni svolte, non siano autorizzati a accedere a tali dati.

L'Autorità ha quindi ritenuto che la comunicazione delle informazioni relative ai motivi delle assenze da lavoro era avvenuta al difuori delle specifiche competenze e degli obblighi sanciti dalla normativa e, trattandosi di categorie particolari di dati, anche in violazione dell'art. 9 del RGPD. Per tale motivo, è stata irrogata una sanzione pecuniaria pari a euro 10.000.

In particolare, le operazioni di trattamento sopra descritte erano state effettuate in

violazione dei principi di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c), RGPD, in quanto le informazioni sulle cause delle assenze da lavoro non erano risultate necessarie a garantire il regolare avvicendamento e la programmazione dei turni di lavoro (provv. 23 giugno 2025, n. 363, doc. web n. 10161545).

Valutazione dello stile di guida

L'Autorità ha adottato un provvedimento nei confronti di una società, facente parte di un gruppo imprenditoriale multinazionale, che, su indicazione della propria capogruppo, aveva installato, sui veicoli aziendali, un dispositivo telematico satellitare capace di rilevare i comportamenti di guida dei conducenti (come la frenata, l'accelerazione, la velocità, le sterzate e le curve) afferenti sia ai viaggi cd. professionali (svolti cioè nell'ambito dell'attività lavorativa) sia ai viaggi cd. privati, assegnando a ciascuno di questi comportamenti uno *score*. La media dei punteggi, su base mensile, permetteva di associare allo stile di guida di ciascun conducente/dipendente un livello di rischio (basso, medio ed elevato), in base al quale prevedere modalità di intervento differenti per migliorare le azioni di guida.

La documentazione acquisita nel corso dell'istruttoria ha evidenziato numerose criticità nel trattamento posto in essere dalla società, soprattutto rispetto all'idoneità dell'informativa resa che, nel caso di specie, non conteneva indicazioni chiare sui soggetti che rivestivano la qualifica di titolare del trattamento, di responsabili e dei destinatari dei dati raccolti tramite i dispositivi.

La documentazione era stata predisposta, infatti, a livello di gruppo e rivolta a tutte le società affiliate, alcune delle quali con sede fuori del territorio dell'Unione europea. Ciò aveva comportato l'inidoneità dell'informativa, letta anche in combinato con le FAQ, a rappresentare, in maniera trasparente e corretta, le caratteristiche essenziali del trattamento, quali le finalità e i presupposti di liceità, i soggetti autorizzati ad accedere ai dati sullo stile di guida dei conducenti e con quale grado di dettaglio (se cioè informazioni relative ai viaggi professionali o anche ai viaggi cd. privati) nonché le modalità del trattamento (se cioè tramite accesso diretto alla piattaforma o tramite comunicazione).

Oltre alla violazione del principio di correttezza e dell'obbligo di rendere un'informativa idonea (artt. 5, par. 1, lett. a) e 13, RGPD), il Garante ha anche rilevato la violazione dei principi di limitazione delle finalità e di minimizzazione dei dati in relazione all'informativa resa (art. 5, par. 1, lett. b) e c), RGPD), in quanto carente dell'indicazione delle finalità del trattamento e, conseguentemente, dei dati ritenuti pertinenti e necessari al loro perseguimento.

Rilevante è stata la valutazione circa le informazioni raccolte dal dispositivo di telematica satellitare idoneo a rilevare dettagliate informazioni afferenti ai viaggi effettuati dal veicolo ed al relativo utilizzo, quali, ad esempio, la data e l'ora di partenza e di arrivo di ciascun viaggio qualificato come professionale, la percorrenza chilometrica giornaliera con la distinzione del chilometraggio ad uso privato, la percorrenza chilometrica di ogni viaggio con l'indicazione della tipologia di percorso, il consumo di carburante, alcuni indicatori sullo stile di guida del veicolo in termini di sicurezza ed eco-sostenibilità".

Poiché, come già ricordato, il punteggio assegnato a ciascun dipendente aveva tenuto conto del numero complessivo degli eventi rilevati dal dispositivo (ovvero sia dei viaggi privati che di quelli professionali), l'Autorità ha in primo luogo considerato che, sebbene la telematica nel caso di specie fosse sprovvista del sistema di geolocalizzazione (determinando un impatto meno invasivo sul controllo dell'attività lavorativa), cionondimeno il dettaglio delle informazioni rilevate, la loro memorizzazione e la conseguente consultazione per 13 mesi dalla loro rilevazione, la valutazione effettuata sui dati, erano stati tali da determinare, nel loro complesso, un controllo sull'attività del lavoratore in assenza delle procedure di garanzia di cui all'art. 4, l. n. 300/1970 (richiamato dall'art. 114 del Codice come condizione di liceità del trattamento) e

quindi in violazione degli artt. 5, par. 1, lett. a) e 88 del RGPD.

L'Autorità ha poi ritenuto che l'acquisizione delle predette informazioni relative anche ai viaggi privati aveva consentito al datore di lavoro di trattare anche dati non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore, soprattutto in considerazione dell'uso privato del veicolo anche da parte dei familiari del dipendente interessato. Tale attività si è posta così in contrasto con la disposizione di cui all'art. 8, l. n. 300/1970 (richiamato dall'art. 113 del Codice come condizione di liceità del trattamento) che vieta al datore di lavoro di effettuare indagini, anche tramite terzi, "su fatti non rilevanti per l'attitudine professionale", sia al momento dell'assunzione che durante il rapporto di lavoro.

Il Garante ha, quindi, ordinato la cancellazione dei dati e delle informazioni raccolte dai suddetti dispositivi, inerenti ai viaggi complessivamente svolti dagli interessati, e ha ingiunto il pagamento di una sanzione pecuniaria pari a euro 120.000 (provv. 18 dicembre 2025, n. 755, doc. web n. 10213711).

Sistemi di geolocalizzazione

A seguito della presentazione di un reclamo, l'Autorità ha accertato la violazione della disciplina in materia di protezione dei dati personali da parte di una società di autotrasporti che aveva installato sui veicoli aziendali (nello specifico 50 trattori) un sistema GPS per la loro rilevazione geografica. Nel corso dell'istruttoria, svolta mediante accertamento ispettivo presso la sede della società, era emerso che il suddetto sistema aveva consentito, attraverso la piattaforma web messa a disposizione dalla società fornitrice del sistema, di acquisire informazioni relative alla posizione del veicolo, al suo stato (acceso o spento), alla telemetria e, indirettamente, anche all'attività degli autisti, in modo continuativo, comprendendo anche le pause dell'attività lavorativa.

Le informazioni raccolte dal sistema venivano poi conservate per un periodo di 180 giorni.

L'Autorità ha, quindi, ritenuto che le modalità del trattamento in concreto svolte erano state eccedenti e non proporzionate rispetto agli scopi e alle finalità dichiarate nell'informativa, perseguibili mediante il trattamento di informazioni più limitate.

Oltre ad avere accertato la violazione degli artt. 5, par. 1, lett. a) e 13 del RGPD con riferimento all'inidoneità dell'informativa resa nei confronti dei propri dipendenti, l'Autorità ha evidenziato come la raccolta delle informazioni particolareggiate sulla posizione del veicolo (rilevata anche durante le pause dell'attività lavorativa) e, indirettamente, sull'attività degli autisti (identificabili tramite il numero di targa associato), con la possibilità di visualizzare su mappa i percorsi effettuati, unitamente alla conservazione dei dati raccolti per un periodo di 180 giorni fossero contrarie ai principi di minimizzazione dei dati e di limitazione della conservazione di cui agli artt. 5, par. 1, lett. c) ed e) del RGPD.

Soprattutto, l'Autorità ha ritenuto che tale attività fosse stata realizzata in difformità a quanto previamente autorizzato dall'Ispettorato del lavoro territorialmente competente, ai sensi dell'art. 4, l. n. 300/1970, con ciò realizzando un monitoraggio illecito sull'attività dei dipendenti anche in considerazione della mancata adozione di soluzioni tecnologiche tali da impedire il trattamento di dati ulteriori e non pertinenti rispetto alle finalità organizzative e produttive.

L'Autorità ha quindi accertato anche la violazione del 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, irrogando una sanzione pecuniaria pari a euro 50.000 (provv. 16 gennaio 2025, n. 7, doc. web n. 10112287).

Account di posta elettronica aziendali

Una società, dopo la cessazione del rapporto di lavoro con un dipendente, aveva mantenuto attivo l'account di tipo individualizzato a suo tempo assegnato nell'ambito del rapporto di lavoro e lo aveva reindirizzato su un altro account aziendale, accedendo

13

così attraverso i propri referenti, per un periodo significativo di tempo (circa sette mesi), al contenuto dei messaggi pervenuti sull'indirizzo e-mail riferito all'ex dipendente. L'Autorità ha stabilito che il trattamento di dati personali che ne è conseguito aveva travalicato quanto sarebbe stato necessario per "non perdere rapporti e comunicazioni" con clienti e fornitori, come argomentato dalla società. In proposito, in base all'orientamento consolidato del Garante, in applicazione dei principi di necessità e minimizzazione, dopo la cessazione del rapporto di lavoro il titolare deve rimuovere l'account dopo averlo previamente disattivato, adottando nel contempo sistemi automatici volti ad informare i terzi della cessazione e, se del caso, fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale dell'impresa (v. linee guida del Garante per posta elettronica e Internet, 1° marzo 2007, spec. punto 5.2, lett. b; tra gli altri, provv.ti 27 aprile 2023, n. 171, doc. web n. 9909235; 9 marzo 2023, n. 68, doc. web n. 9877754) (provv. 13 febbraio 2025, n. 63, doc. web n. 10113552).

In un caso analogo la società aveva mantenuto attivo l'indirizzo di posta elettronica dopo la conclusione del rapporto di lavoro e l'aveva reindirizzato sull'indirizzo del responsabile dell'ufficio per circa un anno, senza fornire riscontro specifico all'istanza di cancellazione presentata dall'interessato nei tempi previsti dall'ordinamento (provv. 17 luglio 2025, n.427, doc. web n. 10182762).

L'Autorità, a seguito della presentazione di un reclamo, ha adottato un provvedimento nei confronti di una società per non avere fornito riscontro a un'istanza, reiterata, di esercizio dei diritti presentata dal reclamante (cancellazione e accesso), dunque in violazione degli artt. 12, 15, e 17 del RGPD. L'Autorità ha inoltre sanzionato la società che, in qualità di titolare del trattamento, aveva predisposto l'inoltro, ad altro indirizzo e-mail, costantemente monitorato, delle comunicazioni in entrata, pervenute successivamente alla cessazione del rapporto di lavoro (30 settembre 2021), sull'indirizzo di posta elettronica assegnato al reclamante, mantenuto attivo per un periodo significativo di tempo (fino, quantomeno, alla presentazione dell'istanza di esercizio dei diritti del reclamante del 7 giugno 2022), in violazione pertanto dell'art. 5, par. 1, lett. b), c), e), RGPD. Con specifico riferimento all'eventuale consenso fornito dal reclamante quale elemento per legittimare la lesione del diritto alla protezione dei dati personali dell'interessato, il Garante ha precisato che la società non aveva fornito evidenze di un consenso prestato dal reclamante in tal senso e formalmente acquisito dal titolare del trattamento, e ribadito che lo squilibrio di potere tra il datore di lavoro e il lavoratore rende improbabile che il lavoratore presti liberamente il proprio consenso al datore di lavoro per un trattamento di dati che lo riguarda (in proposito sono state richiamate le linee guida sul consenso ai sensi del RGPD adottate dal CEPD il 4 maggio 2020). È stato inoltre accertato che il trattamento effettuato dalla società sull'account di posta elettronica aziendale individualizzato e assegnato al reclamante era stato posto in essere in assenza di idonea informativa e dunque in violazione anche del principio di correttezza. L'Autorità, per le violazioni riscontrate, ha disposto una sanzione pecuniaria di euro 8.000 (provv. 16 gennaio 2025, n. 8, doc. web n. 10110927).

L'Autorità ha avviato l'istruttoria preliminare nei confronti di una società, a seguito della presentazione di un reclamo da parte di un ex dipendente che aveva lamentato il mancato riscontro all'istanza di esercizio dei diritti con cui aveva chiesto di ricevere copia, oltre che dei dati contenuti nel suo fascicolo personale, anche di tutta la corrispondenza in entrata e in uscita presente sulla casella di posta elettronica aziendale di tipo individualizzato utilizzata nel corso del rapporto di lavoro. A seguito dell'invito dell'Autorità ad aderire, la società aveva fornito copia della corrispondenza intrattenuta dal reclamante negli ultimi cinque anni, precisando che, dopo l'interruzione del rapporto di lavoro, aveva mantenuto attivo l'account di posta elettronica dello stesso al fine di

consentire un'attività di *digital forensic* che gli fornisse prova della violazione del patto di non concorrenza. Nel corso dell'istruttoria, è stato possibile verificare che l'attività di *digital forensic*, svolta a posteriori sull'account del reclamante aveva consentito l'estrazione di documenti e di e-mail molto risalenti nel tempo che tuttavia non si erano rivelati sufficienti nell'ambito del procedimento giudiziario per accertare la violazione della condotta illecita. Per questo motivo, la società aveva disposto che l'account continuasse a rimanere attivo e a ricevere messaggi che venivano sistematicamente letti da persona autorizzata. Questa specifica operazione è stata ritenuta dall'Autorità particolarmente grave, non soltanto perché protrattasi per un considerevole periodo di tempo e su una molteplicità di documenti (in violazione dei principi di minimizzazione e di limitazione della conservazione), ma anche perché aveva di fatto consentito alla società di effettuare un monitoraggio sulla corrispondenza del reclamante che aveva riguardato indistintamente tutte le e-mail transitate nel tempo, con conseguente violazione della specifica disciplina di settore di cui alla l. n. 300/1970. Tra l'altro, come confermato dalla società nel corso dell'istruttoria, tale procedura era stata effettuata in deroga alle regole aziendali che, invece, prevedevano che, alla cessazione di un rapporto di lavoro, l'account venisse disattivato e la corrispondenza cancellata e, quindi, senza che l'interessato ne fosse stato informato. In proposito, il Garante ha precisato che, in termini generali, l'informativa deve contenere la descrizione di operazioni di trattamento, di per sé, lecite; l'aver informato l'interessato rispetto a un trattamento illecito non scrimina infatti la condotta. Accertata pertanto l'illiceità della condotta posta in essere dalla società, oltre a comminare una sanzione amministrativa pecuniaria pari a euro 40.000, l'Autorità ha prescritto di conformare i documenti informativi alla disciplina in materia di protezione dei dati personali e vietato l'ulteriore trattamento dei dati relativi alla posta elettronica dei dipendenti, con particolare riferimento alla conservazione della corrispondenza (provv. 18 dicembre 2025, n. 808, doc. web n. 10216459).

In un analogo caso, l'Autorità ha deciso su un reclamo da parte dell'amministratore delegato di un importante gruppo imprenditoriale, che aveva lamentato il mancato accesso alla propria casella di posta elettronica successivamente alla cessazione della carica con conseguente inoltro delle e-mail a un altro account aziendale. Nonostante avesse formulato un'istanza volta a ottenere la disattivazione dell'account e l'accesso alla corrispondenza nel frattempo pervenuta, non aveva ricevuto alcun riscontro nei termini indicati dal Regolamento. Nel corso dell'istruttoria, era stato accertato che la società aveva mantenuto attivo l'account individualizzato per i due mesi successivi all'interruzione del rapporto di lavoro, provvedendo, in questo frangente, all'inoltro su un altro account aziendale della corrispondenza nel frattempo pervenuta per asserite mere esigenze organizzative oltre che per difesa dei propri diritti. L'Autorità ha quindi ribadito l'orientamento consolidato del Garante, in applicazione dei principi di necessità e minimizzazione, in base al quale una volta cessato il rapporto di lavoro il titolare deve rimuovere l'account dopo averlo previamente disattivato, adottando nel contempo sistemi automatici volti ad informare i terzi della cessazione e, se del caso, fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale dell'impresa, provvedendo altresì ad adottare misure idonee a impedire la visualizzazione dei messaggi in arrivo, durante il periodo in cui tale sistema automatico è in funzione. Non essendo state adottate tali cautele, la condotta della società è stata ritenuta illecita perché contraria ai principi di liceità, di minimizzazione dei dati e di limitazione della conservazione (art. 5, par. 1, lett. a), c) ed e), RGPD) nonché in violazione degli artt. 12 e 15 del RGPD per avere la medesima società limitato il diritto di accesso dell'interessato alle sole e-mail di carattere personale ed escluso quelle afferenti all'attività lavorativa. Per tale motivo, l'Autorità ha irrogato una sanzione amministrativa pecuniaria pari a euro 40.000. L'Autorità ha, invece,

osservato che il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati – riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente e che, nel caso specifico, le comunicazioni elettroniche erano state ricevute su un account di tipo individualizzato successivamente all'interruzione del rapporto di lavoro, motivo per il quale il limite imposto dalla società (limite che non è contemplato da alcuna disposizione del RGPD) non era lecito (provv. 18 dicembre 2025, n. 754, doc. web n. 10213574).

Di interesse un altro provvedimento adottato nei confronti di un datore di lavoro, concernente la lamentata persistente attivazione (a seguito di cessazione del rapporto contrattuale) dell'indirizzo e-mail personale adibito alle esigenze connesse allo svolgimento del rapporto di lavoro. Nel caso di specie si è ravvisata la violazione degli artt. 5, par. 1, lett. a), c), e) e 13 del RGPD (provv. 23 giugno 2025, n. 364, doc. web n. 10161563).

L'Autorità ha adottato un provvedimento nei confronti di una società che, in qualità di titolare del trattamento, aveva creato un indirizzo di posta elettronica aziendale contenente il nome e il cognome del reclamante, senza informarlo di ciò e mettendo il predetto account a disposizione di terzi, nello specifico dei propri dipendenti e dei collaboratori della società appaltatrice di servizi logistici, e non del reclamante. L'indirizzo di posta, formalmente individualizzato intestato al reclamante, era stato dunque reso, di fatto, un account condiviso tra una molteplicità indefinita di soggetti (anche terzi rispetto alla società) che per più di tre anni l'avevano utilizzato, per esigenze asseritamente "organizzative/produttive".

Il trattamento è stato ritenuto illecito per una molteplicità di violazioni ovvero per:

- la violazione del principio di liceità perché il trattamento era stato effettuato in assenza di una idonea base giuridica;
- la violazione del principio di correttezza in quanto anche nell'ambito del rapporto di lavoro l'esecuzione del contratto deve essere conforme a buona fede e correttezza (art. 1375 c.c.);
- la violazione del principio di minimizzazione posto che l'utilizzo dell'account in esame non era stato adeguato né pertinente rispetto alle finalità perseguite;
- la violazione del principio di limitazione delle finalità e del principio di esattezza in quanto un account di posta elettronica aziendale individualizzato deve essere utilizzato, essendo un dato personale dell'intestatario, dal soggetto al quale si riferisce e non da terzi, come, invece, era accaduto nel caso di specie, ciò anche a tutela, tra l'altro, di coloro che vi entrano in contatto scambiando corrispondenza con l'account in questione;
- la violazione dell'obbligo di idonea informativa quale espressione del principio di correttezza.

Il Garante ha pertanto ordinato alla società di predisporre documenti contenenti le informazioni sui trattamenti relativi agli account di posta elettronica aziendale che siano conformi alla disciplina di protezione dei dati personali e il pagamento di una sanzione amministrativa pecuniaria di euro 15.000 (provv. 25 settembre 2025, n. 534, doc. web n. 10184744).

13.2. *Diritto di accesso ai dati personali nell'ambito del rapporto di lavoro*

A seguito di una richiesta di accesso ai propri dati personali da parte di un lavoratore, una società, dopo aver chiesto di fornire alcuni chiarimenti, che l'interessato aveva tempestivamente inviato allo stesso indirizzo e-mail presso il quale aveva inviato l'istanza, non aveva fornito alcun riscontro nel merito, asseritamente a seguito di un disguido interno.

L'Autorità, con riferimento all'indirizzo e-mail utilizzato dal lavoratore per presentare l'istanza e fornire i chiarimenti richiesti, ha tra l'altro ricordato che, anche in base a quanto indicato dalle linee guida 01/2022 sui diritti degli interessati - Diritto di accesso del CEPD, il titolare del trattamento non può prescrivere un formato specifico per le istanze di esercizio del diritto di accesso né, in linea di principio, specifici requisiti nella scelta di un canale di comunicazione per entrare in contatto con il titolare stesso. Inoltre, alla luce di quanto stabilito dall'art. 12 del RGPD e in applicazione del principio di correttezza, il titolare avrebbe dovuto in ogni caso fornire i dati personali oggetto dell'istanza in relazione ai quali non era stata manifestata l'esigenza di richiedere chiarimenti all'interessato, tenuto anche conto che quest'ultimo era sottoposto a un procedimento disciplinare e aveva pertanto necessità di accedere ad ogni possibile elemento a propria difesa (come esplicitato nella richiesta di accesso).

Con il provvedimento l'Autorità ha infine ribadito che non spetta al titolare del trattamento valutare i motivi sottostanti alla richiesta di esercizio dei diritti, né l'interessato è tenuto a fornire spiegazioni relative alle ragioni della presentazione dell'istanza (provv. 21 maggio 2025, n. 289, doc. web n. 10162944).

In un altro caso l'istanza di accesso era stata presentata da un ex dipendente in relazione alle certificazioni di alcuni corsi di formazione svolti prima del trasferimento di ramo d'azienda. Sebbene le richieste di accesso, inviate tramite e-mail, non avessero fatto espresso riferimento alla disciplina in materia di protezione dei dati personali, l'Autorità ha stabilito che l'oggetto e il significato della richiesta erano stati sufficientemente chiari (la consegna di attestati di formazione riferiti all'interessato) (provv. 11 settembre 2025, n. 571, doc. web n. 10183903).

In un altro caso il diritto di accesso, esercitato dopo la cessazione del rapporto di lavoro con una società, riguardava i dati contenuti nella posta elettronica aziendale. La società aveva fornito all'interessato una risposta negativa, rappresentando che l'ex lavoratore avrebbe già potuto estrarre le proprie e-mail dal computer aziendale restituito dopo alcuni giorni dalla cessazione del rapporto di lavoro e che la casella di posta elettronica aziendale avrebbe dovuto essere utilizzata "solo ed esclusivamente per fini lavorativi".

L'Autorità ha ribadito che la presenza di informazioni relative ai clienti della società nella corrispondenza presente nell'account dell'e-mail aziendale non incide sulla legittimità dell'istanza di accesso, considerato che attraverso la posta elettronica aziendale possono essere veicolate comunicazioni che, anche nell'ambito dell'attività professionale svolta nel contesto del rapporto di lavoro, devono essere tutelate da ingerenze illecite e non proporzionate rispetto alle finalità perseguite.

Tale tutela è applicabile anche al di fuori del lavoro subordinato, laddove il rapporto attribuisca comunque al titolare del trattamento il potere di impostare l'ambito e le caratteristiche della collaborazione, in particolare, come nel caso oggetto del provvedimento, nel rapporto di agenzia.

Quanto alla circostanza che il reclamante avrebbe già avuto la possibilità di accedere al contenuto delle e-mail, l'Autorità ha ribadito che ciò non osta alla possibilità di esercitare, anche successivamente, una richiesta di accesso al titolare del trattamento posto che lo stesso Regolamento prevede espressamente la possibilità che l'interessato presenti più richieste di accesso (art. 12, par. 5, RGPD).

Con riferimento, infine, all'attività di tutela dei diritti in fase contenziosa o precontenziosa, rappresentata dalla società, l'Autorità ha rammentato che, in base a quanto stabilito dall'art. 2-*undecies* del Codice, l'esercizio dei diritti di cui agli artt. da 15 a 22 del RGPD, può subire limitazioni solo qualora dall'esercizio del diritto possa derivare un pregiudizio effettivo e concreto all'esercizio di un diritto in sede giudiziaria

e che anche in questo caso il titolare è tenuto a motivare le ragioni della limitazione del diritto in sede di riscontro, cosa che non è avvenuta nel caso di specie (provv. 9 ottobre 2025, n. 589, doc. web n. 10197127).

13.3. *La protezione di dati personali nell'ambito del rapporto di lavoro pubblico*

Nel 2025, 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 o 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.

13.3.1. Trattamenti di dati personali mediante dispositivi tecnologici

13.3.1.1. Controlli a distanza su metadati di posta elettronica, navigazione web e geolocalizzazione del dipendente in lavoro agile

Lavoro agile

Nell'ambito di accertamenti, anche di natura ispettiva, avviati d'ufficio nei confronti di una regione al fine di verificare l'osservanza delle norme in materia di protezione dei dati personali in relazione ai trattamenti posti in essere in ambito lavorativo, anche con riferimento alle modalità di svolgimento del cd. lavoro agile, il Garante è intervenuto – tra l'altro – sul tema del trattamento dei metadati di posta elettronica e dei log di navigazione in Internet generati dal personale dipendente nello svolgimento della propria attività lavorativa. In particolare, sotto il primo profilo, è stato accertato che i metadati di posta elettronica venivano conservati dalla regione –, in assenza della previa stipulazione di un accordo collettivo con le rappresentanze sindacali (art. 4, comma 1, l. n. 300/1970), cui la regione era comunque addivenuta in corso d'istruttoria, – per un ampio periodo temporale, complessivamente pari a 90 giorni, anche per finalità di sicurezza informatica. Al riguardo, nel richiamare i chiarimenti forniti con il documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", adottato, a seguito di consultazione pubblica (cfr. provv. 6 giugno 2024, n. 364, doc. web n. 10026277), l'Autorità ha accertato la violazione da parte della regione degli artt. 5, par. 1, lett. a), 6 e 88, par. 1, RGPD, nonché 114 del Codice, ricordando in particolare come la conservazione di tali metadati per un esteso arco temporale per fini riconducibili all'alveo del comma 1 del cit. art. 4, l. n. 300/1970, avvenendo automaticamente e indipendentemente dalla percezione e dalla volontà del lavoratore, determina il rischio di un indiretto controllo a distanza dell'attività dei lavoratori e richiede pertanto l'esperimento delle garanzie procedurali previste dalla legge.

Log di navigazione

Quanto, invece, al trattamento dei log di navigazione in Internet, raccolti e conservati dalla regione per un arco temporale prolungato, pari a 365 giorni, il Garante ha evidenziato come tale trattamento aveva dato luogo ad un monitoraggio sistematico e generalizzato dell'attività dei dipendenti, rilevando anche in tal caso l'assenza di accordi previi con le rappresentanze sindacali. Il Garante ha ricordato che l'esigenza di ridurre il rischio di usi impropri della navigazione in Internet, da parte dei dipendenti, non giustifica ogni forma

di interferenza nella vita privata, potendo in generale essere soddisfatta mediante la predisposizione di misure tecniche e organizzative idonee a prevenire in radice che le eventuali informazioni relative alla sfera extralavorativa vengano raccolte dal datore di lavoro, dando luogo a trattamenti di informazioni personali "non pertinenti" che ricadono nell'ambito di applicazione dell'art. 113 del Codice. All'esito dell'attività istruttoria, il Garante ha quindi accertato la violazione degli artt. 5, par. 1, lett. a), c) ed e), e 25 del RGPD, e 113 del Codice, in riferimento all'art. 8 della l. n. 300/1970 e all'art. 10, d.lgs. n. 276/2003. In ragione dei trattamenti ancora in essere, il Garante ha prescritto alla regione di adottare misure tecniche e organizzative aggiuntive rispetto a quelle già in atto al fine di assicurare che l'effettiva possibilità di risalire all'identità del singolo dipendente che ha effettuato la navigazione web risulti in concreto estremamente improbabile; in particolare, tra le misure prescritte, il Garante, anche tenuto conto dell'esperienza applicativa riscontrata in diverse istruttorie che avevano coinvolto altre p.a. aventi caratteristiche analoghe a quelle della regione in termini di estensione territoriale, ambiti di competenza ed entità del personale dipendente impiegato, ha richiesto di assicurare l'anonimizzazione dei log relativi ai tentativi di accesso falliti ai siti web censiti nella apposita *black list*, ivi compresi quelli allo stato presenti nei sistemi, e la riduzione a 90 giorni del termine di conservazione dei log di navigazione in Internet, con possibilità di conservazione per un periodo ulteriore previa anonimizzazione degli stessi, in modo da non consentire l'identificabilità del dipendente. Sulla base delle riscontrate violazioni, anche attinenti ad altri profili, connessi al trattamento dei dati relativi alle richieste di assistenza tecnica del personale dipendente, il Garante ha altresì comminato specifiche sanzioni amministrative di natura pecuniaria (provv. 29 aprile 2025, n. 243, doc. web n. 10134221; v. anche Newsletter 30 maggio 2025, doc. web n. 10135126).

Geolocalizzazione

Sempre con riferimento ai trattamenti di dati personali nell'ambito dello svolgimento dell'attività lavorativa in modalità agile, a fronte di uno specifico reclamo e di una segnalazione del Dipartimento della funzione pubblica, il Garante si è altresì pronunciato sul caso di un'azienda regionale che, in base alle procedure interne, aveva provveduto, per il tramite di un'applicazione, alla rilevazione della posizione geografica del personale operante in smartworking, acquisendo le coordinate geografiche dello smartphone o del PC del dipendente che aveva timbrato, unitamente al suo codice identificativo, alla data e all'ora della timbratura, in entrata e in uscita. Tutto ciò avveniva sia in via generale, all'atto della quotidiana timbratura da parte del dipendente, in occasione dell'inizio e della fine dell'attività lavorativa, sia – come accaduto nel caso oggetto di reclamo – nell'ambito di puntuali attività di controllo mirato su specifici dipendenti. Al riguardo, il Garante, nel richiamare le peculiarità della prestazione lavorativa in modalità agile e nel ricordare come, anche in tal caso, l'impiego di strumenti tecnologici da parte del datore di lavoro, dai quali derivi anche la possibilità di controllare a distanza l'attività dei lavoratori, può avvenire esclusivamente per il perseguimento delle tassative finalità previste dalla legge, ha evidenziato come le procedure utilizzate dall'azienda avevano dato luogo ad un monitoraggio diretto dell'attività dei lavoratori, non consentito dall'ordinamento (art. 114 del Codice, in riferimento all'art. 4, l. n. 300/1970), altresì comportando una raccolta sistematica di informazioni non necessarie e, pertanto, un'interferenza indebita nella vita privata dei lavoratori, in contrasto con il divieto per il datore di lavoro di raccogliere dati non pertinenti previsto dall'art. 113 del Codice. In tale occasione, il Garante ha altresì precisato che, in via generale, l'esigenza di assicurare anche nel caso del lavoro agile la riservatezza e la sicurezza dei dati trattati deve essere perseguita anzitutto impartendo specifiche istruzioni ai dipendenti autorizzati (artt. 4, par. 10, 29, 32 par. 4, RGPD; art. 2-*quaterdecies* del Codice), anche in considerazione delle misure tecniche e organizzative adottate per proteggere i dati, e non invece attraverso la geolocalizzazione

del personale che presta la propria attività lavorativa in modalità agile. Rilevando, altresì, che nel caso oggetto di reclamo, i dati relativi alla posizione geografica dell'interessata erano stati utilizzati a fini disciplinari, ancorché tale procedimento fosse stato poi sospeso e, più in generale, l'azienda avesse dismesso l'utilizzo di tale applicazione in autotutela, il Garante ha ravvisato la violazione degli artt. 5, 6, 13, 25, 35 e 88 del RGPD, nonché 113 del Codice. Il provvedimento in questione risulta impugnato e il giudizio di opposizione è allo stato pendente (provv. 13 marzo 2025, n. 135, doc. web n. 10128005; v. anche Newsletter 8 maggio 2025, doc. web n. 10129281).

13.3.1.2. Gestione della posta elettronica nel contesto lavorativo

Un reclamante, ex dipendente di un comune, aveva lamentato che, al momento della cessazione del rapporto di lavoro, tutti i messaggi di posta elettronica in arrivo e in uscita dalla propria casella di posta erano stati inoltrati all'indirizzo di posta elettronica della segreteria comunale e che, dopo la disattivazione della casella personale, era stato creato un indirizzo di posta virtuale (cd. alias) in apparenza corrispondente a quello personale ma in realtà associato all'indirizzo di posta elettronica della segreteria comunale, con la conseguenza che i messaggi che i mittenti avevano inviato all'indirizzo del reclamante, confidando di corrispondere con lo stesso, erano stati, in realtà, recapitati alla segreteria dell'ente. Ribadendo che anche nel contesto lavorativo pubblico e privato sussiste una legittima aspettativa di riservatezza in relazione ai messaggi oggetto di corrispondenza, costituzionalmente tutelata, il Garante, anche sulla base delle indicazioni da tempo fornite ai titolari in merito alle corrette modalità di gestione della posta elettronica al momento della cessazione del rapporto di lavoro, ha adottato un provvedimento sanzionatorio nei confronti del comune per la violazione degli artt. 5, par. 1, lett. a), 6, 12, 13 e 14 del RGPD (provv. 27 marzo 2025, n. 188, doc. web n. 10140282).

In un altro caso, un reclamante, che aveva prestato servizio come docente a contratto in favore di un ateneo, aveva lamentato che, successivamente alla cessazione dell'attività di docenza, l'ateneo aveva provveduto a resettare la password di accesso al proprio account di posta elettronica, mantenendo tuttavia attiva la relativa casella e conservando per circa due anni, senza alcuna giustificazione e senza aver adottato le necessarie scelte organizzative al riguardo, i messaggi in entrata e in uscita. Per un certo arco temporale, l'ateneo non aveva, inoltre, adottato alcuna misura per informare i mittenti dell'avvenuta cessazione dell'attività lavorativa del reclamante presso l'ateneo e della necessità di inviare ad altro indirizzo istituzionale eventuali comunicazioni afferenti all'attività di docenza già prestata. All'esito dell'istruttoria, è altresì emerso che l'ateneo non aveva fornito pieno e tempestivo riscontro a talune richieste di esercizio dei diritti di cui agli artt. 15-22 del RGPD rivoltegli dal reclamante, e aveva diffuso online sul proprio sito web istituzionale un parere reso da un proprio dipartimento ai fini dell'attribuzione dell'incarico di insegnamento al reclamante, in assenza di una disposizione della disciplina di settore che espressamente richiedesse la pubblicazione di tale atto endoprocedimentale. In ragione della ritenuta violazione degli artt. 5, par. 1, lett. a) ed e), 6, 12, parr. 3 e 4, 17 e 21 del RGPD, nonché 2-*ter* del Codice, l'ateneo è stato destinatario di un provvedimento sanzionatorio (provv. 10 luglio 2025, n. 386, doc. web n. 10162267).

13.3.1.3. Sistemi di videosorveglianza

Controllo a distanza del lavoratore

A seguito di un reclamo di un lavoratore in servizio presso il comando di polizia locale di un'unione montana, che aveva lamentato di essere stato ripreso, assieme al proprio figlio minore, da una telecamera di videosorveglianza installata presso il comando, il Garante ha accertato che tale dispositivo video, il cui raggio di ripresa comprendeva

l'ingresso e parte del parcheggio delle auto di servizio, era stato attivato senza che fossero state previamente esperite le procedure di garanzia di cui all'art. 4, comma 1, l. n. 300/1970 (accordo sindacale o autorizzazione dell'Ispettorato nazionale del lavoro), con un insufficiente livello di trasparenza del trattamento nei confronti degli interessati, nonché in assenza di una previa valutazione di impatto sulla protezione dei dati. Il comune è stato, pertanto, destinatario di un provvedimento sanzionatorio per la violazione degli artt. 5, par. 1, lett. a), 6, 12, 13, 35 e 88, par. 1, RGPD, nonché 114 del Codice (provv. 10 aprile 2025, n. 201, doc. web n. 10139433).

Asili nido

Da un'istruttoria avviata a seguito di un reclamo è emerso che un asilo aveva attivato alcune telecamere di videosorveglianza, operative anche durante l'orario in cui era offerto il servizio educativo, in aree interne ed esterne della struttura, così riprendendo non solo i bambini ma anche il personale scolastico, inclusi gli educatori, nello svolgimento della propria attività lavorativa, connotata da una peculiare dimensione, anche relazionale, con i minori affidati alle loro cure. Il Garante – nel rilevare che la normativa regionale sulla base della quale l'asilo aveva ottenuto i finanziamenti necessari all'installazione delle telecamere non poteva costituire la base giuridica del trattamento, non disciplinando lo stesso e non avendo i requisiti previsti dalla disciplina di protezione dei dati – ha evidenziato che i trattamenti posti in essere dall'asilo non potevano essere ricondotti alle finalità tassativamente indicate dalla disciplina di settore in materia di impiego di strumenti tecnologici sul luogo di lavoro (v. artt. 4 della l. n. 300/1970 e 114 del Codice); nel caso di specie si era invece concretizzato un monitoraggio diretto delle modalità con le quali il personale svolgeva l'attività lavorativa, al fine di prevenire e accertare la commissione di eventuali reati. Tali finalità, nella cornice dell'ordinamento interno, anche sul piano costituzionale, sono, infatti, attribuite in via esclusiva a specifiche autorità competenti (cfr. d.lgs. n. 51/2018), e non, invece, al datore di lavoro, che non può, pertanto, avviare siffatte iniziative all'interno della propria realtà organizzativa. Tenuto conto che l'asilo non aveva assicurato un sufficiente livello di trasparenza del trattamento nei confronti dei lavoratori e non aveva svolto una preventiva valutazione di impatto sulla protezione dei dati, il Garante ha adottato un provvedimento prescrittivo e sanzionatorio per la violazione, tra gli altri, degli artt. artt. 5, par. 1, lett. a), 6, 7, 12, par. 1, 13 e 35 del RGPD e 2-*ter* del Codice (provv. 10 luglio 2025, n. 410, doc. web n. 10162731; v. anche Newsletter 10 settembre 2025, doc. web n. 10163470; cfr. parr.4.3. e 4.7).

Sicurezza urbana e controllo a distanza

In un altro caso, anch'esso originato da un reclamo, è emerso che un comune, a seguito di alcune segnalazioni, aveva utilizzato i filmati estratti da una telecamera di videosorveglianza, installata sulla pubblica via per la tutela della cd. sicurezza urbana e inquadrante anche l'accesso alla sede comunale, per raccogliere elementi probatori a supporto di contestazioni disciplinari poi effettivamente mosse nei confronti della reclamante. L'ente aveva, pertanto, trattato i dati personali dell'interessata per una finalità (disciplinare) incompatibile con quella originaria (sicurezza urbana), non avendo lo stesso assicurato il rispetto delle garanzie previste dagli artt. 4, comma 1, l. n. 300/1970 e 114 del Codice (accordo sindacale o autorizzazione dell'Ispettorato nazionale del lavoro). Il Garante ha ricordato che tali disposizioni tutelano la persona che lavora non solo quando i dispositivi di sorveglianza sono posti all'interno dei luoghi di lavoro – essendo irrilevante la circostanza che l'accesso a detti locali da parte dei lavoratori avvenga in maniera discontinua e per brevi archi temporali – ma anche nel caso in cui sono sottoposte a videosorveglianza aree esterne o perimetrali in cui comunque transitano i lavoratori. Nel caso di specie la reclamante, mentre era assente dal servizio per malattia e si trovava in luoghi pubblici con alcune colleghe, era stata ripresa da un collaboratore comunale, incaricato di acquisire tramite uno smartphone elementi probatori per

muovere contestazioni disciplinari nei suoi confronti. Il Garante, nel rilevare che tale attività investigativa era stata posta in essere in assenza delle necessarie condizioni di liceità, ha rammentato che al datore di lavoro è fatto divieto di trattare informazioni che non siano rilevanti ai fini della gestione del rapporto di lavoro, attesi i rischi di discriminazione ordinariamente connessi a tali trattamenti, e che sussiste una specifica disciplina di settore che regola le modalità con cui il dipendente può fruire dell'assenza per motivi di salute e i flussi informatici di cui il datore di lavoro è destinatario. Peraltro, nel caso di specie, come affermato dall'autorità giudiziaria in sede penale in merito ai fatti occorsi, la condizione di malattia attestata dai certificati prodotti dall'interessata non imponeva il ricovero o il confinamento della lavoratrice presso la propria abitazione. Ritenuti complessivamente violati gli artt. 5, par. 1, lett. a) e b), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 35 e 88 del RGPD, nonché 2-*ter*, 113 e 114 del Codice, l'Autorità ha adottato un provvedimento sanzionatorio nei confronti dell'ente (provv. 23 novembre 2025, n. 628, doc. web n. 10196164; cfr. par. 4.11).

13.3.2. Trattamento di dati per finalità di instaurazione e gestione del rapporto di lavoro

Sulla base di istruttorie avviate a seguito di reclami presentati da dipendenti o da altri interessati che prestano la propria attività lavorativa presso soggetti pubblici e enti che perseguono finalità di interesse pubblico, è stata accertata l'illiceità di taluni trattamenti svolti per finalità connesse all'istaurazione del rapporto di lavoro, nell'ambito di procedure concorsuali o selettive, e, più in generale, nel contesto della gestione del rapporto stesso.

13.3.2.1. Trattamento di dati nell'ambito di procedure concorsuali

A seguito di un reclamo il Garante ha accertato l'avvenuta pubblicazione, sul sito web istituzionale di un ente regionale, dei verbali della commissione di una selezione pubblica contenenti i dati personali del reclamante e degli altri partecipanti alla selezione, tra cui le dichiarazioni relative all'esistenza di procedimenti penali in corso. Tali verbali sono risultati anche indicizzati sui motori di ricerca.

A seguito dell'istanza di esercizio dei diritti del reclamante l'ente aveva dato immediatamente seguito alla richiesta di cancellazione di tali informazioni; tuttavia, l'Autorità, rilevando l'assenza di un'idonea base giuridica del trattamento in questione in quanto la normativa di riferimento non prevede la pubblicazione degli atti interni alla procedura, quali in particolare i verbali redatti dalle commissioni esaminatrici e contenenti i dati personali dei candidati, ha comminato una sanzione amministrativa pecuniaria per violazione degli artt. artt. 5, par. 1, lett. a), 6, 10, RGPD, nonché 2-*ter* e 2-*octies* del Codice (provv. 11 settembre 2025, n. 482, doc. web n. 10176998).

In un altro caso il reclamante aveva richiesto la cancellazione di propri dati personali, tra cui indirizzi privati e numeri di telefono contenuti in una graduatoria pubblicata sul sito web di un istituto scolastico, lamentando di aver esercitato i diritti di cui agli artt. da 15 a 22 del RGPD nei confronti dell'istituto e di non avere ricevuto un idoneo riscontro.

Dall'istruttoria è emerso che seppure l'istituto scolastico avesse fornito riscontro all'istanza di esercizio dei diritti del reclamante rimuovendo la graduatoria dal proprio sito web istituzionale, la stessa era risultata ancora raggiungibile su un diverso sito web estraneo all'istituto.

Per tali ragioni il Garante ha adottato un provvedimento sanzionatorio nei confronti dell'istituto, anche tenuto conto dell'arco temporale in cui la predetta graduatoria era rimasta pubblicata e ha ribadito che la diffusione online costituisce un trattamento particolarmente invasivo poiché consente a chiunque, per effetto dei comuni motori di ricerca esterni ai siti, di reperire indiscriminatamente e in tempo reale un insieme

consistente di informazioni personali che rischiano di rimanere in rete per un tempo indefinito, come nel caso di specie. Il Garante ha pertanto comminato una sanzione amministrativa pecuniaria all'istituto rilevando la violazione degli artt. artt. 5, par. 1, lett. a) e c), 6, par.1, lett. c) ed e), RGPD, nonché 2-*ter* del Codice (provv. 4 dicembre 2025, n. 731, doc. web n. 10209827).

In un altro caso l'Autorità si è espressa sulla pubblicazione da parte di un comune, sul proprio sito web istituzionale, sia della graduatoria intermedia della prova scritta, contenente i nominativi dei candidati ammessi e non ammessi alla prova orale e la relativa votazione, sia della graduatoria finale di merito, contenente non solo il nominativo del candidato risultato vincitore ma anche quello dei candidati idonei e non idonei, con l'indicazione, in corrispondenza del nominativo di ciascuno, del dettaglio delle votazioni conseguite nell'ambito di ciascuna prova concorsuale (votazione scritta, orale e complessiva) nonché, con riguardo a due interessati, dell'indicazione della mancata presentazione alla prova orale. Sotto diverso ma connesso profilo, con riferimento a quanto lamentato dall'interessata nel reclamo, il Garante ha accertato, altresì, la pubblicazione da parte del comune di alcune determinazioni, nella sezione albo pretorio online, contenenti dati personali della reclamante e dettagli in merito a vicende connesse al rapporto di lavoro intercorso con il comune, con particolare riguardo alle circostanze che avevano determinato la cessazione del predetto rapporto, inizialmente indicate come derivanti dal mancato superamento del periodo di prova. Inoltre, nell'ambito dell'istruttoria è emerso che il comune non aveva provveduto a fornire idoneo riscontro alla richiesta di esercizio del diritto di rettifica avanzata dall'interessata. Pertanto il Garante ha adottato un provvedimento sanzionatorio nei confronti del comune per aver, da un lato, diffuso i dati personali della reclamante in relazione alla risoluzione del rapporto di lavoro e omesso di fornire idoneo riscontro alla richiesta di esercizio del diritto di rettifica e, dall'altro, diffuso le graduatorie – anche di natura intermedia, inerenti alla fase selettiva – del concorso pubblico a cui aveva partecipato la reclamante stessa, per la violazione degli artt. 5, 6, 12 e 16 del RGPD, nonché 2-*ter* del Codice (provv. 11 settembre 2025, n. 484, doc. web n. 10183000).

Facendo leva sui compiti di promozione della consapevolezza e della comprensione dei titolari e dei responsabili del trattamento e a sicuro beneficio anche degli stessi interessati, l'Autorità ha adottato specifiche FAQ, condivise con il Dipartimento della funzione pubblica, in materia di pubblicità e trasparenza nel trattamento dei dati personali connesso alle procedure concorsuali e selettive. L'occasione è stata offerta dal recente intervento del legislatore, che si è concretizzato con il d.l. 14 marzo 2025, n. 25, convertito in l. 9 maggio 2025, n. 69 recante disposizioni urgenti in materia di reclutamento e funzionalità delle pubbliche amministrazioni e che ha assicurato il coordinamento con la disciplina di protezione dei dati nonché con le preesistenti disposizioni che regolano le forme di pubblicità e trasparenza della p.a. (cfr. l. n. 241/1990; d.lgs. n. 33/2013), sciogliendo taluni principali nodi interpretativi e applicativi. Le predette FAQ offrono una ricostruzione sistematica delle disposizioni applicabili in tale specifico ambito, stratificatesi nel tempo, anche alla luce dei consolidati orientamenti del Garante, in relazione sia alla pubblicazione online delle sole graduatorie finali sia alle varie forme di comunicazione previste a livello endoprocedimentale in favore dei soli partecipanti alle procedure, e rappresentano un utile strumento operativo per la p.a. finalizzato ad orientare in concreto le valutazioni e le scelte nel contesto in questione, nella prospettiva di assicurare trattamenti di dati conformi alle nuove disposizioni normative del d.lgs. n. 165/2001 e ai principi di protezione dei dati (FAQ in materia di trattamento di dati personali dei partecipanti

alle procedure concorsuali per finalità di pubblicità e trasparenza alla luce delle recenti disposizioni normative, doc. web n. 10187304).

13.3.2.2. Comunicazione di dati personali a terzi nei contesti lavorativi e mancato rispetto del principio di limitazione della finalità

Con un reclamo presentato da un dipendente di un ministero, era stato lamentato che, nel fornire riscontro a tre specifiche e separate istanze relative ad un ricollocamento interno e formulate da tre dipendenti, tra i quali anche il reclamante, l'ufficio competente aveva trasmesso un'unica nota, recante in intestazione il nominativo di tutti e tre i predetti individui, in tal modo rendendo ciascuno di essi reciprocamente edotto della circostanza che ciascuno dei destinatari aveva presentato tale istanza e che, peraltro, la stessa era stata rigettata. Nel ricordare che, in tali casi, il datore di lavoro deve ricorrere a forme di comunicazione individualizzate, il Garante, ha preso atto che nel caso di specie l'omessa adozione di accorgimenti intesi ad oscurare il nominativo dei destinatari della nota aveva comportato una comunicazione di dati personali in violazione degli artt. 5, par. 1, lett. a), e 6 del RGPD e 2-*ter* del Codice ed ha pertanto ammonito il ministero (provv. 16 gennaio 2025, n. 4, doc. web n. 10110716).

Dati sulla salute

In un altro caso, una dipendente di un ministero aveva lamentato il trattamento di dati idonei a rivelare informazioni di dettaglio sul proprio stato di salute, che la stessa aveva trasmesso agli uffici ministeriali al solo scopo di comprovare il proprio impedimento fisico per il differimento della data dell'audizione nell'ambito di un procedimento disciplinare a suo carico. In particolare, la reclamante aveva lamentato che, una volta acquisite, tali informazioni erano state utilizzate dal ministero per avviare un distinto procedimento relativo all'accertamento della sua inidoneità psicofisica al servizio ai sensi del d.P.R. n. 171/2011. In tal caso, il Garante, precisando come il ministero avrebbe dovuto astenersi dall'utilizzare ulteriormente le predette informazioni per scopi diversi e ulteriori rispetto a quello che aveva contrassegnato l'iniziativa intrapresa dall'interessata nell'ambito del procedimento disciplinare, ha accertato la violazione degli artt. 5, par. 1, lett. a), 6 e 9, par. 2, lett. b) e g), RGPD e 2-*ter* e 2-*sexies* del Codice ed ammonito il titolare del trattamento (provv. 30 gennaio 2025, n. 34, doc. web n. 10112637).

A seguito di un reclamo, il Garante ha accertato che un comune, in persona dell'allora comandante della polizia locale, nel dar seguito a una segnalazione di un reclamante, in servizio presso il Comando, relativa a possibili criticità in materia di sicurezza del lavoro, aveva indirizzato la propria nota di riscontro al sindaco, al segretario generale del comune e a un assessore, disponendo anche l'affissione della stessa in una bacheca collocata all'interno del comando, affinché potesse essere conosciuta da tutto il personale ivi in servizio. In tale nota si era dato conto di informazioni personali del reclamante, anche relative allo stato di salute, così rivelando dati inconferenti e ultronei rispetto alla questione oggetto di segnalazione, la cui trattazione all'interno dell'organizzazione del titolare non richiedeva in ogni caso il disvelamento dell'identità del segnalante. Ravvisata la violazione degli artt. 5, par. 1, lett. a), 6 e 9, par. 2, lett. b), RGPD, nonché 2-*ter* del Codice, il Garante ha adottato un provvedimento sanzionatorio nei confronti dell'ente (provv. 27 febbraio 2025, n. 101, doc. web n. 10123227).

In un altro caso, il reclamante, quale membro del collegio dei revisori dei conti di un ente nazionale di ricerca, controllo e consulenza tecnico-scientifica in materia di sanità pubblica, aveva partecipato a una riunione tenutasi presso l'ente nel periodo dell'emergenza pandemica da SARS-CoV-2, venendo in contatto con una persona poi risultata positiva al virus ed essendo successivamente coinvolto nell'attività di tracciamento dei contagi da parte del Responsabile del servizio di prevenzione e protezione (RSPP) dell'ente. In tale contesto, è emerso che l'ente aveva comunicato a due altri componenti del collegio, in assenza di base

giuridica, dati personali del reclamante relativi alla pratica assicurativa attivata a seguito del predetto contatto e alla corrispondenza con l'ente e il RSPP in relazione ai fatti occorsi nella citata riunione; l'ente non aveva, inoltre, reso edotto il reclamante dei dati di contatto del proprio RPD e aveva negato all'interessato il diritto d'accesso ai propri dati personali, sulla base di un riscontro inidoneo a giustificare il diniego stesso, in violazione degli artt. 5, par. 1, lett. a), 6, parr. 1, lett. c) ed e), e 2 e 3, 13, par. 1, lett. b), e 15 del RGPD, nonché 2-*ter* del Codice. Tenuto conto di tutte le circostanze del caso, il Garante ha ritenuto sufficiente ammonire il titolare del trattamento (provv. 4 dicembre 2025, n. 734, doc. web n. 10210784).

Con altro reclamo, un dipendente di un'azienda sanitaria aveva lamentato l'inoltro, da parte del coordinatore della struttura di appartenenza ai sedici componenti dell'equipe ove lo stesso prestava servizio, di un messaggio di posta elettronica, in forma integrale, con il quale l'interessato aveva comunicato al coordinatore stesso e, per conoscenza, ad un collega, che avrebbe usufruito di un permesso per l'espletamento di una specifica visita medica. Pur prendendo atto che la comunicazione era avvenuta per mero errore materiale e che l'azienda aveva assunto in tale contesto apprezzabili iniziative per prevenire il ripetersi di simili eventi, il Garante ha ammonito il titolare, ravvisando la violazione degli artt. 5, par. 1, lett. a), 6 e 9 del RGPD, nonché 2-*ter* del Codice (provv. 18 dicembre 2025, n. 753, doc. web n. 10210247).

Con reclamo è stato rappresentato che un'azienda sanitaria aveva caricato, tramite protocollo informatico, il provvedimento conclusivo del procedimento disciplinare nei confronti del reclamante, seppure non in forma integrale, rendendo il documento in tal modo visibile anche ad altro personale operante in diversi uffici e unità organizzative e non specificamente autorizzati a trattare le informazioni ivi contenute. In tale caso il Garante ha comminato una sanzione amministrativa pecuniaria rilevando la violazione degli artt. 5 e 6 del RGPD, nonché 2-*ter* del Codice (provv. 13 febbraio 2025, n. 70, doc. web n. 10118395).

In un altro caso, un dipendente di un istituto scolastico aveva lamentato l'iniziale acquisizione al protocollo informatico ordinario del ricorso dallo stesso presentato per la rettifica del periodo di comporto riconducibile a gravi patologie contenente, in particolare, dati relativi alla salute nonché dati concernenti la controversia di lavoro intercorsa. La predetta acquisizione al protocollo ordinario aveva reso in tal modo visibile il ricorso e i relativi allegati anche ad altro personale operante sia nella medesima unità organizzativa del reclamante sia in altri uffici, sebbene non specificamente autorizzato a trattare le informazioni ivi contenute. In tale contesto, il Garante ha ribadito la necessità da parte del datore di lavoro di adottare adeguate misure tecniche e organizzative per assicurare l'accesso selettivo alla documentazione presente nel protocollo informatico, al fine di evitare la consultabilità di documenti da parte di personale non autorizzato e prevenire pertanto ogni occasione di superflua e ingiustificata conoscibilità dei dati personali dei dipendenti ivi contenuti, soprattutto quando siano relativi allo stato di salute o ad altri dati relativi allo specifico rapporto di lavoro. In aggiunta, l'Autorità ha accertato ulteriori violazioni da parte dell'istituto scolastico, quali la tardiva informazione ai dipendenti in merito al trattamento dei propri dati personali nel contesto di lavoro nonché le tardive istruzioni agli stessi in qualità di soggetti autorizzati al trattamento. Il Garante ha pertanto comminato una sanzione amministrativa pecuniaria rilevando la violazione degli artt. 5, par. 1, lett. a), 6, 9, par. 2, lett. b) e g), 13 e 29 del RGPD nonché artt. 2-*ter*, 2-*sexies* e 2-*quaterdecies* del Codice (provv. 4 dicembre 2025, n. 733, doc. web n. 10212783).

All'Autorità è, inoltre, pervenuto un reclamo con il quale era stato lamentato che, nell'ambito di una procedura selettiva, nel quadro di pur meritevoli iniziative volte a contrastare il rischio dell'abbandono scolastico, un liceo avesse trasmesso i curriculum

Abbandono scolastico

dei quattro docenti che avevano presentato la propria candidatura – ivi inclusa la reclamante – a quarantaquattro famiglie di studenti, individuati come soggetti a rischio di abbandono scolastico, affinché ciascuna di esse potesse prenderne visione ed esprimere conseguentemente la propria preferenza in ordine al docente da affiancare allo studente. Prescindendo dalla eventuale qualificazione del predetto avviso di selezione come atto amministrativo generale, menzionato dall'art. 2-*ter* del Codice quale fonte astrattamente idonea a legittimare un trattamento di dati personali, il Garante ha evidenziato al riguardo che l'avviso di selezione non poteva contravvenire né modificare o innovare le norme sovraordinate di riferimento, dispiegando un mero effetto integrativo dell'ordinamento, tenuto conto, in particolare, dell'art. 70, comma 13, d.lgs. n. 165/2001, secondo cui, in materia di reclutamento del personale, le pubbliche amministrazioni sono tenute a rispettare le disposizioni nazionali che regolano l'accesso al pubblico impiego nonché lo svolgimento di incarichi nel contesto pubblico, regolando la materia in coerenza con i principi ivi previsti. Ciò risulta necessario anche nella prospettiva della certezza del diritto e del principio di non discriminazione, non essendo consentiti livelli differenziati di tutela della protezione dei dati personali tra le singole amministrazioni e, in particolare, tra le singole istituzioni scolastiche sul territorio nazionale. All'esito dell'attività istruttoria, l'Autorità ha quindi comminato al liceo una sanzione amministrativa pecuniaria, rilevando la violazione degli artt. 5, par. 1, lett. a) e c), e 6 del RGPD e 2-*ter* del Codice (provv. 9 ottobre 2025, n. 584, doc. web n. 10197090).

Formazione

Con un reclamo era stato lamentato l'invio, da parte degli uffici amministrativi di un ministero, di una comunicazione a mezzo e-mail al fine di sollecitare i destinatari – oltre venti dipendenti – ad effettuare i percorsi formativi previsti sulla piattaforma Syllabus, corredando tale comunicazione di un file riepilogativo recante, per ciascuno dei predetti dipendenti, l'indicazione del numero e dei titoli dei test mancanti e in tal modo rendendo ciascuno di tali soggetti reciprocamente edotti di queste circostanze. A tal riguardo, l'Autorità ha ricordato che devono essere impiegate modalità di trasmissione delle comunicazioni nonché selezionate le informazioni ivi contenute affinché ne siano garantiti la ricezione e il conseguente trattamento da parte del solo personale autorizzato, evitando ogni forma di superflua circolazione di informazioni riguardanti i dipendenti nel contesto lavorativo. Per tali ragioni, il Garante ha ammonito il ministero, rilevando la violazione degli artt. 5, par. 1, lett. a) e c) e 6 del RGPD e 2-*ter* del Codice (provv. 9 ottobre 2025, n. 582, doc. web n. 10191660).

Istanza di trasferimento

In un altro caso, con reclamo presentato da un magistrato in servizio presso una corte di giustizia tributaria, era stato lamentato, tra l'altro, che, nell'ambito di una procedura avviata sulla base di un'istanza di trasferimento avanzata dallo stesso reclamante, era stato fatto esplicito riferimento al nominativo dell'interessato e alle proprie condizioni personali, tanto nell'interpello rivolto ai magistrati della corte quanto nel decreto che aveva infine disposto il trasferimento. Al riguardo, il Garante, evidenziando come tali informazioni evocassero comunque la presenza di possibili vicende problematiche o delicate nell'ambito della sfera personale o della vita privata o familiare dell'interessato, ha rilevato che tale trattamento era avvenuto in assenza di adeguate motivazioni a sostegno della conoscibilità dei dati da parte della generalità dei magistrati della corte, potendo la finalità perseguita essere ugualmente soddisfatta senza ricorrere all'esplicitazione dei dettagli sopra indicati. Nell'ammonire il titolare del trattamento, è stata quindi accertata in tal caso la violazione degli artt. 5, par. 1, lett. a) e c) e 6 del RGPD e 2-*ter* del Codice. Il provvedimento in questione risulta impugnato e il giudizio di opposizione è allo stato pendente (provv. 27 novembre 2025, n. 702, doc. web n. 10209810).

In un altro caso, a fronte di un reclamo, il Garante è intervenuto sul trattamento di dati personali effettuato, in occasione del riscontro ad un sollecito di pagamento, da un

comune che aveva inviato una comunicazione, oltre che alla stessa interessata che aveva formulato il sollecito, anche all'indirizzo PEC dell'amministrazione presso cui essa risultava all'epoca dei fatti in comando, facendo ivi riferimento ad una pregressa segnalazione trasmessa ad ANAC in ordine all'operato assunto dalla reclamante in tale specifico contesto. Non ravvisando specifici presupposti giuridici o ragioni che potessero giustificare l'invio del riscontro, da parte del comune, anche ad un indirizzo diverso da quello utilizzato nel caso di specie dalla reclamante all'atto dell'invio dell'istanza, il Garante ha ammonito il comune sul presupposto della violazione degli artt. 5, par. 1, lett. a) e 6 del RGPD e 2-*ter* del Codice (provv. 27 novembre 2025, n. 703, doc. web n. 10210489).

13.3.2.3. Trattamento di dati personali relativi alla vaccinazione dei dipendenti

Alcuni reclami hanno riguardato il trattamento illecito di dati personali con riferimento alle informazioni riguardanti il possesso del requisito vaccinale anti SARS-CoV-2, previsto dall'art. 4, d.l. n. 44/2021 ovvero comunicazioni di dati personali non conformi ai principi di liceità, correttezza e trasparenza, e in assenza di una base giuridica.

In un caso un'azienda ospedaliera aveva inviato alla casella di posta elettronica dell'ufficio del RPD, a cui accedevano oltre al RPD la reclamante e un altro dipendente, informazioni sullo stato vaccinale della reclamante e sulla sospensione dal servizio dell'altro dipendente, a causa della mancata vaccinazione, rendendoli, in tal modo, vicendevolmente edotti dello stato vaccinale di ciascuno. Il Garante ha comminato una sanzione amministrativa pecuniaria per la violazione degli artt. 5, 6 e 9 del RGPD, nonché 2-*ter* e 2-*sexies* del Codice (provv. 30 gennaio 2025, n. 35, doc. web n. 10111962).

Analogamente un'azienda sanitaria aveva creato e conservato una cartella di rete condivisa contenente l'elenco dei lavoratori, tra cui l'interessato, con l'indicazione dello stato vaccinale di ciascuno. L'accessibilità alla predetta cartella aveva comportato la conoscibilità delle informazioni relative allo stato vaccinale del personale da parte di tutti i dipendenti abilitati, rendendo di fatto ciascuno di essi edotto circa l'avvenuta o mancata vaccinazione degli altri colleghi. In tal caso il Garante ha comminato una sanzione amministrativa pecuniaria per la violazione degli artt. 5, 6 e 9 del RGPD, nonché 2-*ter* e 2-*sexies* del Codice (provv. 30 gennaio 2025, n. 36, doc. web n. 10112750).

Con reclamo è stato rappresentato che un ente aveva e notificato contestualmente a tre dipendenti una delibera a mezzo della quale era stata confermata la sospensione dal servizio degli stessi per effetto della accertata carenza del requisito professionale della vaccinazione anti SARS-CoV-2, avendoli resi, in tal modo, vicendevolmente edotti di informazioni di carattere personale particolarmente delicate ed avendo dato pertanto corso a una comunicazione di dati personali in violazione degli artt. 5 e 6 del RGPD, nonché 2-*ter* del Codice. Il provvedimento in questione risulta impugnato e il giudizio di opposizione è allo stato pendente (provv. 27 febbraio 2025, n. 92, doc. web n. 10114763).

In un altro caso il Garante ha accertato che un ministero, nell'ambito degli adempimenti finalizzati alla verifica degli obblighi vaccinali del personale in servizio, aveva creato un "foglio di lavoro" concernente diverse informazioni su alcuni lavoratori anche con riferimento a dati relativi alla salute degli stessi. In particolare è emerso che, oltre al nome e al cognome di ciascun interessato, erano stati indicati la data della raccomandata di sollecito per regolarizzare l'obbligo vaccinale, il numero di dosi effettuate da ciascuno, nonché specifiche ulteriori annotazioni di dettaglio. Il predetto "foglio di lavoro", inoltre, era stato pubblicato, seppure per alcuni minuti, sul canale social utilizzato per comunicazioni di servizio mettendo, in tal modo, a disposizione dei lavoratori che avevano accesso al canale social tali delicate informazioni. Per tali ragioni il Garante ha comminato una sanzione amministrativa pecuniaria al ministero, rilevando la violazione degli artt. 5, 6 e 9 del RGPD, nonché 2-*ter* e 2-*sexies* del Codice (provv. 11 settembre 2025, n. 485, doc. web n. 10183218).

13.3.2.4. Esercizio dei diritti degli interessati

Il Garante ha adottato un provvedimento di ammonimento nei confronti di un ateneo in ragione dell'intempestivo riscontro a un'istanza di esercizi dei diritti di accesso ai dati personali, opposizione al trattamento e cancellazione dei dati, rivoltagli da un partecipante a una procedura concorsuale, in violazione di quanto previsto dall'art. 12, parr. 3 e 4, RGPD (provv. 13 febbraio 2025, n. 67, doc. web n. 10114359).

13.3.3. 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 (cfr. par. 4.4.2), peraltro in molti casi indicizzate sui motori di ricerca.

Albo pretorio

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 da parte dei comuni sul proprio sito web istituzionale di:

- delibere contenenti dati personali dell'interessato, seppure indirettamente individuato, riguardanti informazioni su un procedimento penale per reati contro la p.a. Inoltre era emerso che il comune non aveva dato riscontro a una richiesta di esercizio dei diritti dell'interessato. Per tali ragioni il Garante ha comminato al comune una sanzione amministrativa pecuniaria, rilevando la violazione degli artt. 5, par. 1, lett. a) 6 e 10 e degli artt. 12, par. 3 e 4 e 17 del RGPD, nonché degli artt. 2-*ter* e 2-*octies* del Codice (provv. 25 settembre 2025, n. 530, doc. web n. 10184967);
- decreti, nella sezione albo pretorio online, contenenti i dati personali del reclamante riguardanti informazioni relative al rapporto di lavoro dello stesso con il comune, tra cui la presa d'atto delle proprie dimissioni. In tal caso il Garante ha comminato al comune una sanzione amministrativa pecuniaria, rilevando la violazione degli artt. 5, par. 1, lett. a) e c) e 6 del RGPD, nonché dell'art. 2-*ter*, commi 1 e 3 del Codice (provv. 17 luglio 2025, n. 423, doc. web n. 10181686);
- deliberazioni, nella sezione albo pretorio online, contenenti dati personali del reclamante con riferimenti a vicende personali e comunque connesse allo specifico rapporto di lavoro dell'interessato. Inoltre, nell'ambito dell'istruttoria è emerso che il comune non aveva fornito il dovuto riscontro a una richiesta di esercizio dei diritti dell'interessato. Pertanto il Garante ha comminato una sanzione amministrativa pecuniaria per la violazione degli artt. 5, 6 e 12 del RGPD, nonché 2-*ter* del Codice (provv. 13 marzo 2025, n. 133 doc. web n. 10127776);
- atti e documenti contenenti informazioni riguardanti vicende personali e comunque connesse allo specifico rapporto di lavoro con il reclamante, in particolare anche dati relativi alla salute, quali la percentuale di invalidità riconosciuta al reclamante e il riferimento alla fruizione del congedo straordinario retribuito. Per tali ragioni il Garante ha comminato una sanzione amministrativa pecuniaria per la violazione degli artt. 5, 6 e 9 del RGPD e dell'art. 2-*ter* e 2-*septies*, comma 8 del Codice (provv. 4 giugno 2025, n. 320, doc. web n. 10163025);
- deliberazioni di approvazione del piano sulle *performance* riguardante le valutazioni individuali di singoli dipendenti ai fini dell'attribuzione dei relativi emolumenti, con riferimento a singole annualità. Ai documenti era altresì allegato l'elenco dei nominativi dei dipendenti con l'indicazione del punteggio attribuito a ciascuno di essi all'esito della valutazione. In tale caso è stata comminata una sanzione amministrativa pecuniaria rilevando la violazione degli artt. 5 e 6 del RGPD, nonché 2-*ter* del Codice (provv. 10 aprile 2025, n. 204, doc. web n. 10140369).

13.3.4. Dati personali di lavoratori in banche dati pubbliche

Portale nazionale del sommerso

Successivamente all'emanazione del decreto del Ministro del lavoro e delle politiche sociali 20 novembre 2024, n. 170, concernente la creazione, presso l'INL, del Portale nazionale del sommerso (PNS) – ove confluiscono le risultanze dell'attività di vigilanza in materia da parte di INL, INPS, INAIL, Arma dei Carabinieri e Guardia di finanza – che, nel recepire le osservazioni formulate dal Garante, rinviava a un successivo decreto dello stesso ministero, da adottarsi ai sensi dell'art. 10, comma 1-*ter*, d.lgs. 23 aprile 2004, n. 124, l'indicazione degli elementi essenziali del trattamento dei dati personali (cfr. Relazione 2024, p. 161), è stato trasmesso lo schema di decreto in questione, su cui il Garante si è pronunciato con parere favorevole, essendo state recepite le osservazioni fornite nel corso di serrate interlocuzioni informali che hanno riguardato, tra l'altro: i ruoli di titolari del trattamento assunti dai soggetti a vario titolo coinvolti; l'adozione di specifiche garanzie per i diritti e le libertà degli interessati con riferimento al trattamento di dati personali relativi a condanne penali e reati eventualmente presenti nel PNS nell'ambito delle istruttorie conseguenti agli accertamenti ispettivi; la messa in consultazione, tramite il PNS, delle informazioni relative alle generalità delle persone denuncianti, solo successivamente all'adozione di specifiche misure di sicurezza aggiuntive da definire con i soggetti cooperanti; la definizione dei tempi di conservazione dei dati trattati nell'ambito del PNS e delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato ai rischi, da impartire anche ai soggetti cooperanti con riferimento ai propri sistemi che si interfacciano con il PNS. L'Autorità ha altresì evidenziato come eventuali modifiche e integrazioni al decreto che incidano sugli aspetti essenziali del trattamento dei dati personali dovranno essere disciplinate all'interno di un atto-fonte che abbia lo stesso rango, previa consultazione del Garante, ferma restando la possibilità di regolare taluni aspetti di dettaglio anche mediante che protocolli d'intesa tra le parti (provv. 29 aprile 2025, n. 255, doc. web n. 10129880).

Lavoratori esposti a radiazioni ionizzanti

Il d.lgs. n. 101/2020 recante attuazione della direttiva 2013/59/EURATOM, che stabilisce norme fondamentali di sicurezza relative alla protezione contro i pericoli derivanti dall'esposizione alle radiazioni ionizzanti, e riordino della normativa di settore in attuazione dell'art. 20, comma 1, lett. a), l. n. 117/2019 ha previsto l'istituzione, presso il Ministero del lavoro e delle politiche sociali, dell'Archivio nazionale dei lavoratori esposti alle radiazioni ionizzanti.

Il Garante, in attuazione dell'art. 126 del predetto decreto legislativo, ha reso parere favorevole sullo schema di decreto del Ministero del lavoro e delle politiche sociali e relativo allegato, al fine di stabilire le modalità e i criteri di costituzione, alimentazione e gestione del predetto Archivio nonché le modalità di accesso da parte dell'Ispettorato nazionale per la sicurezza nucleare e la radioprotezione (ISIN), delle altre autorità di vigilanza e delle amministrazioni dello Stato interessate per le specifiche finalità istituzionali. Il parere è stato preceduto da numerose interlocuzioni finalizzate a far sì che nei trattamenti fosse assicurata la puntuale individuazione di tutti i soggetti pubblici e privati che alimentano e/o accedono all'Archivio in considerazione del ruolo assunto da tali soggetti e in relazione alla specifica finalità perseguita da ciascuno, nonché la trasparenza nei confronti degli interessati e una chiara ripartizione degli obblighi e delle responsabilità previste dal RGPD, anche con riferimento al ruolo assunto da eventuali soggetti terzi delegati alla realizzazione e gestione dell'Archivio. Il Garante ha evidenziato in proposito che i trattamenti effettuati attraverso l'Archivio si collocano in uno scenario particolarmente complesso e delicato, nell'ambito del quale i lavoratori, in ragione delle mansioni assegnate e dei compiti in concreto svolti, risultano esposti a gravi rischi per la propria salute; tale circostanza giustifica, peraltro, la previsione a carico del datore di lavoro di ulteriori e più specifici obblighi, che possono comportare altresì, al ricorrere

delle condizioni previste dalla legge, il trattamento di informazioni di natura sensibile normalmente sottratte alla sfera di conoscibilità riservata dall'ordinamento al datore di lavoro. In particolare le indicazioni fornite dal Garante sono state volte ad assicurare: la puntuale individuazione delle tipologie di dati personali acquisiti nonché le misure volte ad assicurare il trattamento dei soli dati esatti e aggiornati; la corretta individuazione dei tempi di conservazione delle diverse tipologie dei dati personali; le garanzie di non identificabilità degli interessati, nell'ambito delle attività di sorveglianza sanitaria, di vigilanza, di assicurazione sul lavoro, di ricerca, sperimentazione e controllo e di sicurezza nucleare e radioprotezione da parte di ciascun ente a ciò preposto; le garanzie di anonimizzazione dei dati personali dei lavoratori alla cessazione del termine di conservazione dei dati stessi; l'individuazione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato ai rischi (parere 18 dicembre 2025, n. 790, doc. web n. 10213930).

13.3.5. Trattamento di dati nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti (whistleblowing)

Nel 2025, il Garante, in continuità con gli orientamenti già assunti in materia, ha espresso parere su due proposte di delibera dell'ANAC relative al whistleblowing (la prima riguardante l'approvazione delle linee guida per le segnalazioni interne; la seconda relativa all'aggiornamento delle linee guida per le segnalazioni esterne), con l'obiettivo di rendere la gestione delle segnalazioni, sia interne che esterne, più uniforme ed efficace, di assicurare la piena tutela della riservatezza dell'identità del segnalante e del contenuto della segnalazione, nonché la tutela dei dati delle persone a vario titolo coinvolte. Tra i punti di attenzione evidenziati nel parere vi sono stati, in particolare, i possibili rischi derivanti dall'utilizzo della posta elettronica come canale di segnalazione; la necessità di una previa valutazione di impatto sulla protezione dei dati, anche con l'eventuale supporto dei fornitori di tecnologia; i tempi di conservazione della segnalazione e della relativa documentazione; la possibilità, in talune circostanze, di condividere il canale di segnalazione, ferma restando la necessità di adottare misure tecniche e organizzative per garantire che ciascun ente abbia accesso solo alle segnalazioni di propria competenza; linee guida sui canali interni di segnalazione che forniscano indicazioni e princìpi ai datori di lavoro sull'attivazione dei propri canali di acquisizione e gestione della segnalazione. In tale contesto si è posta particolare attenzione alle misure tecniche e organizzative che, nel rispetto del principio di responsabilizzazione, i datori di lavoro pubblici e privati, e gli altri soggetti obbligati, potranno adottare per proteggere i dati delle persone nel corso del processo di acquisizione e gestione della segnalazione, come, ad esempio, accorgimenti per impedire la tracciabilità della persona segnalante che acceda ai canali interni di segnalazione dalla rete dati interna all'organizzazione del datore di lavoro (provv. 9 ottobre 2025, n. 581, doc. web n. 10184673; v. anche Newsletter 27 novembre 2025, doc. web n. 10193417).

14 Le attività economiche

14.1. *Trattamento di dati personali in ambito assicurativo*

Il settore assicurativo, ancora nel 2025, è stato oggetto di un elevato numero di segnalazioni e reclami riguardanti, per lo più, l'esercizio del diritto di accesso ai dati personali trattati dalle compagnie assicurative; in più occasioni l'Autorità ha, tuttavia, dovuto ribadire la differenza tra il diritto di accesso ai dati personali previsto dall'art. 15 del RGPD e il diritto di accesso ad atti e documenti riconosciuto da altre normative di settore, tra cui, in particolare, l'art. 146, d.lgs. n. 209/2005 (codice delle assicurazioni private).

Inoltre, sulla scorta del provvedimento adottato dal Garante il 26 ottobre 2023, n. 520 (doc. web n. 9954881), sono stati esaminati diversi reclami con i quali gli interessati, eredi e chiamati all'eredità, avevano lamentato il rifiuto opposto dalle compagnie assicurative a comunicare i dati identificativi dei beneficiari di polizze stipulate in vita da persone decedute. In tutti i casi presi in considerazione nel corso del 2025, l'Ufficio, all'esito dei procedimenti istruttori, ha ritenuto corretta la valutazione effettuata dalle compagnie assicurative circa la (in)sussistenza dei presupposti (alla conoscibilità) individuati nel provvedimento anzi citato.

Tra le pronunce dell'Autorità maggiormente significative in ambito assicurativo si segnala il provv. 10 luglio 2025, n. 389 (doc. web n. 10154110), con il quale ad una compagnia di assicurazioni è stata comminata una sanzione pari a euro 80.000 per avere comunicato i dati relativi a tre polizze vita intestate alla reclamante a un soggetto terzo non autorizzato che li aveva poi utilizzati nell'ambito di un procedimento giudiziario intentato nei confronti della reclamante. Nella fattispecie esaminata l'istituto assicurativo, a fronte di specifiche richieste di accesso che sembravano provenire dal soggetto legittimato ad accedervi (in quanto recanti le sue generalità e firma autografa), aveva trasmesso specifiche informazioni e copiosa documentazione tramite e-mail a una casella di posta elettronica che l'interessata non aveva mai indicato quale suo contatto; ciò era avvenuto in ragione del comportamento negligente della compagnia che, in violazione del principio di cui all'art. 5, par. 1, lett. a) e f), RGPD, aveva provveduto ad inviare le informazioni richieste omettendo di porre in atto ogni misura idonea a verificare l'effettiva rispondenza tra l'indirizzo di posta elettronica in utilizzo e l'identità della cliente. L'Autorità ha altresì contestato alla compagnia assicurativa la mancata ottemperanza all'obbligo di notificare all'Autorità la violazione dei dati personali entro 72 ore dal suo accertamento, ai sensi dell'art. 33, par. 1, RGPD. Nel caso esaminato, infatti, la notifica anzidetta era stata effettuata a distanza di quasi quattro mesi dal disconoscimento della casella e-mail in questione da parte dell'interessata e, quindi, con grave ritardo rispetto al momento in cui la compagnia aveva avuto la "ragionevole" evidenza (cfr. pp. 31 e 33 delle linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD, adottate dal CEPD 28 marzo 2023) che un proprio operatore avesse inviato i dati personali riferiti all'interessata ad un soggetto estraneo.

Parimenti di interesse è il provv. 4 giugno 2025, n. 325 (doc. web n. 10164296),

14

emanato a seguito di una segnalazione di un padre, il quale aveva rappresentato al Garante che, a causa di urgente ricovero ospedaliero, la figlia aveva dovuto rinunciare al viaggio di istruzione e, di conseguenza, aveva inoltrato richiesta all'istituto scolastico per poter ottenere il rimborso dell'importo pagato. La compagnia assicurativa della scuola aveva comunicato che al fine di poter istruire la pratica era necessario firmare un "modello privacy" debitamente compilato da uno dei due genitori, in quanto la figlia era ancora minorenne, nonché successivamente fornire anche i documenti relativi alla cartella clinica. Nell'istruttoria condotta dall'Autorità è emerso, però, che l'agenzia assicurativa mandataria aveva contravvenuto alle specifiche prescrizioni impartite dalla compagnia principale, contenute nell'accordo di designazione a responsabile del trattamento (ex art. 28 del RGPD) e, in particolare, aveva mancato nel fornire le informazioni corrette al genitore dell'interessata minorenne rispetto allo specifico trattamento dei dati personali, con conseguente violazione degli artt. 28, e 5, par. 1, lett. a), RGPD.

Rete RPD nel settore assicurativo

Nel corso del 2025, il Gruppo di lavoro "Rete dei RPD nel settore assicurativo" ha concluso l'analisi delle risultanze del questionario (v. par. 14.1. Relazione 2024) che ANIA aveva rivolto ai RPD delle imprese assicurative allo scopo di poter disporre di una visione d'insieme circa il grado di penetrazione e di operatività della figura del RPD nel contesto assicurativo.

L'analisi condotta ha coinvolto 85 imprese assicurative e hanno aderito all'iniziativa l'87% delle imprese invitate – che rappresentano oltre il 90% dei servizi assicurativi erogati – suddivise in grandi, medie e piccole imprese.

Le risposte fornite dai diversi RPD sono state analizzate da ANIA che, il 22 maggio 2025, ha trasmesso all'Autorità un documento di sintesi (ove i dati sono riportati in forma aggregata) denominato "*Survey* sul Responsabile per la protezione dei dati nel settore assicurativo", il cui contenuto è stato illustrato e ampiamente commentato in un incontro tenutosi presso l'Autorità il 12 novembre 2025 cui hanno preso parte tutti i partecipanti alla rete. Nel corso dell'incontro è stato altresì avviato il progetto di realizzare, anche nel settore assicurativo come in quello bancario, informative omogenee e semplificate da rendere mediante l'utilizzo di icone standardizzate.

Parere sul decreto IVASS in materia di oblio oncologico

Con provv. 18 dicembre 2025, n. 750 (doc. web n. 10212338) l'Autorità ha espresso parere favorevole, ai sensi degli artt. 36, par. 4, e 58, par. 3, lett. b), RGPD sullo schema di provvedimento IVASS in attuazione dell'art. 2, comma 7, l. n. 193/2023 recante disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone che sono affette da malattie oncologiche. Lo schema di decreto attuativo dell'IVASS riconosce alle persone guarite da tumori il diritto di non dare informazioni, né subire controlli, sulla loro malattia pregressa trascorso un certo periodo senza recidive, né per i nuovi contratti, né per i rinnovi assicurativi. Non è consentito acquisire informazioni sul rischio di malattie oncologiche dell'assicurato, né sullo stato di salute dei suoi familiari. Inoltre le imprese assicurative hanno l'obbligo di cancellare le informazioni sulla patologia oncologica pregressa, entro trenta giorni dal ricevimento della certificazione attestante i requisiti per l'esercizio dell'oblio oncologico.

A seguito delle interlocuzioni condotte con l'IVASS, in particolare, l'Autorità ha ritenuto conformi alla disciplina in materia di protezione dei dati personali le disposizioni del decreto relative a:

- l'informativa sul diritto all'oblio oncologico nei documenti precontrattuali assicurativi;
- divieto di raccolta ed utilizzo delle informazioni sulle patologie oncologiche pregresse per la determinazione del premio assicurativo e di altre condizioni contrattuali;
- modalità di esercizio del diritto alla cancellazione delle informazioni e disciplina dei relativi obblighi.

14.2. *Trattamento di dati personali in ambito bancario-finanziario e sistemi di informazione creditizia*

Nel corso del 2025 l'Autorità ha ricevuto un numero significativo di reclami e segnalazioni concernenti profili del trattamento dei dati degli interessati nell'ambito dell'attività bancaria, già oggetto di precedenti provvedimenti del Garante (tra tutti, v. le linee guida per i trattamenti dei dati relativi al rapporto banca-clientela, adottate il 25 ottobre 2007, doc. web n. 1457247).

Accesso indebito ai dati dei clienti di istituti di credito

Alcuni reclami e segnalazioni hanno riguardato il tema degli 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 sempre all'attenzione del Garante, che, già con provv. 12 maggio 2011, n. 192 (doc. web n. 1813953), ha prescritto ai titolari del trattamento l'adozione di misure specifiche (tra le quali, 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 *inquiry*); l'implementazione di sistemi di *alert* idonei a rilevare comportamenti anomali o a rischio; lo svolgimento di audit interni al fine di valutare la tenuta e l'efficacia delle misure predisposte). Tali misure intendono consentire alle banche di impedire illecite operazioni di trattamento ai danni dei clienti e di conoscere chi abbia effettuato il trattamento dei dati dei clienti e il momento in cui ciò è avvenuto.

In numerosi casi, all'esito dell'attività istruttoria avviata dall'Autorità, è emerso trattarsi di accessi effettuati da soggetti autorizzati e nell'ambito della corretta operatività bancaria.

In particolare, in un caso in cui il reclamante aveva lamentato un possibile accesso indebito al suo stato patrimoniale e alle linee di credito in essere con la banca, nonché ai saldi e ai movimenti dei propri conti correnti, è stata effettuata una verifica presso la banca (nell'ambito dell'attività di accertamento prevista dall'art. 58, par. 1, lett. a), e) ed f), RGPD e dagli artt. 157 e 158, commi 1 e 2, del Codice), nel corso della quale è stata esaminata la vicenda oggetto del reclamo.

In tale contesto la banca, nell'evidenziare che, al momento dell'accertamento, la questione oggetto di reclamo era stata rimessa anche di fronte al giudice civile territorialmente competente (con ricorso ai sensi dell'art. 10 del lgs. n. 151/2011 notificato in data 13 agosto 2024), aveva rappresentato di avere effettuato l'estrazione dei log di accesso ai dati dell'interessato, depositandoli presso un notaio e che le operazioni bancarie eseguite si riferivano alla normale operatività della banca, non rientrando quindi nella casistica degli accessi illeciti.

Le risultanze istruttorie hanno confermato che gli accessi oggetto di doglianza erano stati effettuati nell'ambito dell'attività operativa posta in essere dalla banca, non ponendosi, pertanto, in violazione della disciplina in materia di protezione dei dati personali, né del provv. 12 maggio 2011, n. 192, recante prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (doc. web n. 1813953 - v. nota 25 marzo 2025).

L'Autorità, infine, muovendo anche da notifiche di *data breach* effettuate da taluni istituti bancari, ha proseguito l'attività iniziata nel corso del 2024 in questo ambito, al fine di individuare, in ragione del lungo tempo trascorso dall'adozione del sopra indicato provv. 12 maggio 2011, n. 192, ulteriori misure idonee a contrastare e controllare il fenomeno, tenendo conto sia del principio di *accountability* introdotto dal RGPD, che delle previsioni contenute negli artt. 32, 33 e 34 dello stesso RGPD.

Esercizio dei diritti degli interessati

Come di consueto, sono pervenute molteplici istanze in materia di esercizio dei diritti degli interessati che sono state dichiarate infondate in quanto presentate senza conformarsi alle disposizioni operanti in materia e, per quanto riguarda specificamente

14

il diritto di accesso ai dati personali, senza tenere conto delle indicazioni contenute nelle linee guida CEPD 1/2022 del 18 gennaio 2022 in materia di diritto d'accesso.

In tale ambito, sono state numerose le richieste di documentazione bancaria, rivolte alle banche e agli intermediari finanziari ai sensi delle norme di settore vigenti (in particolare, ai sensi dell'art. 119 del d.lgs. n. 385/1993 - Testo unico bancario), la cui osservanza è presidiata da autorità diverse dal Garante e che, ove disattese, consentono di rivolgersi all'autorità giudiziaria ordinaria o, per alcuni profili, all'Arbitro bancario e finanziario (ABF). In tali casi si è dunque reso necessario tornare a precisare che il diritto di accesso ai dati personali riconosciuto agli interessati dall'art. 15 del RGPD è altro dal diritto di accesso ai documenti bancari e che l'esercizio del diritto di accesso riconosciuto dalla normativa in materia di protezione dei dati personali consente all'interessato di avere "conferma che sia o meno in corso un trattamento dei dati personali che lo riguardano", qualora oggetto di effettivo trattamento da parte del titolare, il quale rende all'interessato, "[…] le comunicazioni di cui agli articoli da 15 a 22 […] relative al trattamento in forma concisa […]" (v. art. 12, par. 1 del RGPD) e, sempre che ciò non leda i diritti e le libertà altrui, copia dei dati personali trattati (su qualsiasi supporto reputato congruo dal titolare a tale scopo). In proposito, si è pertanto rilevato che il diritto riconosciuto all'interessato dall'art. 15 del RGPD consente di avere accesso ai dati e alle informazioni di cui alle lett. da a) ad h) del citato art. 15, ma non anche di ottenere la riproduzione dei documenti originali (non consente, ad es., di ottenere la copia di contratti o di estratti conto o di altri documenti bancari). Questi ultimi (che, peraltro, possono contenere anche informazioni diverse da dati personali, oltre che dati personali riferiti a terzi), sono ottenibili, eventualmente, ai sensi di altre disposizioni normative, che danno modo, ai soggetti legittimati, di ricevere copia integrale di tutta la documentazione.

L'Autorità ha sanzionato un istituto di credito per un importo pari a euro 100.000 per il fatto di avere comunicato al reclamante i dati contenuti nelle registrazioni telefoniche intercorse con il servizio clienti solo tardivamente, ovvero dopo la presentazione del reclamo all'Autorità. Nel caso esaminato l'istituto di credito aveva rappresentato come il ritardo era stato causato da un errore della banca nella individuazione di tutte le chiamate ricevute dal servizio clienti da parte dell'interessato; la procedura prevista dalla casa-madre a tale riguardo consentiva a ciascun *outsourcer* del servizio clienti di accedere esclusivamente alle comunicazioni con la clientela gestite dal medesimo *outsourcer*, salvo richiedere evidenza di tutte le ulteriori comunicazioni a un team interno della banca deputato alla gestione delle richieste di recupero delle registrazioni. Il reclamo ha rappresentato così l'occasione, per la banca, di rivedere la procedura di estrazione delle registrazioni telefoniche prevedendo la creazione di un processo *ad hoc* volto a consentire al servizio clienti di gestire in autonomia l'invio delle registrazioni alla clientela (provv. 10 luglio 2025, n. 413, doc. web n. 10168555).

Rete dei RPD nel settore bancario

Nel 2025 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 bisognose di approfondimento e confronto (tra cui, l'applicazione della cd. normativa sull'antiriciclaggio e l'individuazione di soluzioni operative per valutare l'eventuale adozione di linee guida sul tema dell'accesso indebito dei dipendenti di istituti di credito ai dati della clientela, allo stato disciplinato dal citato provvedimento del Garante 12 maggio 2011, n. 192, recante prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (doc. web n. 1813953).

Furti di identità e frodi informatiche

Nel corso di quest'anno, inoltre, è stato realizzato, con ABI, il progetto di informativa omogenea e semplificata da rendere mediante icone standardizzate (v. Relazione 2024, p. 166), avente lo scopo di migliorare e rendere più chiaro il rapporto tra i titolari del

trattamento e gli interessati, garantendo, al contempo, il rispetto dei principi applicabili al trattamento dei dati personali.

Nel corso dell'anno sono pervenute anche richieste di intervento rivolte al Garante in casi di furto d'identità e frodi informatiche.

Nei casi esaminati, si è rammentato che, preso atto del dilagare di comportamenti fraudolenti sempre più sofisticati e complessi sul piano tecnologico, il Garante ha già da tempo reso disponibile, sul proprio sito, una scheda informativa per sensibilizzare l'utenza affinché adotti accorgimenti e cautele per evitare di rimanere vittima di illeciti penali (v. doc. web n. 5779928; v. anche doc. web n. 9873859 e le ulteriori pagine informative indicate in calce a quest'ultimo documento).

Si è pure ribadito che indicazioni sui comportamenti da assumere o evitare per non incorrere in questa tipologia di frodi sono sempre presenti sui siti istituzionali di ogni banca e intermediario finanziario allo scopo di consentire alla clientela di operare a distanza e che agli strumenti e alle iniziative già adottate in materia di sicurezza da ABI, istituzioni e singole banche si affianca anche un vademecum (varato fin dal 2022 e sottoposto ad accurati aggiornamenti periodici) realizzato congiuntamente da ABI e dalla Polizia di Stato e consultabile sui rispettivi siti istituzionali.

Considerato, peraltro, che gli interessati avevano già denunciato gli eventi occorsi nelle sedi preposte all'accertamento delle fattispecie di reato rinvenibili nelle condotte oggetto di istanze all'Autorità, ci si è riservati – anche alla luce dell'art. 167, comma 4, del Codice – di assumere eventuali determinazioni all'esito e sulla base delle risultanze di tali accertamenti.

Trattamento dei dati nei Sistemi di informazione creditizia (SIC)

Nel corso del 2025 sono stati numerosi i reclami e le segnalazioni in materia di trattamenti di dati personali censiti nei Sistemi di informazione creditizia gestiti da soggetti privati (cd. SIC).

Alcune richieste hanno riguardato il tema del preavviso da rendere all'interessato, al verificarsi di ritardi nel pagamento degli importi pattuiti e prima dell'inserimento dei dati nei SIC; altre i tempi di conservazione dei dati nei SIC (diversi a seconda che il rapporto censito sia stato stipulato o meno e, in caso positivo, che abbia o meno un andamento regolare); altre ancora l'esercizio di taluni diritti (in particolare, di accesso, di aggiornamento e di cancellazione dei dati censiti nei SIC).

Nella maggior parte dei casi esaminati, tuttavia, non sono risultate comprovate violazioni della normativa in materia di protezione dei dati personali, ma 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 - O.d.M. (doc. web n. 9818201) e fornite agli interessati indicazioni per esercitare i propri diritti nei confronti dei SIC e/o dei partecipanti a questi ultimi.

I reclami presentati all'Autorità nei confronti dei gestori dei SIC per l'omesso o inidoneo riscontro alle istanze avanzate dagli interessati ai sensi degli artt. 15 e ss. del Regolamento, hanno riguardato, per lo più, casi nei quali il titolare del trattamento ha comunicato i dati richiesti con ritardo rispetto al termine di un mese previsto dall'art. 12, par. 3, RGPD, in ragione di errori o disservizi di tipo tecnico (provv. 23 ottobre 2025, n. 630, doc. web n. 10196194).

14.3. *Imprese*

Anche il 2025 è stato contraddistinto da un elevato numero di istanze (segnalazioni, reclami, quesiti e richieste di parere) riguardanti molteplici profili concernenti il trattamento di dati personali effettuato nel settore delle attività a carattere economico.

Pubblicazione online di immagini relative a minori

Il Garante si è in particolare pronunciato nei confronti di una società che aveva raccolto immagini di minori ritratti in maniera riconoscibile in un centro estivo e le aveva successivamente diffuse online in assenza del preventivo consenso degli esercenti la potestà genitoriale (provv. 13 novembre 2025, n. 726, doc. web n. 10210803).

Il provvedimento ha innanzitutto costituito l'occasione per ribadire che la manifestazione di volontà volta ad autorizzare un trattamento di dati personali relativi a minori richiede sempre il consenso informato di entrambi i genitori, anche laddove sia disposto il regime di affidamento condiviso del medesimo minore (cfr. in tal senso provv. 13 novembre 2024, n. 681, doc. web n. 10076481 e la giurisprudenza ivi richiamata), e che tale consenso, inoltre, può essere revocato da quest'ultimi "in qualsiasi momento" (art. 7, par. 3, RGPD).

Più nello specifico, nel corso dell'istruttoria il titolare non aveva fornito alcuna prova, ai sensi dell'art. 7, par. 1, RGPD, dell'avvenuta acquisizione del consenso degli esercenti la responsabilità genitoriale alla raccolta delle immagini relative ai figli in occasione della loro partecipazione al centro estivo e alla successiva diffusione anche online di video e/o fotografie che li riguardavano; l'Autorità ha pertanto dichiarato l'illiceità del relativo trattamento per la violazione dell'art. 5, par. 1, lett. a) e dell'art. 6, par. 1, lett. a), RGPD.

Inoltre, il Garante tenuto conto che l'illecita diffusione era riconducibile ad un errore umano dell'operatore preposto al montaggio delle immagini e che la società aveva provveduto tempestivamente alla rimozione del video in parola nonché a cancellare i fotogrammi ivi contenuti, ha formulato un ammonimento nei confronti del titolare ai sensi dell'art. 58, par. 2, lett. b), RGPD.

Da ultimo, avendo l'Autorità constatato che nel modulo di adesione al centro estivo in questione, la sezione relativa a il "Rilascio consenso per minori" non conteneva indicazioni chiare ed esaustive in ordine all'effettivo ambito di diffusione delle immagini dei minori acquisite nel corso dello svolgimento delle attività sociali né in merito alle connesse finalità perseguite dal titolare, ha prescritto a quest'ultimo di adottare alcune misure correttive volte a garantire, attraverso la compilazione del predetto modulo, l'acquisizione di un consenso specifico ed inequivocabile rispetto a tale trattamento di dati, in conformità agli artt. 6 e 7 del RGPD e a quanto chiarito in tal senso anche dal CEPD nelle linee guida 5/2020 sul consenso ai sensi del Reg. (UE) 2016/679, adottate il 4 maggio 2020 (cfr. parr. 75 e 84).

Misure atte a garantire l'esercizio dei diritti

Il Garante si è pronunciato nei confronti di una società di autonoleggio al fine di ribadire l'obbligo a carico del titolare di disporre, al proprio interno, di un sistema organizzativo e gestionale contraddistinto da misure reali ed efficaci volte a garantire l'esercizio dei diritti degli interessati sanciti dagli artt. 15-22 del Regolamento.

La decisione è scaturita a seguito della ricezione di due reclami aventi ad oggetto l'inidoneo riscontro, da parte della società, alle istanze di accesso presentate da alcuni clienti. Sul punto, al netto delle specifiche violazioni riscontrate con riferimento ai singoli reclami, è emersa, più in generale, una criticità di carattere sistemico in termini di inadeguatezza delle misure organizzative implementate dalla società, al fine di adempiere agli obblighi di cui agli artt. 15-22 del RGPD.

Più nello specifico, è stato chiarito che l'attuazione del principio di *accountability*, con riferimento all'esercizio dei diritti dell'interessato, pone, in capo al titolare, l'onere di predisporre un sistema organizzato per la gestione delle istanze presentate ai sensi degli artt. 15-22 del Regolamento, individuando specifiche istruzioni da fornire al personale incaricato (quali l'obbligo di monitorare l'e-mail dedicata, di chiarire le tempistiche da rispettare e quello di individuare le casistiche di differimento dei termini), mettendo a disposizione modelli di risposta (ad es. istanza di cancellazione; differimento dei termini

con motivazione) e moduli operativi per fronteggiare le diverse casistiche (ad es. indicazioni sui referenti da contattare e sulle azioni da effettuare in caso di ricezione di un invito ad aderire del Garante; istruzioni sulle attività da porre in essere in caso di sollecito dell'istanza).

È stata pertanto rilevata l'illiceità della condotta della società rispetto agli artt. 5, par. 2, 12, par. 3, 15, nonché 24 del RGPD ed è stata, al contempo, applicata una sanzione pecuniaria di euro 50.000 (provv. 25 settembre 2025, n. 535, doc. web n. 10187975).

Illecito trattamento dei dati personali contenuti nelle tessere sanitarie

Di interesse è inoltre il provv. 23 ottobre 2025, n. 631 (doc. web n. 10210718), a mezzo del quale l'Autorità ha applicato una sanzione pecuniaria pari a euro 10.000 nei confronti della titolare di una tabaccheria per avere conservato e utilizzato tessere sanitarie altrui, al fine di eludere il vincolo di plafond imposto alla propria carta prepagata, in violazione degli artt. 5, comma 1, lett. a), b), c) ed e), 6 e 13 del RGPD.

Illecita comunicazione di dati inerenti alla salute

L'Autorità ha infine applicato una sanzione pecuniaria di euro 30.000 a seguito di un reclamo concernente presunte violazioni della normativa in materia di trattamento dei dati personali effettuate in occasione di una visita di idoneità alla mansione lavorativa. In base agli elementi acquisiti in sede istruttoria, era risultato che la società, che agiva in qualità di medico competente, aveva illecitamente comunicato i dati dell'interessato al datore di lavoro in assenza di una valida base giuridica e in contrasto con il principio di minimizzazione, in violazione degli artt. 5, par. 1, lett. b), c) e f), 6, par. 1 e 9, par. 2, RGPD (provv. 10 luglio 2025, n. 450, doc. web n. 10168519).

14.4. *Concessionari di pubblici servizi*

In relazione ai trattamenti effettuati da concessionari di pubblici servizi, il 2025 è stato caratterizzato da un'intensa attività di vigilanza e di controllo volta a verificare il corretto adempimento della normativa in materia di protezione dei dati personali da parte dei gestori aeroportuali, con specifico riferimento al trattamento dei dati dei passeggeri per il tramite di sistemi di riconoscimento facciale volti a facilitare le operazioni di accesso e transito all'interno dell'aeroporto.

Sistemi di riconoscimento facciale in aeroporti

È stata condotta una specifica istruttoria a seguito dell'avvenuta installazione, presso l'aeroporto di Milano Linate, di un sistema di riconoscimento facciale, denominato *FaceBoarding*, volto a consentire l'identificazione dei passeggeri ai varchi di accesso all'area sterile e alle porte di imbarco.

Con il provvedimento adottato è stata ordinata la sospensione dell'utilizzo della specifica soluzione tecnologica adottata – che alla data del 31 luglio 2025 risultava ancora funzionante presso l'aeroporto di Milano Linate e riguardava 24.550 persone interessate – poiché ritenuta incompatibile con la vigente disciplina europea sulla protezione dei dati personali e con il parere 11/2024 del CEPD, adottato il 24 maggio 2024 (*Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR* - v. Relazione 2024, p. 208 e ss.).

Invero, a seguito delle verifiche effettuate, è emerso che il sistema *FaceBoarding* così concepito aveva comportato la memorizzazione dei *template* biometrici dei passeggeri in un archivio centralizzato presso il gestore aeroportuale, senza garantire al contempo ai predetti interessati un potere di controllo esclusivo sui propri dati biometrici. Tale situazione si configurava sia con riferimento all'ipotesi in cui la fase di adesione al sistema avveniva in aeroporto per il tramite dei chioschi ivi situati, sia ove la stessa era effettuata mediante l'applicazione mobile all'uopo specificatamente dedicata. In tali termini il sistema era da inquadrare nel cd. scenario 3.1 della suddetta *Opinion*, che lo

14

riteneva in contrasto con gli artt. 5, par. 1, lett. f), 25 e 32 del RGPD (cfr. sez. 3.2.3.1 dell'*Opinion* 11/2024).

Inoltre, il trattamento in questione era risultato in contrasto anche con gli artt. 5, par. 1, lett. e), 6, 13 e 32 del RGPD, stante l'inadeguatezza, di alcune misure tecniche e organizzative implementate (inerenti alla presenza di alcune informazioni inesatte nel modello di informativa; alla mancata adozione di misure di cifratura del *template* biometrico all'atto della conservazione di quest'ultimo nei propri sistemi; ai tempi di conservazione dei *template* biometrici estesi fino a 12 mesi nel caso di adesione del passeggero al "programma a lungo termine"; alla "natura ibrida" dei varchi dedicati al *FaceBoarding* che comportava il trattamento di dati biometrici del passeggero non aderente al sistema in assenza del suo consenso esplicito).

Pertanto, il Garante, in ragione dell'elevata gravità delle constatate violazioni, del cospicuo numero di interessati coinvolti e della particolare natura dei dati personali trattati, ha ritenuto, con il provvedimento citato, di dover adottare in via d'urgenza, ai fini di tutelare i diritti e le libertà degli interessati, la misura della limitazione provvisoria del trattamento (art. 58, par. 2, lett. f), RGPD - v. provv. 11 settembre 2025, n. 489, doc. web n. 10167745).

15 Altri trattamenti in ambito privato

15.1. *Trattamenti di dati personali all'interno del condominio e nella gestione del condominio*

Continuano ad essere numerose le segnalazioni e i reclami aventi ad oggetto trattamenti di dati effettuati nell'ambito della gestione della compagine condominiale, con particolare riguardo all'impiego di apparati di videosorveglianza, anche da parte di singoli all'interno di spazi condominiali. Esse riguardano fattispecie in larga misura già oggetto di esame in passato (ad es., in relazione all'utilizzo, sovente controverso per le modalità di impiego, di apparati di ripresa video e audio da parte di singoli condomini in spazi di terzi o comuni), ma pure se ne segnalano relative a profili innovativi, concernenti l'utilizzo dei cd. spioncini elettronici da parte di singoli condomini e l'impiego di droni in prossimità degli immobili condominiali. Solo occasionalmente è portata all'attenzione del Garante la diffusione indebita di dati personali mediante la pubblicazione di documentazione nella bacheca condominiale (oggetto di reiterati interventi dell'Autorità e, non diversamente, della giurisprudenza di legittimità).

Rispetto agli aspetti che già in passato hanno formato oggetto di esame da parte del Garante, l'Autorità provvede a fornire chiarimenti, anche mediante l'invio di comunicazioni volte a promuovere una maggiore consapevolezza degli obblighi gravanti sui soggetti coinvolti nelle operazioni di trattamento.

Circolazione di dati personali riferiti ai condomini all'interno della compagine condominiale

Tra gli aspetti tuttora più ricorrenti si segnala quello della circolazione dei dati tra i partecipanti alla compagine condominiale (di solito mediante comunicazioni di posta elettronica, ma si segnala il fenomeno emergente anche dell'utilizzo di piattaforme). Al riguardo l'Autorità, sulla scorta dei suoi costanti orientamenti (e del concorde indirizzo della Corte di cassazione), ha ribadito che le informazioni personali riferibili a ciascun partecipante possono essere trattate, nel rispetto dei principi generali stabiliti dall'art. 5 del RGPD, per la finalità di gestione ed amministrazione del condominio e che, per tali finalità, dette informazioni possono essere condivise all'interno della compagine condominiale; ciò sulla scorta delle disposizioni contenute nel codice civile in materia di condominio negli edifici che attribuiscono al singolo condomino il diritto di prendere visione dei documenti giustificativi di spesa detenuti dall'amministratore e, secondo le regole di diritto comune, di estrarne copia in ogni tempo, al fine di poter disporre di un quadro chiaro della situazione contabile del proprio condominio (cfr. artt. 1130 e 1130-*bis*, c.c.).

È stato inoltre ribadito che, fatte salve eventuali diverse disposizioni da parte del regolamento di condominio, è di regola richiesto il consenso dei partecipanti per il trattamento di dati personali, quali le utenze telefoniche o gli indirizzi di posta elettronica individuali, che non sono annoverabili tra quelli oggetto di necessario trattamento per dare esecuzione all'attività gestoria, non essendo indispensabili rispetto alla determinazione dei diritti o degli oneri relativi al bene comune ovvero, più in generale, alla gestione della cosa comune.

Funzionalità "ccn"

Il Garante ha chiarito che l'utilizzo di un indirizzo di posta elettronica costituisce un trattamento di dati personali e che, quindi, deve avvenire nel rispetto dei princìpi di cui

all'art. 5 del RGPD ed essere sorretto, ai fini della sua liceità, da un'adeguata base giuridica, quale il consenso dell'interessato (art. 6, par. 1, RGPD).

Muovendo da tale assunto, l'Autorità ha confermato il proprio (tradizionale) indirizzo secondo il quale ben possono essere inviate in unica soluzione comunicazioni aventi il medesimo tenore ad una pluralità di destinatari (nel caso di specie, condomini) mediante la previa adozione di semplici accorgimenti – quale, semplicemente, l'impiego della funzione "ccn" (copia conoscenza nascosta) presente in tutti i servizi di messaggeria –, sì da impedire, senza onere aggiuntivo alcuno, la contestuale e agevole conoscibilità della documentazione trasmessa a tutti i destinatari, precludendo a ciascuno di essi di conoscere l'indirizzo di posta elettronica degli altri.

Quanto alla comunicazione di dati personali riferibili ai condomini a soggetti esterni alla compagine condominiale, è stato ribadito che, in termini generali, in assenza di altra idonea base giuridica per tale trattamento, il consenso degli interessati opera di regola quale presupposto di liceità per la condivisione delle informazioni relative ai singoli condòmini.

Consultazione sulle nuove linee guida relative al trattamento dei dati personali nell'ambito del condominio

A fronte delle persistenti (numerose) istanze dirette all'Autorità, con provv. 10 aprile 2025, n. 209 (doc. web n. 10128634), il Garante ha approvato le linee guida sul "Trattamento dei dati personali nell'ambito del condominio", volte ad aggiornare il più risalente documento di orientamento adottato con il provvedimento generale 18 maggio 2006 (doc. web n. 1297626) come pure il Vademecum "Il condominio e la privacy" (doc. web n. 2680257), deliberando contestualmente di "avviare una consultazione pubblica, volta ad acquisire osservazioni e proposte in merito alla congruità della individuazione dell'ambito materiale in cui l'amministratore di condominio ricoprirebbe il ruolo di titolare del trattamento dei dati personali e, più in generale, all'interpretazione delle disposizioni di protezione dati nell'ambito dell'amministrazione del condominio".

Si è quindi proceduto all'avvio della consultazione, con la pubblicazione delle citate linee guida nella G.U. 9 maggio 2025, n. 106, mettendo a disposizione il testo anche sul sito del Garante e indicando la notizia nella Newsletter dell'8 maggio 2025, n. 534 (doc. web n. 10129281). Allo scopo di favorire la più ampia partecipazione, in particolare da parte degli operatori del settore, si è altresì provveduto ad inoltrare una comunicazione *ad hoc* a 27 associazioni di categoria, ricomprendenti anche quelle degli amministratori di condominio (e quanti offrono consulenza in detta materia) nonché a 4 associazioni di proprietari, estratte dall'elenco delle associazioni professionali concernente le professioni non organizzate in ordini o collegi previsto dalla l. n. 4/2013.

All'esito della consultazione pubblica così avviata sono pervenuti all'Autorità 17 contributi, nella maggior parte dei casi provenienti da associazioni di categoria, per lo più rientranti nel novero (più ampio) delle associazioni invitate a partecipare, ovvero da operatori che si occupano della gestione di condomini e di servizi di consulenza agli amministratori di condominio nonché da parte di professionisti attivi in tale ambito. Esaminati i contributi pervenuti – recanti anche valutazioni critiche rispetto ad alcuni dei profili qualificanti dello schema posto in consultazione (in particolare con riguardo al segnalato aspetto concernente la delimitazione della titolarità del trattamento nell'ambito della gestione del condominio) – l'Autorità ha avviato ulteriori approfondimenti in vista dell'adozione del testo definitivo delle linee guida.

15.2. *Trattamento di dati da parte di associazioni e fondazioni*

Dal contesto associativo continuano a pervenire questioni di diversa natura in relazione alle quali sono state fornite indicazioni, anzitutto concernenti il corretto esercizio del

diritto d'accesso e degli altri diritti accordati agli interessati (disciplinati agli artt. 15 ss. del RGPD) che, in molti casi, consentono una rapida risoluzione delle questioni controverse, altrimenti, spesso direttamente sottoposte all'attenzione dell'Autorità.

Principio di minimizzazione

L'Autorità è stata investita più volte, anche nel corso del 2025, di questioni concernenti la verifica, oltre che del rispetto degli obblighi informativi da fornire agli interessati al momento della raccolta dei dati (v. *infra*), anche dell'osservanza dei principi declinati all'art. 5, par. 1, RGPD, con particolare riferimento ai principi di "liceità, correttezza e trasparenza" nonché di "minimizzazione" (anche in relazione a casi di diffusione di dati personali) (art. 5, par. 1, lett. a) e c), RGPD). In più occasioni è stato così ribadito che in ambito associativo i dati personali riferiti agli associati possono essere trattati quando e in quanto necessari per eseguire gli obblighi derivanti dal vincolo associativo, in coerenza con le finalità perseguite dall'associazione, individuate di regola nell'atto costitutivo, nello statuto e in altri idonei atti, adottati in base alle regole interne di funzionamento dell'associazione; ovvero qualora il presupposto di liceità del trattamento sia riconducibile al consenso espresso dell'interessato, salva l'evidenza di altra base giuridica di cui all'art. 6 del RGPD.

Informative inidonee

Anche al fine di prevenire l'insorgere di controversie circa gli ambiti di circolazione dei dati trattati nel contesto associativo e delle relative finalità, è indispensabile non ridurre l'obbligo di fornire informative idonee a un mero esercizio formale. Ciò si è verificato, ad esempio, in relazione ad un formulario di adesione ad un'associazione recante la dizione "Autorizzo al trattamento dei miei dati personali in accordo con l'art. 13 della legge italiana n. 196/2003", ritenuta dal Garante totalmente inidonea a soddisfare i requisiti previsti dalla legge sia in punto di informativa che di consenso dell'interessato (cfr. provv. 30 gennaio 2025, n. 37, doc. web n. 10136950).

15.3. *Videosorveglianza nel settore privato*

Videosorveglianza: l'evoluzione di un fenomeno sociale

La materia della videosorveglianza rappresenta uno degli ambiti nei quali più elevato, ed in costante ascesa (cfr. sez. IV, tabb. 12 e 13) è il numero di segnalazioni e reclami che pervengono all'Autorità, in parte veicolate da altri organi dello Stato a seguito di verifiche condotte nell'ambito delle proprie attribuzioni o a seguito di segnalazione della cittadinanza (non di rado frutto di alterchi o altre forme di conflittualità nei rapporti di vicinato).

Dal punto di osservazione dell'Autorità, pare evidente, e va segnalato con grande preoccupazione, l'incremento nel ricorso agli apparati di ripresa – tradizionalmente presenti nei contesti industriale, commerciale o professionale, tipicamente a tutela del patrimonio ovvero, in ambiti particolari, a tutela dell'incolumità delle persone – in particolare, e in modo ormai "pulviscolare", anche in ambiti più propriamente riconducibili alla quotidianità del vivere sociale, nello svolgimento di attività personali e domestiche.

Le ragioni di tale incremento, al di là dell'obiettivo di elevare il livello di sicurezza individuale (reale o solo percepito), sono plurime: decrescenti (e comunque contenuti) i costi di acquisto degli apparati di ripresa, potenziamento delle funzionalità degli stessi, con immagini spesso accessibili da remoto attraverso apposite app, e facilità di loro (auto)installazione.

D'altro canto, a questa tendenza fa da contraltare, ma in direzione esattamente inversa, una generalizzata preoccupazione in quanti entrano o, in molti casi, vivono "nell'obiettivo" della telecamera del vicino (sempre più sofisticata e, *by design*, invasiva), talora imponendo forzati cambiamenti nello stile di vita, salva la ricorrenza nei casi più gravi, di condotte invasive penalmente rilevanti. Ciò dipende da molteplici fattori: le caratteristiche tecniche dei sistemi (dotati di zoom, funzione audio bidirezionale, visione

notturna e sensori di movimento, visualizzazione da remoto, variazioni di inquadratura), la loro ubicazione (su muri di confine o perimetrali o in spazi antistanti delle abitazioni private) o anche la conformazione dei luoghi in cui sono dislocati (tra loro confinanti o comunque ravvicinati o di accesso comune).

Quanto sinteticamente rappresentato rende conto del numero crescente di segnalazioni e reclami presentati all'Autorità nei confronti di soggetti privati che si avvalgano di sistemi di ripresa; si tratta di una parte consistente, e in termini percentuali prevalente, di quelli ricevuti su base annuale in materia di videosorveglianza.

E si tratta, a ben vedere, solo della parte affiorante di un "iceberg" che tocca ben altre profondità del nostro vivere sociale, posto che indubitabilmente la videosorveglianza rappresenta un fenomeno, da tempo (fin dalle origini, potrebbe dirsi) segnalato dal Garante, di primaria rilevanza sociale e divenuto ormai di costume, strutturatosi in tutte le dimensioni del vivere sociale, rispetto al quale la risposta ordinamentale non può collocarsi nella sola dimensione dell'*enforcement*.

Non di rado, come anticipato, le segnalazioni in materia discendono da (o si accompagnano a) rapporti litigiosi – in ambito famigliare o afferenti ai rapporti di vicinato (cfr., ad es., provv. 18 dicembre 2025, n. 758, doc. web n. 10211207) – talvolta con connotazioni suscettibili di avere rilevanza penale, dovuti alle ragioni più varie, rispetto ai quali marginali sono le ragioni di ricorso al Garante (se non talora puramente strumentali) e i profili rispetto ai quali l'Autorità è tenuta a pronunciarsi.

I contenuti di segnalazioni e reclami

I profili oggetto di lamentela sono per lo più ricorrenti (e già da tempo presi in considerazione dal Garante, nel provvedimento generale dell'8 aprile 2010 in materia di videosorveglianza, doc. web n. 1712680, e in tempi successivi all'adozione del Regolamento, dal Comitato europeo, con le linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video): l'orientamento degli apparati di ripresa (quanto meno apparente) ovvero l'installazione di apparati mobili, anche grazie a sensori negli stessi incorporati, sprovvisti di idonei accorgimenti volti a inibire le riprese indebite (quali calotte o pannelli opportunamente installati) e, più in generale, già la sola presenza degli stessi nelle prossimità (in particolare) di luoghi di abitazione civile costituiscono i fattori di lamentela assolutamente prevalenti. Tale circostanza è ulteriormente acuita dal fatto che i più recenti apparati di ripresa rendono oltremodo difficile per l'osservatore esterno comprendere su quali spazi insistano le riprese (si pensi alle telecamere cd. "a bulbo" o a parete dotati di protezione esterna). Altri profili di criticità abitualmente segnalati sono la possibile captazione sonora (già in passato oggetto provvedimenti sanzionatori: cfr. provv. 12 ottobre 2023, n. 477, doc. web n. 9949494); l'assenza di informativa (o la sua inidoneità in ragione di elementi minimi della stessa, a partire dall'identità e dai dati di contatto del titolare del trattamento); la visione (anche) notturna; l'alterità delle finalità (reali) perseguite dal titolare del trattamento rispetto a quelle (talora) dichiarate (solitamente, genericamente riconducibili alla sicurezza o alla tutela del patrimonio); l'assenza di idonei presupposti di liceità del trattamento, in particolare in contesti nei quali operano anche lavoratori (con l'inosservanza delle garanzie previste dallo Statuto dei lavoratori); i tempi di conservazione dei dati memorizzati.

Le difficoltà negli accertamenti

In termini generali, rispetto al fenomeno della videosorveglianza solo in rare occasioni la richiesta di intervento al Garante è accompagnata da elementi tali da offrire prova di una violazione attuale, in considerazione dell'indisponibilità di *frame* video da parte del soggetto che lamenta l'illecito trattamento mediante gli apparati di ripresa. Al contrario, di regola è solo affermata l'esistenza di apparati di ripresa (più o meno tecnologicamente avanzati) asseritamente lesivi di diritti individuali (come si è detto in ragione della loro collocazione e angolatura apparente), non di rado accompagnata da materiale documentale

(per lo più fotografie degli apparati di ripresa), senza che però ciò consenta di accertare, anzitutto, se i trattamenti siano effettivamente realizzati e, in seconda battuta, quali siano le aree effettivamente oggetto di ripresa.

Nel contesto in esame si presenta quindi particolarmente difficoltosa per l'Autorità l'acquisizione di elementi di prova volti a definire con certezza le circostanze di fatto dell'impiego degli apparati di ripresa in assenza di accertamenti *in loco*. Accertamenti che non possono realisticamente essere effettuati per ciascuno dei casi portati all'attenzione del Garante, posta la loro numerosità oltre che in ragione delle risorse a disposizione dell'Autorità. In termini generali (cfr. cap. 18), le verifiche sono effettuate, con riguardo alla complessiva azione del Garante, secondo criteri di priorità e proporzionalità che tengano conto della gravità dei fatti segnalati e del rischio concreto di violazione dei diritti delle persone.

Peraltro, nel settore specifico qui considerato, l'esperienza ha evidenziato l'estrema facilità nel modificare, in ogni momento (talvolta anche in tempi immediatamente successivi alle verifiche), il funzionamento ed orientamento di apparati di ripresa (semplicemente spostandone temporaneamente l'angolatura o utilizzando forme più evolute di apparati di ripresa in grado, mediante comandi impartiti da remoto, di modificare il proprio angolo di ripresa).

La risposta dell'Autorità

In presenza della realtà così descritta, la risposta dell'Autorità – necessariamente ispirata ad un approccio graduato – muove dai (e si articola intorno ai) compiti che l'art. 57 del RGPD attribuisce (in generale) alle autorità di protezione dei dati. Tra questi, i primi a venire in gioco sono quelli identificati all'art. 57, par. 1, rispettivamente alle lett. b) e d), RGPD. Ciò implica, nel settore qui in esame, che in presenza di segnalazioni o reclami in relazione ai quali non risultino sufficientemente comprovate violazioni della disciplina di protezione dei dati personali, l'Autorità provvede, quale primo passo, a inviare una comunicazione al segnalante (o al reclamante) volta a rappresentare la cornice normativa di riferimento; in pari tempo una comunicazione dettagliata è inviata al soggetto che, in base a quanto segnalato, fa uso del sistema di videosorveglianza (potenzialmente in qualità di titolare del trattamento), asseritamente in violazione della disciplina di protezione dei dati, per renderlo pienamente consapevole della necessità dello scrupoloso rispetto degli obblighi imposti dal Regolamento, con contestuale invito a fornire conferma di ciò al Garante.

Operando in questo modo, anche in ossequio al principio di semplicità ed economicità dell'azione amministrativa, vengono poste le premesse per assicurare che, con la spontanea cooperazione delle parti, l'eventuale trattamento abbia luogo nel rispetto della vigente cornice normativa.

Tuttavia, la risposta del Garante, in base alle evidenze a disposizione, non può che muovere anche dal compito che il RGPD affida alle autorità di controllo le quali sono chiamate a sorvegliare e assicurare l'applicazione della disciplina di protezione dei dati personali. In questa prospettiva, il Garante, in continuità con gli orientamenti già consolidati, ha adottato nel corso dell'anno una pluralità di provvedimenti sanzionatori, per lo più rivolti a operatori economici e, occasionalmente, a soggetti privati.

Violazioni più ricorrenti

I profili di violazione più ricorrenti circa i trattamenti di dati personali effettuati mediante i sistemi di videosorveglianza riguardano il principio di trasparenza (di cui agli artt. 5, par. 1, lett. a) e 13 del RGPD), a causa del mancato (o dell'inidoneo) adempimento dell'obbligo di fornire agli interessati un'idonea informativa, anche nelle forme semplificate (e ormai note alla collettività) del cartello segnaletico (cfr. provv.ti 16 gennaio 2025, n. 9, doc. web n. 10136889; 13 febbraio 2025, n. 64, doc. web n. 10138728; 27 febbraio 2025, n. 97, doc. web n. 10143908; 13 marzo 2025, n. 137, doc. web n. 10137429; 4 giugno 2025, n. 332, doc. web n. 10167594; 17

luglio 2025, n. 429, doc. web n. 10175221; 17 luglio 2025, n. 432, doc. web n. 10176090; 17 luglio 2025, n. 433, doc. web n. 10176106; 11 settembre 2025, n. 491, doc. web n. 10183218; 23 ottobre 2025, n. 650, doc. web n. 10200460), nonché i principi di liceità del trattamento, pertinenza, e limitazione nella raccolta dei dati rispetto alle finalità perseguite (minimizzazione dei dati), posto che non di rado le riprese effettuate riguardano aree che non sono di pertinenza esclusiva del titolare del trattamento investendo, infatti, spazi pubblici (quali strade e piazze), aree comuni o condominiali, spazi di pertinenza di terzi (quali balconi, accessi alle abitazioni e giardini: cfr. provv. 13 marzo 2025, n. 136, doc. web n. 10127915) ovvero aree di accesso a locali commerciali di terzi (provv.ti 27 marzo 2025, n. 172, doc. web n. 10167265; 13 febbraio 2025, n. 65, doc. web n. 10136966; 17 luglio 2025, n. 431, doc. web n. 10175329; 17 luglio 2025, n. 433, cit.).

Videosorveglianza da parte di persone fisiche

Come è noto, i trattamenti effettuati per l'esercizio di attività a carattere esclusivamente personale o domestico sono esclusi dall'ambito di applicazione materiale delle disposizioni in materia di protezione dati ai sensi dell'art. 2, par. 1, lett. c), RGPD. Tale esenzione non trova tuttavia applicazione, con conseguente applicazione del RGPD e del Codice, nei casi in cui ricorra l'utilizzo di un sistema di videocamera installato da una persona fisica sulla sua abitazione familiare per proteggere i beni, la salute e la vita dei proprietari dell'abitazione, ove il sistema sorvegli parimenti lo spazio pubblico e, più in generale, aree che non siano di pertinenza esclusiva del titolare del trattamento (v. al riguardo la sentenza della Corte di giustizia, Quarta Sezione), 11 dicembre 2014, causa C 212/13, Ryneš).

In questa prospettiva numerose sono le segnalazioni suscettibili di rientrare nell'ambito di applicazione della disciplina di protezione dei dati. Non sono mancati provvedimenti del Garante aventi ad oggetto fattispecie nelle quali persone fisiche risultavano estendere (oltre misura) le aree oggetto di ripresa, interessando spazi pubblici (o privati), ben al di là delle aree di rispettiva pertinenza, ovvero ambiti condominiali o vie di accesso ad essi o riprendendo abitazioni private, potendo così indebitamente monitorare i movimenti, rispettivamente, dei consociati o di altri condomini, in assenza di basi giuridiche che consentano tale attività (cfr., ad es., provv. 23 ottobre 2025, n. 727, doc. web n. 10210749). Una vicenda peculiare ha visto l'intervento del Garante (su segnalazione dei Carabinieri) con riguardo a trattamenti, effettuati da parte di un soggetto privato – cui la legge non attribuisce alcuna funzione di vigilanza –, in violazione del principio di liceità e di correttezza (art. 5, par. 1, lett. a), RGPD), in uno spazio pubblico nel quale si sarebbe svolta una sagra con modalità clandestine, stante la peculiare dislocazione e la dissimulazione degli apparati di ripresa in prossimità dell'area interessata (cfr. provv. 11 settembre 2025, n. 577, doc. web n. 10184252).

Il coinvolgimento delle realtà associative

Considerando che non di rado i fatti segnalati o oggetto di accertamento hanno luogo all'interno e nelle prossimità degli esercizi commerciali, il Garante – per il tramite di una comunicazione indirizzata al Presidente di Confcommercio-Imprese per l'Italia – ha rappresentato le criticità rilevate, segnalando i rischi di impieghi impropri dei sistemi di videosorveglianza, in particolare in relazione ai negozi di prossimità e alle imprese del commercio di piccole dimensioni, al fine di avviare forme di collaborazione efficaci e sensibilizzare gli associati a prevenirne gli abusi (cfr. Newsletter 1° agosto 2025, doc. web n. 10153922). Nel riscontro pervenuto al Garante il 4 agosto 2025, pur venendo manifestate persistenti preoccupazioni rispetto a fenomeni di macro e micro criminalità cui le attività del terziario di mercato sono costantemente esposte, sì che la videosorveglianza viene ritenuta uno strumento utile quantomeno ai fini dello svolgimento di indagini, è stato ribadito l'impegno di Confcommercio "a continuare a diffondere, presso le proprie articolazioni territoriali e le

Federazioni nazionali, sia il quadro delle regole che sovrintendono all'uso dei sistemi di videosorveglianza, che gli strumenti divulgativi messi a disposizione dall'Autorità".

Infine, alla luce dei casi segnalati all'Autorità (taluni dei quali già oggetto di decisione (provv.ti 4 giugno 2025, n. 331, doc. web n. 10167242; 17 luglio 2025, n. 430, doc. web n. 10175293), merita di essere evidenziata con particolare preoccupazione, oltre a fattispecie nelle quali il titolare del trattamento ha espressamente dichiarato di utilizzare il sistema di videosorveglianza per controllare l'attività dei lavoratori (cfr. provv. 11 settembre 2025, n. 493, doc. web n. 10183820), la recrudescenza di un fenomeno che interessa in particolare gli esercizi commerciali di piccole dimensioni, attività di vicinato o artigianali. Si tratta dell'utilizzo di sistemi di ripresa, anche durante l'orario di apertura dell'esercizio commerciale – nei quali di regola non sono presenti beni di valore significativo, – idonei a monitorare costantemente tutti gli spazi interni da remoto (mediante app installate sui telefoni cellulari del titolare, nei casi esaminati di regola non presente nei locali commerciali). Tali modalità di trattamento lasciano intendere un utilizzo degli strumenti di videosorveglianza da parte del datore di lavoro preordinato al controllo a distanza dell'attività del lavoratore in violazione dell'art. 4, l. n. 300/1970 (richiamato dall'art. 114 del d.lgs. n. 196/2003) e tale da incidere pesantemente sulla libertà e sulla dignità delle persone.

Controllo a distanza dei lavoratori

Su questi ambiti, già oggetto di intervento nell'anno preso in considerazione (cfr. provv.ti 30 gennaio 2025, n. 38, doc. web n. 10111962; 27 marzo 2025, n. 173, doc. web n. 10196838; 17 luglio 2025, n. 433, cit.; 4 agosto 2025, n. 457, doc. web n. 10174466; 11 settembre 2025, n. 492, doc. web n. 10183236; 18 dicembre 2025, n. 757, doc. web n. 10211799), anche grazie alla collaborazione con altri organi dello Stato e delle amministrazioni locali, l'Autorità continuerà a mantenere una costante vigilanza.

15.4. *Trattamento di dati personali da parte di liberi professionisti*

Le istanze, in particolar modo segnalazioni e reclami, relative al trattamento dei dati personali da parte dei liberi professionisti hanno riguardato la verifica della corretta applicazione dei principi di liceità, in correlazione alla sussistenza di una idonea base giuridica (art. 5, par. 1, lett. a) e 6 del RGPD), e di correttezza (artt. 5, par. 1, lett. a), RGPD) del trattamento.

Le istruttorie hanno valutato la fondatezza di un presupposto di liceità considerando il rispetto del principio di liceità nella sua duplice declinazione, intesa sia quale riconducibilità del trattamento ad una valida base giuridica, sia come effettiva aderenza dello stesso all'intero quadro di garanzie introdotto dal RGPD, al fine di verificare che ogni trattamento sia effettuato in modo lecito, corretto e trasparente ed effettivamente idoneo a tutelare i diritti degli interessati.

In tale ambito, il Garante ha adottato un provvedimento sanzionatorio in relazione alla divulgazione, mediante l'invio ad una casella PEC di natura istituzionale ad accesso condiviso, di informazioni relative a vicende professionali della reclamante. Tale comunicazione risultava sprovvista di alcuna delle basi giuridiche di cui all'art. 6 del RGPD. Nella vicenda considerata si è ritenuto altresì violato il principio di correttezza nel trattamento (art. 5, par. 1, lett. a), RGPD), valutata la concreta possibilità di effettuare la comunicazione con modalità tali da prevenire l'indebita conoscenza di vicende interpersonali (indipendentemente dalla fondatezza delle stesse) in alcun modo correlate con la sfera professionale della reclamante né alla funzione pubblica dell'account di posta elettronica utilizzato (provv. 18 dicembre 2025, n. 759, doc. web n. 10210431). Merita inoltre segnalare che nel caso di specie ha formato oggetto di censura anche il mancato riscontro alla richiesta di informazioni,

15

formulata ai sensi dell'art. 157 del Codice, indirizzata alla professionista titolare del trattamento, condotta sanzionabile ai sensi dell'art. 166 del Codice (profilo già oggetto di conferma da parte di Cass., sez. II civ., ord. 12 giugno 2018, n. 15332).

Inoltre, il Garante ha adottato un provvedimento di ammonimento nei confronti di due avvocati per avere effettuato alcune operazioni di trattamento riferite alla registrazione di una conversazione in violazione della disciplina in materia di protezione dei dati personali; in particolare, uno degli avvocati aveva trasmesso la registrazione della conversazione che il proprio cliente aveva avuto con il reclamante all'avvocato di due società, il quale l'aveva usata nell'ambito della procedura di opposizione alla omologazione del concordato preventivo della società di cui il reclamante era amministratore unico.

L'opposizione alla omologazione di concordato preventivo ex art. 180 legge fallimentare era stata presentata dalle società e da altri soggetti tra i quali, però, non rientrava la persona che aveva preso parte alla conversazione registrata, seppure creditore della società parte della procedura di opposizione.

Con il provvedimento è stato precisato che l'istruttoria, effettuata a seguito della presentazione del reclamo, non aveva preso in considerazione il trattamento relativo alla produzione in giudizio della registrazione della conversazione predetta in quanto in proposito trova applicazione l'art. 160-*bis* del Codice.

Il procedimento amministrativo e il provvedimento hanno avuto per oggetto il trattamento posto in essere nella fase precedente alla produzione in giudizio della registrazione, consistente nella consegna della registrazione in questione da parte di uno degli avvocati e nella conseguente ricezione della registrazione da parte dell'altro avvocato che l'aveva espressamente richiesta.

Ritenute prive di fondamento le obiezioni procedurali sollevate in sede istruttoria, l'Autorità ha accertato che gli avvocati avevano agito come titolari del trattamento, nello svolgimento dell'attività difensiva, e che le condotte da loro poste in essere erano state effettuate in concorso ex art. 5, l. n. 679/1981.

In particolare è stato accertato che il trattamento era stato effettuato in assenza di una idonea condizione di liceità del trattamento e in violazione di quanto prescritto dagli artt. 5, par. 1, lett. a), e 6 del RGPD. In conformità a consolidato orientamento giurisprudenziale, la registrazione di conversazione tra presenti è pienamente legittima a condizione che la stessa sia effettuata da uno degli interlocutori, per finalità di difesa di un proprio diritto in giudizio e sempre che tale registrazione non sia destinata alla diffusione o alla comunicazione sistematica (v. Cass. pen. 8 giugno 1999, n. 7239; Cass. pen. 16 marzo 2011, n. 31342; Cass. pen., sez. III, 13 maggio 2011, n. 18908; Cass. pen., sez. III, 3 ottobre 2012, n. 43898; Cass. pen. 8 marzo 2024, n. 10079).

La *ratio* della legittimità della registrazione di cui sopra si basa, a detta della stessa Corte di cassazione, sulla circostanza che "chi conversa accetta il rischio che la conversazione sia documentata mediante registrazione", fermo restando che la comunicazione della suddetta registrazione può comportare la violazione del diritto alla protezione dei dati personali se effettuata per scopi diversi "dalla tutela di un diritto proprio o altrui" (v. Cass. pen, cit., n. 18908/2011; confermata anche da Cass. pen., 10 giugno 2016, n. 24288).

In base agli accertamenti condotti dall'Autorità è risultata evidente l'insussistenza, nel caso di specie, dei presupposti che la giurisprudenza ritiene necessari affinché sia legittima la produzione in giudizio della registrazione di una conversazione, in quanto la registrazione era stata prodotta in giudizio da un soggetto diverso rispetto ai presenti alla conversazione e in un procedimento (opposizione all'omologazione) del quale il partecipante alla conversazione non era parte.

L'Autorità ha accertato, inoltre, la violazione del principio di correttezza (provv. 27 novembre 2025, n. 705, doc. web n. 10213452).

16 Intelligenza artificiale e diritto alla protezione dei dati personali

16.1. *L'evoluzione della cornice regolatoria*

Anche il 2025 è stato caratterizzato da una significativa evoluzione della cornice regolatoria in materia di intelligenza artificiale (IA) che, a tutt'oggi, pur definita nelle sue linee portanti, non può tuttavia ancora considerarsi né pienamente operativa, né (sufficientemente) stabilizzata, sia al livello europeo che a livello nazionale.

Reg. IA

Nell'ambito del panorama normativo europeo, occorre innanzitutto ricordare che nel corso dell'anno d'interesse il reg. (UE) 2024/1689 sull'IA del 13 giugno 2024 (il cd. AI Act) – i cui tratti essenziali sono stati già delineati nelle precedenti Relazioni (Relazione 2023, p. 187 e Relazione 2024, p. 178) – ha trovato una (sia pur parziale) applicazione e sono stati adottati rilevanti provvedimenti attuativi dello stesso regolamento da parte della Commissione europea. Esaminando più nel dettaglio le prescrizioni del reg. IA divenute applicabili nel 2025 (e, quindi, pienamente vincolanti) si ricordano, per quanto d'interesse: le "Disposizioni Generali" (Capo I) che includono le "Definizioni" afferenti ai sistemi di IA (art. 3) – integrate, sul piano interpretativo, dagli "Orientamenti della Commissione sulla definizione di sistema di intelligenza artificiale stabilita dal reg. (UE) 2024/1689 (reg. sull'IA)", Bruxelles, 29 luglio 2025 C(2025) 5053 –; le "Pratiche di IA vietate" (Capo II), disciplinate dall'art. 5 (e meglio illustrate dagli "Orientamenti della Commissione relativi alle pratiche di intelligenza artificiale vietate ai sensi del reg. (UE) 2024/1689 (reg. sull'IA)" rilasciati dalla Commissione UE il 29 luglio 2025, C(2025) 5052); le disposizioni in materia di "Modelli di IA per finalità generali" ("GPAI"), in riferimento alle quali la Commissione ha pubblicato, il 10 luglio 2025, un "*Code of Practice*" per cui è prevista l'adesione volontaria; le prescrizioni in materia di *governance* (di cui agli artt. 70 e ss.).

Pacchetto Omnibus digitale

In parallelo a questa attività di supporto alla graduale applicazione del reg. IA, la Commissione ha poi presentato anche due proposte di regolamento finalizzate alla parziale modifica di diversi provvedimenti nel settore digitale, tra cui il Regolamento (UE) 2016/679 e lo stesso reg. IA: si tratta della Proposta del 19 novembre 2025, COM(2025) 837 *final*, 2025/0360 (COD), il cd. Omnibus digitale, e della Proposta del 19 novembre 2025, COM(2025) 836 *final*, 2025/0359 (COD), il cd. Omnibus digitale sull'IA (cfr. cap. 20 per approfondimenti in materia).

La legge n. 132/2025 sull'IA

Il contesto nazionale è stato caratterizzato dall'approvazione della l. 23 settembre 2025, n. 132 "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", oltre che dall'adozione delle prime linee guida in materia di utilizzo di sistemi di IA da parte di alcune p.a. centrali. Il testo normativo approvato dal Parlamento in via definitiva corrisponde, salva qualche modifica, all'impianto generale del disegno di legge A.S. 1146 sul quale, come già indicato nella precedente Relazione (p. 179), il

16

Garante ha fornito il proprio contributo anche in sede di audizione parlamentare. Al riguardo, nonostante la chiara previsione contenuta nell'art. 74, par. 8, reg. IA – evocata sia dal CEPD, sia, più puntualmente con riguardo alla realtà nazionale, dal Garante (v. nell'anno preso in esame l'audizione del Presidente del Garante tenutasi alla Camera dei deputati, Commissioni IX e X riunite il 7 maggio 2025, doc. web n. 10129226) –, in sede legislativa è risultato confermato lo scostamento dell'ordinamento nazionale (v. già Relazione 2024, p. 35); la disciplina nazionale, infatti, non ha attribuito né al Garante né ad altro soggetto dotato di equivalente requisito di indipendenza, il ruolo di autorità di vigilanza del mercato con riguardo, segnatamente, ai sistemi di IA di cui all'all. III reg. IA, ai numeri 1, 6, 7 ed 8: si tratta, in chiave sintetica, dei sistemi biometrici, in particolare dei sistemi di identificazione biometrica remota, dei sistemi di IA impiegati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti basati sulla deduzione di tali attributi o caratteristiche e dei sistemi di IA suscettibili di essere utilizzati per il riconoscimento delle emozioni (n. 1); di alcuni sistemi di IA suscettibili di essere utilizzati dalle autorità di contrasto (nel dettaglio individuati al n. 6); di alcuni sistemi di IA suscettibili di essere utilizzati dalle autorità pubbliche competenti (o per loro conto) in relazione alle materie della migrazione, asilo e gestione del controllo delle frontiere (nel dettaglio individuati al n. 7); infine, dei sistemi di IA che possono essere utilizzati nell'amministrazione della giustizia, ovvero nell'ambito dei processi democratici nonché dei sistemi di IA destinati a essere utilizzati per influenzare l'esito di un'elezione o di un referendum o il comportamento di voto delle persone fisiche (n. 8). Sistemi che, come è agevole intendere, tra quelli ad alto rischio, in modo più marcato sono suscettibili di incidere sui diritti fondamentali delle persone oltre che su interessi di natura generale connessi alla democraticità dell'ordinamento, ragioni per le quali il legislatore europeo richiede un più marcato livello di indipendenza delle autorità di vigilanza.

Con riguardo poi ai profili di *governance*, di particolare rilievo sia per assicurare la reciproca cooperazione tra le varie autorità di vigilanza e (nelle forme e nei casi previsti dal reg. IA) le autorità di tutela dei diritti fondamentali (cfr. art. 77 reg. IA), l'art. 20, l. n. 132/2025 prevede, con formulazione generale, che "le Autorità nazionali per l'intelligenza artificiale di cui al comma 1 assicurano il coordinamento e la collaborazione con le altre pubbliche amministrazioni e le autorità indipendenti, nonché ogni opportuno raccordo tra loro per l'esercizio delle funzioni di cui al presente articolo". La disposizione aggiunge che "a quest'ultimo fine, presso la Presidenza del Consiglio dei ministri è istituito un Comitato di coordinamento, composto dai direttori generali delle due citate Agenzie e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri medesima. Al suddetto Comitato partecipano, quando si trattano questioni di rispettiva competenza, rappresentanti di vertice della Banca d'Italia, della CONSOB e dell'IVASS [...]».

Anche da questo punto di vista deve rilevarsi la mancata previsione di forme di partecipazione delle autorità di tutela dei diritti fondamentali e, tra queste, del Garante ed è auspicabile che, in sede di attuazione della disciplina nazionale in materia di IA, demandata alla futura approvazione di diversi decreti attuativi, possano essere introdotte le opportune misure per agevolare la cooperazione tra le varie autorità coinvolte nell'articolata cornice di *governance* (cfr. al riguardo gli artt. 9, 20 comma 3 e art. 24, l. n. 132/2025), dando compiuta attuazione alle previsioni contenute nel reg. IA, valorizzando il principio di leale collaborazione cui, proprio nell'ambito dell'economia digitale, la stessa Corte di giustizia in tempi recenti è tornata a fare riferimento (cfr. sentenza 4 luglio 2023, causa C-252/21, Meta).

16.2. *Le iniziative a livello sovranazionale per l'IA*

Come evidenziato in precedenti Relazioni, la crescente diffusione di iniziative che prevedono lo sviluppo o l'utilizzo di tecnologie riconducibili alla macrocategoria dell'IA rende sempre più evidente l'importanza del ricorso a principi (per quanto possibile) condivisi in ambito internazionale. Anche nel 2025, quindi, muovendo dalla considerazione che in molti casi i sistemi di IA prevedono il trattamento di dati personali, in fase di sviluppo o di successivo utilizzo, l'Autorità (nelle sue varie articolazioni) ha preso parte a numerose iniziative, partecipando a tavoli di lavoro di respiro sovranazionale.

CEPD

L'Autorità ha continuato ad assicurare una piena collaborazione nella partecipazione all'elaborazione di documenti in seno al CEPD in materia di IA: fra le attività svolte, vanno menzionate, per complessità e per impegno richiesto, quelli finalizzati al chiarimento delle aree di sovrapposizione e interrelazione tra il RGPD e il reg. IA, oltre che quelli afferenti le prime osservazioni del CEPD in merito alle due proposte avanzate dalla Commissione UE per la semplificazione di diversi provvedimenti normativi in materia di digitale, tra cui come detto il RGPD e il reg. IA (il cd. Pacchetto Digital Omnibus su menzionato) (cfr. par. 20.1).

CoE

Quanto alla cornice internazionale, anche nel corso del 2025, d'intesa con il Ministero degli affari esteri e della cooperazione internazionale nonché della Rappresentanza permanente d'Italia presso il Consiglio d'Europa a Strasburgo, l'Autorità ha assicurato, attraverso un proprio rappresentante, il suo contributo sia ai lavori del *Committee on Artificial Intelligence* (CAI) – che nel 2025 ha esaurito il proprio mandato, e il cui testimone verrà raccolto dallo *Steering Committee for New and Emerging Digital Technologies* (CDNET), in relazione al quale pure l'Autorità continuerà ad assicurare la propria collaborazione –, sia, con precipuo riferimento alle implicazioni derivanti dalle tecnologie IA sulle regole democratiche, allo *Steering committee on Democracy* (CDDEM).

Con particolare riferimento al CAI merita segnalare che – dopo aver portato a termine i lavori relativi alla Convenzione quadro ed aver focalizzato la propria attenzione nell'elaborazione di una Metodologia (denominata "*Human Rights, Democracy, and the Rule of Law Impact Assessment for AI Systems*", HUDERIA *Methodology*) suscettibile di essere tenuta in considerazione per valutare l'impatto derivante dall'impiego di sistemi di IA, ed approvata dal Comitato dei ministri il 26 febbraio 2025 – nel corso dell'anno ha messo a punto un Modello (anch'esso approvato Comitato dei ministri il 25 febbraio 2026), vale a dire uno strumento flessibile, applicabile ai diversi elementi o fasi del processo di valutazione (anche secondo modalità "scalabili") volto a facilitare la realizzazione della valutazione d'impatto (anche raccogliendo materiali di supporto e risorse a tal fine utilizzabili). Sviluppata nelle sue due componenti (Metodologia e Modello) grazie alla partecipazione all'interno del CAI di governi, industria e società civile, HUDERIA mira a fornire supporto ai team di progetto sull'IA nella valutazione e nella gestione dei rischi per i diritti umani, la democrazia e lo stato di diritto. Entro questa cornice, nel giugno 2025, personale del Garante ha partecipato ad un'iniziativa del Consiglio d'Europa, denominata "HUDERIA *Academy*", nel corso della quale è stato illustrato nel dettaglio il Modello HUDERIA e fornita ai partecipanti (di diversa formazione e provenienza geografica) l'opportunità di testarlo concretamente applicandolo ad un "caso d'uso", in confronto tra loro e con l'ausilio e la supervisione degli esperti dell'Alan Turing Institute (dall'inizio parte attiva nel progetto).

Nell'ambito dello *Steering Committee on Democracy* (CDDEM), riunitosi in plenaria

OCSE

in due occasioni nel corso del 2025, è stato presentato uno studio interdisciplinare volto ad esaminare i vantaggi e i rischi che, in particolare l'IA generativa (GenAI), comporta per i processi democratici, con particolare attenzione al dibattito pubblico (e al discorso sulle *fake news*), alle elezioni e ai media.

L'Autorità ha assicurato la presenza di suoi rappresentanti anche su altri tavoli di lavoro internazionali, ed in particolare nell'ambito del Gruppo di esperti OCSE su "*AI, data governance and privacy*", prendendo parte all'*High-Level Roundtable* su *"International Data Governance and Privacy in the Age of Artificial Intelligence*" e a quella su "*Trustworthy and Accountable Data Governance in the Age of AI*", nonché ai periodici incontri del gruppo di esperti "*AI, Data, and Privacy*". Anche all'esito di questi scambi, OECD ha curato nel mese ottobre la pubblicazione dell'*Artificial Intelligence Paper* No. 48, intitolato "*Mapping relevant data collection mechanisms for AI training*" (cfr. par. 20.3.3).

G7 delle autorità privacy

Anche in occasione della *G7 Roundtable of Privacy and Data Protection Authorities*, cui il Garante ha preso parte e tenutosi in Canada nel giugno 2025, il tema dell'IA ha continuato a formare oggetto di trattazione, con l'adozione del "*G7 Leaders' Statement on AI for Prosperity*" nella più ampia cornice delle nuove tecnologie emergenti oggetto del documento intitolato "*Championing privacy in a digital age: Collective action today for a trusted tomorrow*", nel quale ci si è soffermati sulle implicazioni, sulla centralità delle autorità di protezione dati in tale ambito e sull'importanza del loro allineamento e stretta collaborazione nella prospettiva di garantire un'effettiva tutela della protezione dei dati personali e dei diritti fondamentali degli individui nelle diverse giurisdizioni nazionali (cfr. par. 20.3.2).

16.3. *Attività del Garante*

Nel corso dell'anno si è registrato un incremento delle richieste di supporto – soprattutto da parte di p.a. – nell'ambito di progetti di sviluppo o di utilizzo di sistemi di IA. Questa attività, caratterizzata da una proficua e leale collaborazione oltre che da un importante momento di confronto in merito alle sfide dell'IA, si è conclusa con il rilascio di alcuni pareri da parte del Garante e, in taluni casi, anche con l'adozione di provvedimenti di natura sanzionatoria (cfr. ad es. provv. 10 aprile 2025, n. 202, doc. web n. 10140338, in relazione all'impiego di un sistema di IA per raccogliere ad analizzare dati relativi alla mobilità nel traffico cittadino con rilevazioni effettuate su campo - cfr. par. 4.11). In questo panorama di particolare interesse, in quanto costituisce uno dei primi esempi di documento di indirizzo da parte di un'amministrazione centrale verso le sue articolazioni periferiche, sono le "linee guida per l'introduzione dell'intelligenza artificiale nelle istituzioni scolastiche" rilasciate dal Ministero dell'istruzione e del merito. Il documento (in uno al decreto ministeriale di cui le stesse linee guida costituivano un allegato), adottato nella versione definitiva dal Ministero all'esito di diverse consultazioni preliminari con il Garante, è stato poi oggetto di una complessiva valutazione positiva (provv. 4 agosto 2025, n. 454, doc. web n. 10162698, cfr. par. 4.3). Tale provvedimento è stato poi menzionato anche nell'aggiornamento del Vademecum sulla scuola del Garante "La scuola a prova di privacy" (Newsletter 27 novembre 2025, doc. web n. 10193417).

Analoghi tavoli di confronto con altre amministrazioni sono attualmente in corso.

Chatbot

Con riguardo all'attività di *enforcement*, in continuità con gli interventi segnalati nella precedente Relazione, si segnala in particolar modo l'adozione di un provvedimento di limitazione definitiva del trattamento nel settore delle *chatbot* inizialmente accessibile, anche da utenti italiani, attraverso i principali app store (provv. 30 gennaio 2025, n. 33, doc. web doc. web n. 10098477, cfr. par. 12.2).

Nudification app

Con altro provvedimento di limitazione provvisoria il Garante è intervenuto nei confronti del gestore di un sito, stabilito in un paese terzo (e che non ha preso parte all'istruttoria), che fornisce un servizio di AI generativa di cd. *deep nude* che consente all'utente, previo *upload* nel proprio account di fotografie di persone vestite, di generare risultati realistici, in forma di immagine, riguardanti le medesime persone private, prive degli indumenti, ovvero di generare ulteriori alterazioni delle immagini, in base alle diverse funzionalità del servizio fornito (provv. 1° ottobre 2025, n. 574, doc. web n. 10174164, cfr. par. 12.2).

Deepfake

Con particolare preoccupazione l'Autorità osserva la diffusione sul mercato di numerosi servizi che consentono agli utenti di utilizzare la voce o le immagini anche di terze persone – personaggi noti e non – per la generazione di contenuti audio, fotografici e/o audiovisivi basati su tali voci o immagini con modalità tali da ledere il diritto all'identità personale o alla protezione dei dati personali delle persone fisiche cui l'*output* prodotto da questi sistemi sia riferibile (deepfake). Al fine di prevenire lesioni (anche gravi) delle situazioni giuridiche soggettive protette dal diritto alla protezione dei dati personali, il Garante, nell'adottare un avvertimento di natura generale, ha evidenziato la necessità che i fornitori dei servizi di generazione di contenuti artificiali basati sull'utilizzo di voci o immagini di terzi, sin dalla fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere tali funzioni, tengano conto del diritto alla protezione dei dati (provv. 18 dicembre 2025, n. 78, doc. web n. 10207132, cfr. par. 12.2).

***Training* degli algoritmi e diritto di opposizione**

Nel dare eco all'annuncio di una piattaforma social dell'intenzione di utilizzare i dati contenuti nei post pubblici degli utenti maggiorenni e quelli derivanti dall'utilizzo dei propri servizi di IA per sviluppare e migliorare i propri servizi (quali *chatbot* e modelli linguistici), con un comunicato il Garante – in precedenza interessato da reclami nella stessa materia (cfr. provv.ti 13 novembre 2025, nn. 693 e 694, rispettivamente doc. web n. 10198751 e n. 10198779) – ha dato ulteriore diffusione alle modalità utilizzabili per opporsi a questo uso ulteriore per finalità di *training* degli algoritmi (comunicato 29 aprile 2025, doc. web n. 10125702, cfr. par. 12.2; v. anche le indicazioni fornite in ottobre 2025, doc. web n. 10183938).

CINI

È stata rinnovata a gennaio per un ulteriore triennio (2025-2027) la collaborazione tra il Garante e 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. All'interno di tale cornice, nell'autunno 2025 è stata organizzata un'attività formativa di complessive 30 ore, denominata "Avvicinamento all'intelligenza artificiale", destinata al personale dell'Autorità sulle tematiche connesse all'IA, differenziandone i contenuti in base ai profili dei partecipanti all'iniziativa (così distinguendo il personale operante in Autorità con prevalente formazione giuridica rispetto a quello con background informatico ed ingegneristico). A una lezione introduttiva sulle tecnologie dell'IA, ha fatto seguito (con cadenza tendenzialmente settimanale) la trattazione dei seguenti temi: apprendimento automatico, AI e Cybersecurity; elaborazione del linguaggio naturale; visione artificiale; robotica; gestione dei dati nei sistemi di IA; sicurezza dei modelli LLM; certificazione dei sistemi IA. L'auspicio è che tale forma di collaborazione, potendo fare affidamento su risorse aggiuntive, possa ulteriormente strutturarsi nel prossimo futuro.

17 Violazione dei dati personali

Dal 1° gennaio al 31 dicembre 2025 sono state notificate all'Autorità 2.415 violazioni dei dati personali ai sensi dell'art. 33 del RGPD o dell'art. 26 del d.lgs. n. 51/2018 (cfr. sez. IV, tab. 9) da parte di soggetti pubblici (21,3% dei casi) e privati (78,7% dei casi). Gran parte delle violazioni dei dati personali è stata notificata per fasi (circa il 62,1% dei casi) con l'invio, in un primo momento, di una notifica preliminare e, successivamente, di una o più notifiche integrative (cfr. sez. 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 società del settore assicurativo, bancario, energetico, sanitario, dei trasporti e delle telecomunicazioni, ma anche piccole e medie imprese e professionisti.

La maggior parte delle violazioni dei dati personali notificate ha riguardato la perdita di riservatezza e/o di disponibilità (anche solo temporanea) dei dati personali (circa il 90% dei casi; cfr. sez. 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.

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.

Provvedimenti correttivi adottati in via d'urgenza

In tale contesto, nell'ambito di un'istruttoria avente ad oggetto una rilevante violazione dei dati personali che ha comportato la perdita di riservatezza dei dati trattati da numerosi titolari che operano nel settore dei servizi di mobilità e di sosta (es. aziende e consorzi regionali che gestiscono il trasporto pubblico locale, enti locali che gestiscono aree di sosta a pagamento), l'Autorità è intervenuta adottando, in via d'urgenza, alcuni provvedimenti correttivi nei confronti di due società informatiche. In particolare, a fronte dell'acquisizione, da parte degli autori dell'attacco informatico, dei dati personali di circa 7,6 milioni di interessati (tra i quali, dati anagrafici e di contatto, credenziali di autenticazione, dati relativi alla fruizione di servizi di mobilità e di sosta), l'Autorità ha

rilevato l'inadeguatezza delle iniziative intraprese dalle due società per adempiere gli obblighi in materia di violazione dei dati personali e di sicurezza del trattamento che il RGPD pone in capo a titolari e responsabili del trattamento. Per tali ragioni, una società – che effettua trattamenti di dati in qualità sia di titolare che di responsabile – è stata destinataria di due provvedimenti correttivi, con i quali l'Autorità ha ingiunto, da un lato, di comunicare la violazione agli interessati e informare adeguatamente i titolari del trattamento coinvolti e, dall'altro, di adottare talune misure per attenuare i possibili effetti negativi della violazione (provv.ti 4 agosto 2025, n. 473, doc. web n. 10193088; 9 ottobre 2025, n. 612, doc. web n. 10193174). Analogamente, all'altra società – che effettua trattamenti di dati in qualità di responsabile o sub-responsabile – è stato ingiunto di informare adeguatamente i titolari del trattamento coinvolti e di adottare alcune misure per attenuare i possibili effetti negativi della violazione (provv. 4 agosto 2025, n. 472, doc. web n. 10193065).

Nei casi in cui è emersa 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, l'Autorità ha irrogato sanzioni amministrative pecuniarie. Per maggiori informazioni in merito, si fa rinvio ai parr. 4.8, 5.3.3 e 5.3.4 della presente Relazione.

18 L'attività ispettiva

18.1. *Considerazioni generali e collaborazione con la Guardia di finanza*

La mera comparazione dei dati statistici generali (relativi all'attività ispettiva svolta nel corso dell'anno 2025) con quelli concernenti la precedente annualità dimostra come tale attività si sia mantenuta sugli stessi livelli quantitativi. Anche nell'anno 2025 sono state effettuate complessivamente 130 attività ispettive *in loco*. Di queste 78 sono state curate direttamente dal competente dipartimento ispettivo e dalle altre articolazioni dell'Ufficio del Garante, mentre 52 attività sono state delegate al Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza. Gli accertamenti sono stati svolti tenuto conto degli ambiti di intervento individuati nelle due deliberazioni concernenti la programmazione semestrale dell'attività ispettiva adottate dal Garante (provv. 19 dicembre 2024, n. 808, doc. web n. 10100360 e provv. 4 agosto 2025, n. 451, doc. web n. 10165144).

Un esame più accurato dei dati consente però di svolgere qualche considerazione aggiuntiva.

È molto significativo constatare l'aumento degli interventi curati direttamente dall'Ufficio, pur a fronte dei diversi avvicendamenti effettuati nel corso dell'anno fra gli ispettori della Guardia di finanza operanti presso il Garante in posizione di fuori ruolo.

È sicuramente aumentata la capacità di programmazione dell'Ufficio e, soprattutto, si è consolidato il "gioco di squadra" che caratterizza ormai l'attività dei team ispettivi. Questi, infatti, sono stabilmente costituiti da ispettori dell'apposito dipartimento, funzionari del dipartimento giuridico specificamente interessato e da esperti informatici del servizio tecnologico del Garante per assicurare quelle competenze tecniche ormai imprescindibili anche negli accertamenti apparentemente più semplici. Questa composizione interdipartimentale richiede naturalmente un accurato lavoro di preparazione che inizia fin dal momento dell'elaborazione del programma ispettivo semestrale che, non a caso, nasce da un confronto serrato con i dirigenti dei dipartimenti dell'area giuridica.

Per quanto riguarda la ripartizione delle attività, quelle collegate a importanti istruttorie aperte presso i dipartimenti dell'area giuridica sono state curate direttamente dal dipartimento ispezioni. Le deleghe al Nucleo speciale della Guardia di finanza hanno riguardato, in particolare, lo svolgimento di attività di accertamento *in loco* volte ad effettuare notificazioni di atti e provvedimenti oppure l'acquisizione di informazioni e documenti mediante la redazione di appositi verbali di operazioni compiute.

Inoltre, in merito ai trattamenti di dati personali svolti da siti Internet di informazione locale, blog, ecc., risulta preziosa la collaborazione della Guardia di finanza, anche attraverso le articolazioni territoriali del Corpo, per una corretta identificazione e localizzazione dei relativi titolari del trattamento e, conseguentemente, per un'efficace

esecuzione degli eventuali provvedimenti prescrittivi dell'Autorità. Molto utile anche il lavoro di *back office* svolto dal Nucleo speciale che, su richiesta dell'Ufficio, fornisce report aggiornati sulla consistenza economica dei vari titolari del trattamento destinatari dei provvedimenti sanzionatori dell'Autorità, permettendo così una corretta quantificazione delle sanzioni da applicare.

18.2. *I principali ambiti di intervento*

Dal punto di vista della tipologia dei soggetti ispezionati, è facile constatare come gli accertamenti abbiano riguardato un amplissimo panorama di attività economiche ed un altrettanto vasto insieme di enti pubblici nazionali e locali, coprendo un arco di attività, procedimenti, situazioni che da soli evidenziano la pervasività dei trattamenti di dati personali e la vastità dei rischi cui gli stessi sono quotidianamente sottoposti.

In questa sede può essere opportuno soffermarsi su alcuni ambiti di intervento particolarmente significativi, peraltro oggetto di un'attenzione che non si è limitata all'anno 2025:

- violazioni di dati personali. Sotto questa denominazione, o sotto quella ormai entrata nel linguaggio comune di *data breach*, rientrano le numerose ispezioni svolte dall'Ufficio per approfondire e verificare alcuni dei casi di maggior rilievo segnalati al Garante (e spesso oggetto anche di attenzione da parte degli organi di stampa), sia in ragione della delicatezza dei dati trattati, sia in relazione al numero di interessati coinvolti. Da questo punto di vista, l'attenzione prioritaria è stata dedicata alle attività ispettive *in loco* condotte dalla cd. task force interdipartimentale che opera ormai da più di un anno per svolgere gli accertamenti sul preoccupante fenomeno dell'illecita acquisizione di informazioni provenienti dalle più grandi ed importanti banche di dati pubbliche (anagrafe tributaria, banche dati dell'INPS, delle forze di polizia, ecc.) (cfr. Relazione 2024, cap. 19 e par. 4.9.2). La grande quantità di informazioni e documenti acquisiti ha già permesso di individuare carenze dal punto di vista delle misure di sicurezza e prassi non adeguate dal punto di vista degli ambiti di azione degli operatori autorizzati. Un focus specifico è stato dedicato, in tutte le sessioni ispettive, alla tipologia ed al numero di persone autorizzate ad accedere alle varie banche dati soggette al controllo. Da queste verifiche sono a volte "germinati" ulteriori controlli *in loco* per ricostruire l'intera filiera dei trattamenti svolti ed identificare le "falle" da cui sono fuoriusciti i dati personali in questione;
- trattamento dei dati personali dei lavoratori. È un profilo che emerge da una pluralità di segnalazioni e reclami ed impone un'attività accurata di verifica per evitare, soprattutto, che le nuove tecnologie abbiano una ricaduta invasiva sui lavoratori in termini di controllo diretto o indiretto della loro attività, superando i limiti tracciati dalla legislazione vigente ed in particolare dal cd. Statuto dei lavoratori (l. n. 300/1970). Sono stati numerosi i controlli sul corretto utilizzo degli strumenti di videosorveglianza, ma a questi sempre più spesso si affiancano le verifiche sull'impiego di apparati informatici capaci di "seguire" o "monitorare" il lavoratore nelle varie fasi della sua prestazione lavorativa o strumenti per raccogliere ed incrociare (illecitamente) informazioni sulle opinioni, lo stato di salute o i rapporti interpersonali dei dipendenti. Si tratta di un ambito di intervento di estrema delicatezza che si sta recentemente confrontando anche con le sfide degli strumenti che cominciano ad utilizzare le potenzialità dell'intelligenza artificiale;
- telemarketing. Si tratta di uno dei campi di azione che hanno maggiormente impegnato l'Autorità nell'ultimo decennio. È un fenomeno che ha spinto il Garante a

18

promuovere un'ampia serie di iniziative a molteplici livelli (da quello normativo e regolamentare all'impegno nelle verifiche *in loco*). L'attenzione prioritaria si è concentrata sui diversi call center (individuati attraverso una previa attività di verifica cui ha attivamente partecipato la Guardia di finanza) che operano sulla base di estese banche dati illecitamente acquisite o comunque formate in spregio alla disciplina di protezione dei dati. Non sono mancati significativi risultati che hanno permesso di adottare rilevanti provvedimenti prescrittivi e sanzionatori di cui vi è traccia nelle apposite sezioni di questa stessa Relazione.

19 Il contenzioso giurisdizionale

19.1. *Considerazioni generali*

In applicazione del quadro normativo vigente, tutte le controversie che riguardano l'applicazione della disciplina in materia di protezione dei dati personali devono essere comunicate al Garante, anche se non sono relative all'impugnazione di provvedimenti dell'Autorità (art. 152 del d.lgs. n. 196/2003 e art. 10, comma 9, d.lgs. n. 150/2011, come modificato dall'art. 17 del d.lgs. n. 101/2018).

In relazione a tale incombente informativo, si registra, nel decorso anno un sensibile aumento rispetto al 2024: a fronte dei 101 nel 2023 e dei 74 ricorsi del 2024, nel 2025 è stata comunicata all'Autorità la pendenza di 89 ricorsi.

Permane, invece, non sempre puntualmente adempiuto l'altro obbligo, a carico delle cancellerie, di trasmettere al Garante copia dei provvedimenti emessi dall'autorità giudiziaria in materia di protezione dati e di criminalità informatica (art. 154, comma 6, del Codice).

Tali comunicazioni consentono all'Autorità di avere conoscenza dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e di segnalare al Parlamento e al Governo gli eventuali interventi normativi ritenuti necessari per la tutela dei diritti degli interessati.

19.2. *Le opposizioni ai provvedimenti del Garante e le decisioni giudiziali di maggior rilievo*

L'anno 2025 ha registrato un lieve aumento nella proposizione delle opposizioni a provvedimenti dell'Autorità: 87 a fronte dei 85 ricorsi del 2024.

Nell'anno di riferimento, inoltre, l'Autorità ha avuto notizia di 90 decisioni dell'autorità giudiziaria relative ad opposizioni a provvedimenti del Garante, a fronte delle 92 pervenute nel 2024.

Di seguito si dà conto delle sentenze di maggior rilievo.

Amministrazioni pubbliche

Con sentenza 13 novembre 2025, n. 1377, il Tribunale di Perugia ha confermato un provvedimento sanzionatorio del Garante 29 aprile 2021, n. 170 (doc. web n. 9681778) concernente un reclamo nei confronti di una regione a mezzo del quale l'interessato aveva lamentato che, dopo aver presentato domanda di partecipazione ad alcune procedure concorsuali bandite per l'anno 2015 dalla medesima regione, continuava a vedere indicizzate dai motori di ricerca, a distanza di circa tre anni dalla effettuazione delle prove selettive, le griglie degli ammessi con riserva e/o la convocazione per la pre-selezione. Il Garante aveva, quindi, adottato il citato provvedimento sanzionatorio attraverso il quale aveva rilevato l'illiceità del trattamento di dati personali effettuato dalla regione per aver determinato un'indebita diffusione di dati personali, in violazione degli artt. 5, 6, par. 1, lett. c) ed e), e 17 del RGPD e 2-*ter*, commi 1 e 3, d.lgs. n. 196/2003. Nel confermare il suddetto provvedimento, il Tribunale ha evidenziato che,

per poter ritenere corretto il comportamento della regione, sarebbe stato necessario che il trattamento, oltre a trovare il proprio fondamento in una espressa previsione di legge, fosse anche limitato nel tempo (nel caso di specie, al massimo fino all'esecuzione della prova da parte del singolo candidato) e contenesse unicamente i dati strettamente necessari allo scopo.

Nella vicenda in esame, invece, l'aver indicato oltre ai dati anagrafici, il giorno, l'ora ed il luogo di esecuzione della prova selettiva era palesemente in contrasto con i criteri suddetti, oltre che con le previsioni normative nella materia concorsuale, che prevede l'ostensibilità delle sole graduatorie finali dei vincitori di concorso e non anche gli avvisi di convocazione dei candidati. Con la medesima sentenza, il Tribunale ha affermato che l'illecita diffusione di dati è soggetta alla disciplina in vigore al momento in cui i dati sono rimossi, trattandosi di un illecito permanente, e che il bando di concorso non può essere assimilato a uno dei provvedimenti di cui all'art. 2-*ter*, comma 1, del Codice.

Attività ispettive

Con ordinanza della Corte di cassazione 13 giugno 2025, n. 15882 è stata confermata l'ordinanza-ingiunzione del Garante 28 maggio 2018, n. 297 (doc. web n. 9370122) al pagamento di euro 800.000 nei confronti di una società di telefonia per violazione degli artt. 23, 24, 162 comma 2-*bis* e 164-*bis* del d.lgs. n. 196/2003 *ante* riforma in relazione ad intestazioni di più linee telefoniche in capo ad un interessato inconsapevole. La Cassazione ha confermato che la fattispecie prevista dall'art. 164-*bis*, comma 2, d.lgs. n. 196/2003 *ante* riforma (banche dati di particolare rilevanza o dimensioni) costituisce una figura di illecito del tutto autonoma e non un'ipotesi aggravata rispetto alle violazioni semplici ivi richiamate.

In merito alla mancata acquisizione del consenso e alla circostanza che l'eventuale nullità/annullabilità di un contratto per "errore" del titolare non esonera lo stesso titolare dall'adempimento degli obblighi in materia di protezione dati, la Suprema Corte ha richiamato il proprio precedente 11 ottobre 2021, n. 27544, che aveva confermato la sentenza del Tribunale di Milano n. 6460/2018 relativa ad altra controversia tra le stesse parti.

Con sentenza 24 aprile 2025, n. 1300, il Tribunale di Nola ha confermato il provvedimento sanzionatorio del Garante 14 dicembre 2017, n. 532 (doc. web n. 8187572) adottato nei confronti di una società, che aveva intestato a tre persone, a loro insaputa, un numero complessivo di sette schede telefoniche, in assenza del loro consenso ai sensi dell'art. 23 del Codice previgente, la cui violazione era sanzionata dall'art. 162, comma 2-*bis*, del medesimo Codice. Il giudice, tra l'altro, ha ritenuto infondata l'eccezione di decadenza dal potere sanzionatorio ex art. 14, l. n. 689/1981, proposta dalla ricorrente, in quanto, conformemente al consolidato orientamento della giurisprudenza di legittimità (Cass. nn. 16286/2018 e 26734/2011), tale norma, facendo riferimento all'accertamento e non alla data di commissione della violazione, deve essere interpretata nel senso che il termine di novanta giorni ivi previsto comincia a decorrere dal momento in cui è compiuta o si sarebbe dovuta compiere, anche in relazione alla complessità o meno della fattispecie, l'attività amministrativa volta a verificare tutti gli elementi dell'infrazione. Parimenti, ha ritenuto infondata l'eccezione di prescrizione del diritto ex art. 28, l. n. 689/1981, non essendo trascorso il termine dei cinque anni tra la notifica del verbale di contestazione e la notifica dell'ordinanza-ingiunzione emessa dal Garante.

Con sentenza 29 settembre 2025, n. 13293, il Tribunale di Roma ha confermato l'ordinanza-ingiunzione 2 febbraio 2017, n. 47 (doc. web n. 6009876) con la quale il Garante, sulla base di elementi emersi in sede di indagine penale effettuata dalla Guardia di finanza, aveva irrogato ad una società di *money transfer* una sanzione pecuniaria di euro 5.880.000 per le violazioni di cui agli artt. 162, comma 2-*bis*, e 164-*bis*, comma 2,

del Codice, nei confronti di 583 persone in vita, i cui dati, contenuti in una banca dati di particolare rilevanza e dimensioni, erano stati utilizzati a loro insaputa per attribuire, tramite agenzie sub-mandatarie, trasferimenti di denaro in Cina a soggetti differenti dai reali mittenti, mediante i cd. furti di identità, e, quindi, senza aver acquisito il previo consenso dei medesimi. Nel confermare il suddetto provvedimento, il Tribunale ha evidenziato che il titolare può effettuare il trattamento senza richiedere il consenso in esecuzione di una prestazione contrattuale, ai sensi del previgente art. 24, comma 1, lett. b), d.lgs. n. 196/2003 (v. ora art. 6, par. 1, lett. b), RGPD), solo in quanto l'interessato sia effettivamente il contraente che richiede la prestazione. Se, invece, come nel caso di specie, non vi è tale coincidenza, allora l'"interessato" è una persona diversa, i cui dati sono trattati illecitamente se in assenza del consenso e senza che egli ne sia consapevole, neanche se il consenso viene acquisito implicitamente attraverso la richiesta di una prestazione contrattuale. Sotto altro profilo, la qualità di titolare non può essere delegata o trasferita, poiché si finirebbe in tal modo per eludere gli obblighi, le garanzie, e le connesse responsabilità oggetto della disciplina sulla protezione dei dati personali. Non vi è, in capo al responsabile o all'incaricato (v. artt. 29 e 30 del d.lgs. n. 196/2003 previgente, ora art. 28 del RGPD), un potere del tutto autonomo, poiché i dati sono trattati nell'esercizio delle funzioni attribuite dall'ente, per le finalità proprie di questo e nell'ambito dei suoi poteri. Inoltre, il Tribunale ha confermato che la fattispecie prevista dall'art. 164-*bis*, comma 2, d.lgs. n. 196/2003 *ante* riforma (banche dati di particolare rilevanza o dimensioni) costituisce una figura di illecito del tutto autonoma e non un'ipotesi aggravata rispetto alle violazioni semplici ivi richiamate.

Attività economiche

Il Tribunale di Firenze, con sentenza 13 febbraio 2025, n. 507 ha dichiarato inammissibile la domanda proposta avverso un'ipotesi di silenzio inadempimento del Garante, volta ad ottenere una pronuncia di accertamento del mancato rispetto del termine di 12 mesi per la conclusione del procedimento di reclamo ai sensi dell'art. 143 del Codice. Il giudice ha ritenuto che, pur essendo pacifico che il Garante non aveva rispettato il termine meramente ordinatorio previsto dalla citata norma, difettava, tuttavia, nel caso di specie l'interesse ad agire della ricorrente in ordine alla richiesta di accertamento proposta, non avendo indicato quale specifica utilità o vantaggio avrebbe conseguito dalla richiesta pronuncia giudiziale. La sola violazione del termine di cui al richiamato art. 143, non sostenuta da un interesse personale, attuale e concreto, si configura infatti come una mera lamentela, come tale non tutelabile in giudizio. Nel merito, il Tribunale ha ritenuto fondata la domanda nei confronti della compagnia assicuratrice volta ad ottenere l'accertamento del diritto della ricorrente di conoscere il nominativo del/dei beneficiario/i della polizza vita stipulata dal *de cuius*, in quanto il diritto alla riservatezza, lungi dall'essere un diritto assoluto, deve essere bilanciato volta per volta con eventuali altri interessi coinvolti nel caso. Conseguentemente, il diritto alla riservatezza dei dati personali di terzi beneficiari di polizze assicurative deve cedere di fronte alla tutela di altri interessi giuridicamente rilevanti, tra cui quello dell'esercizio del diritto di difesa in giudizio del chiamato all'eredita, avente rilievo costituzionale ai sensi dell'art. 24 Cost. (in tal senso, Cass. civ., sez. I, ord., 13 dicembre 2021, n. 39531).

Marketing e trattamento di dati personali

Il Tribunale di Roma, con sentenza 18 settembre 2025, n. 12783 ha respinto il ricorso presentato da un operatore del settore energetico avverso il provvedimento sanzionatorio 8 febbraio 2024, n. 81 (doc. web n. 9988710), con il quale era stata irrogata una sanzione amministrativa pecuniaria nei confronti della società per la violazione degli artt. 5 e 28 del RGPD. Il provvedimento aveva accertato, in particolare, la vulnerabilità dei sistemi della società e l'assenza di qualsivoglia controllo del trattamento da parte della propria filiera, al punto da consentire a società terze l'inserimento e l'operatività non autorizzata nel sistema di tenuta dei dati trattati. Nel confermare la correttezza del

provvedimento dell'Autorità, utile ad arginare l'incontrollata proliferazione del cd. telemarketing selvaggio a danno dei cittadini, il Tribunale adito ha altresì aderito al consolidato orientamento giurisprudenziale, secondo cui il termine per contestare una condotta illecita decorre soltanto dal momento in cui l'Autorità di controllo possieda una piena ed effettiva conoscenza della stessa, acquisiti e valutati tutti gli elementi necessari, specialmente nel corso di una istruttoria lunga e complessa. La sentenza è stata impugnata dinanzi alla Corte di cassazione.

Con ordinanza 13 giugno 2025, n. 15881 della Corte di cassazione è stata confermata l'ordinanza-ingiunzione 13 luglio 2016, n. 308 (doc. web n. 5751157) adottata dal Garante nei confronti di una società che aveva effettuato un trattamento di dati personali mediante il proprio sito Internet, consistente nella creazione di una mailing list e nell'invio ai propri utenti, tramite e-mail, di una newsletter periodica e di informazioni di natura commerciale e promozionale relative al sito, senza che fosse stato acquisito il consenso specifico dell'interessato nelle forme previste dall'art. 23, la cui violazione era sanzionata dall'art. 162, comma 2-*bis,* d.lgs. n. 196/2003 *ante* riforma. La Suprema Corte, cassando con rinvio la sentenza del Tribunale di I grado in ordine alla sola omessa statuizione del giudice di prime cure sull'applicabilità dell'attenuante di cui all'art. 164-*bis,* d.lgs. n. 196/2003 previgente, ha ribadito il principio di diritto, enunciato da Cass. n. 7555/2023, per il quale l'art. 130, comma 4, del Codice va interpretato nel senso che non è necessario il consenso dell'interessato se il titolare del trattamento, ai fini della vendita diretta di propri prodotti o servizi, utilizza le coordinate di posta elettronica fornite dal destinatario nel contesto della vendita, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni; diversamente, deve essere richiesto il consenso, ai sensi del primo e del secondo comma dello stesso articolo, nell'ipotesi in cui l'interessato abbia solamente effettuato la registrazione sul sito web, abbia concluso un contratto di prova o comunque abbia concluso un contratto a titolo gratuito con il titolare del trattamento. La sentenza è stata riassunta davanti al Tribunale di Roma.

Attività giornalistica

La Corte di cassazione, con sentenza 8 aprile 2025, n. 9274, ha confermato il provvedimento 31 agosto 2023, n. 390 (doc. web n. 9944538) con il quale l'Autorità aveva sanzionato una testata giornalistica per avere pubblicato, nella propria versione online, l'immagine di ragazze minorenni in relazione a una notizia di cronaca di molestie subite dalle vittime. Il Tribunale di I grado aveva già respinto il ricorso proposto dalla società, ritenendo sussistente la violazione del principio di essenzialità dell'informazione (art. 137, comma 3, del Codice), per aver esposto le minori a una possibile identificazione, sebbene la fotografia non arricchisse la notizia, tenuto conto che l'unica informazione aggiuntiva che essa poteva dare era proprio la riconoscibilità delle ragazze. La Cassazione ha confermato tale decisione, impugnata sostanzialmente nel merito, ricordando che è da "ritenersi inammissibile il ricorso per cassazione che, sotto l'apparente deduzione del vizio di violazione o falsa applicazione di legge (come pure di ogni altro vizio astrattamente riconducibile al disposto dell'art. 360, comma 1, c.p.c.) miri, in realtà, ad una rivalutazione dei fatti storici operata dal giudice di merito".

Analogamente, con sentenza 31 marzo 2025, n. 1123, il Tribunale di Torino ha confermato il provvedimento 31 agosto 2023, n. 391 (doc. web n. 9944579) con il quale l'Autorità aveva sanzionato una testata giornalistica per avere pubblicato l'immagine di una ragazza minorenne in relazione a una notizia di cronaca di molestie subite dalla vittima stabilendo che il diritto alla riservatezza personale di soggetti minorenni limita fortemente il diritto di cronaca giornalistica e, dunque, di pubblicazione di

foto di minorenni. La pubblicazione della foto del minore deve essere indispensabile ed essenziale per il racconto della notizia. Nel caso di specie, nel pubblicare la fotografia contestata non erano state adottate le misure di protezione idonee a garantire la non identificabilità delle minori. Inoltre, il giudice ha ritenuto la pubblicazione della fotografia non essenziale ai fini della narrazione della notizia, ed anzi del tutto superflua.

Con sentenza 22 maggio 2025, n. 8977, il Tribunale di Roma ha confermato il provvedimento sanzionatorio 20 ottobre 2022, n. 356 (doc. web n. 9827446), con riduzione dell'importo, nei confronti di un policlinico per aver consentito nel febbraio 2022 l'accesso agli ambulatori solo a coloro che fossero in possesso di una certificazione verde (cd. green pass), indicazione che era riportata anche sul sito Internet del predetto policlinico. In particolare, il Tribunale ha evidenziato che il trattamento effettuato attraverso il controllo delle certificazioni verdi si qualifica come un trattamento per motivi di sanità pubblica e, in quanto tale, trova la relativa base giuridica nella specifica disciplina di settore (cfr. art. 9, par. 2, lett. i), RGPD). Nella vicenda in esame, ha affermato il Tribunale, a fronte di una normativa nazionale che disponeva, nel periodo di riferimento, il divieto di trattamento dei dati effettuato attraverso il controllo delle certificazioni verdi per l'accesso alle prestazioni ospedaliere, anche la mera richiesta di esibizione (così come qualsiasi forma di differenziazione tra i possessori di green pass e i non possessori) "deve ritenersi priva di adeguata base giuridica, anche qualora l'interessato avesse prestato un consenso esplicito, in applicazione dell'art. 9, par. 2, lett. a) del Regolamento (UE) 2016/679". Nella vicenda in esame, il policlinico, prevedendo modalità evidentemente differenziate tra possessori e non possessori di certificazione verde, aveva di fatto trattato i dati sanitari in modo diverso per le due categorie di persone, perseguendo finalità non più consentite dalla legge allora vigente, alla quale avrebbero dovuto, invece, tempestivamente adeguarsi. La sentenza è stata impugnata dinanzi alla Corte di cassazione.

Con ordinanza 6 marzo 2025, n. 6067 della Suprema Corte è stato accolto il ricorso proposto dal Garante avverso la sentenza del Tribunale di Udine 20 novembre 2023, n. 811, che aveva annullato il provvedimento prescrittivo e sanzionatorio 15 dicembre 2022, n. 416 (doc. web n. 9845156), adottato dal Garante nei confronti di un'azienda sanitaria per l'illecito trattamento dei dati personali contenuti nelle banche dati aziendali e nel FSE, disciplinato dall'art. 12, d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla l. n. 221/2012, nel testo applicabile *ratione temporis* al caso esaminato, e dal d.P.C.M. n. 178/2015. In particolare, la Suprema Corte ha statuito che la liceità del trattamento dei dati del FSE, costituito dall'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi che riguardano l'assistito, riferiti anche alle prestazioni erogate al di fuori del SSN, si fonda su un duplice consenso, specifico, libero ed informato da parte dell'assistito: il primo è costituito dal consenso all'"alimentazione del FSE con i dati" (art. 6, comma 2, lett. d) e art. 7 del d.P.C.M.); il secondo dal consenso alla "consultazione dei dati e dei documenti (in chiaro) contenuti nel FSE" per le finalità di prevenzione, diagnosi, cura e riabilitazione di cui alla lett. a), comma 2, art.12 (art. 6, comma 2, lett. e) e art. 7 del d.P.C.M.). I titolari del trattamento per le finalità di prevenzione, diagnosi, cura e riabilitazione (che richiede il secondo consenso) sono i soggetti del SSN e dei servizi socio-sanitari regionali e gli esercenti le professioni sanitarie che prendono in cura l'assistito; le informazioni da trattare sono esclusivamente quelle pertinenti al processo di cura in atto dell'assistito; per la finalità di cura si possono prevedere anche servizi di elaborazione di dati, relativi a percorsi diagnostici-terapeutici, per supportare i processi di prevenzione, diagnosi e cura, ma "limitatamente all'assistito preso in cura". Non è previsto alcun trattamento dei dati

in chiaro che esorbiti dalla posizione e dall'interesse terapeutico del singolo assistito a cui si riferisce il FSE. Pertanto, il trattamento dei dati contenuti nel FSE per finalità di cura è puntualmente circoscritto ai dati direttamente collegati all'assistito preso in cura e non prevede alcuna rielaborazione generale dai dati appartenenti ad una pluralità di assistiti volta alla realizzazione di un documento di sintesi in funzione di programmazione sanitaria; per altro verso, le diverse finalità previste dalla lett. b) e c) dell'art.12, comma 2, d.l. n. 179/2012 di ricerca e di governo, sono anch'esse espressamente disciplinate e vanno perseguite "senza l'utilizzo dei dati identificativi degli assistiti".

Diritto all'oblio e deindicizzazione

Con sentenza 26 dicembre 2025, n. 34217 della Suprema Corte, è stato rigettato il ricorso avverso la sentenza del Tribunale di Napoli 24 settembre 2024, che aveva confermato il provvedimento 28 settembre 2023, n. 480 (doc. web n. 9946736), con cui il Garante aveva ritenuto che la fattispecie di cui all'art. 64-*ter* disp att. c.p.p. fosse pur sempre da leggere "ai sensi e nei limiti dell'artt. 17 del RGPD" e, pertanto, a seguito del bilanciamento previsto dalla suddetta disposizione, aveva ritenuto la richiesta di deindicizzazione, presentata dal reclamante, infondata. In particolare, la Suprema Corte ha statuito che l'annotazione della deindicizzazione prevista dall'art. 64-*ter*, commi 1 e 3, disp. att. c.p.p. "ai sensi e nei limiti dell'articolo 17 del Regolamento (UE) 2016/679 (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016", apposta su uno dei provvedimenti ivi indicati, non determina una presunzione assoluta di fondatezza dell'istanza così da precludere al destinatario di quella misura qualsiasi potere valutativo. Ne consegue che i medesimi soggetti che già anteriormente all'entrata in vigore di detta norma si occupavano di vagliare le corrispondenti domande – ovverosia, ognuno con le proprie prerogative, il gestore del motore di ricerca oppure l'autorità amministrativa preposta o, infine, l'autorità giudiziaria – continuano ad operare nello stesso modo anche nel vigore del nuovo assetto prescrittivo, bilanciando, nel concreto, la tutela da apprestare al soggetto interessato all'oblio ed i diritti all'informazione, di cronaca e connessi. Pertanto, anche a seguito dell'entrata in vigore dell'art. 64-*ter* disp. att. c.p.p., un dato lecitamente inserito nel web vi permane legittimamente fino a quando le ragioni che ne hanno giustificato la pubblicazione siano venute meno in considerazione, tra l'altro, di un apprezzabile intervallo temporale da essa trascorso, all'esito del quale sarà possibile ottenere, ricorrendone gli altri presupposti desumibili dell'art. 17 del menzionato RGPD, la deindicizzazione.

Con sentenza 27 novembre 2025, n. 19439, il Tribunale di Roma, confermando il provvedimento del Garante 2 marzo 2023, n. 62 (doc. web n. 9880427), ha ritenuto che la diffusione dei dati personali dei figli di un personaggio pubblico risultasse effettivamente eccedente e non essenziale rispetto all'interesse pubblico alla conoscenza dei fatti trattati. Il contemperamento degli opposti diritti costituzionalmente garantiti deve essere sempre risolto a favore della preminenza del diritto alla riservatezza rispetto al diritto di cronaca, ogni qualvolta l'indicazione del nome e delle generalità dell'interessato non siano necessarie ai fini della notizia. Per citare il Tribunale: "Il diritto ad essere dimenticati (cd. *right to be forgotten*) consiste, dunque, nel diritto a non rimanere esposti, senza limiti di tempo, ad una rappresentazione non più attuale della propria persona, per la ripubblicazione, a distanza di tempo, di una notizia relativa a fatti o a vicende nelle quali si è rimasti in qualche modo coinvolti. Accade così che il fatto, completamente acquisito dalla collettività, dopo aver perduto la connotazione pubblica, nell'intervenuto decorso del tempo, con il trascolorare dell'interesse alla sua conoscenza diventa privato e, là dove riproposto, apre lo spazio al riconoscimento del diritto all'oblio". La sentenza è stata impugnata dinanzi alla Corte di cassazione.

Libera manifestazione del pensiero

Con sentenza 27 dicembre 2025, n. 34224, la Suprema Corte ha accolto il ricorso del Garante avverso la sentenza del Tribunale di Messina 17 aprile 2024, n. 995, che aveva annullato il provvedimento sanzionatorio del Garante 13 maggio 2021, n. 197 (doc. web

n. 9670001) nei confronti di un amministratore comunale per aver diffuso, attraverso il suo account social, dati e informazioni di soggetti anche vulnerabili, in violazione della disciplina concernente il trattamento per finalità di libera manifestazione del pensiero (artt. 136 e ss. del Codice). La Suprema Corte ha fornito al riguardo un'interpretazione stringente di ciò che deve intendersi per esecuzione di un compito di pubblico interesse ai sensi dell'art. 6 del RGPD e dell'art. 2-*ter* del Codice. In questa vicenda l'amministratore comunale, nel diffondere determinante immagini, era soggetto alle regole della libera manifestazione del pensiero in bilanciamento con i diritti delle persone ritratte. La Suprema Corte ha in particolare affermato il principio di diritto secondo cui "ai fini dell'art. 137 del d.lgs. n. 196/2003" (norma che autorizza il trattamento dei dati personali nell'ambito dell'attività giornalistica anche senza il consenso dell'interessato) "non rileva solo il trattamento di dati personali avvenuto nell'esercizio dell'attività giornalistica ma anche il trattamento, inclusa la pubblicazione e diffusione anche su profilo personale social network, ove accessibile a un numero indefinito di persone, finalizzato alla libera manifestazione del pensiero ai sensi del primo comma dell'art.136, lett. c). Il rispetto delle disposizioni contenute nelle regole deontologiche – nello specifico dell'art. 7 a tutela dei minori e della Carta di Treviso ivi richiamata – costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali.".

Il Tribunale di Salerno con sentenza 18 giugno 2025, n. 2679 ha confermato l'ordinanza-ingiunzione 1° marzo 2018, n. 124 (doc. web n. 8998644) emanata dal Garante nei confronti di un comune che aveva utilizzato dati biometrici al fine di rilevare la presenza dei dipendenti sul luogo di lavoro, confermando che, come più volte ricordato dall'Autorità, tale utilizzo non è consentito dalla vigente disciplina in materia di protezione dei dati personali e che possono a tal fine essere utilizzati sistemi meno invasivi, a nulla rilevando che i dati acquisiti dal sistema di rilevamento vengano o meno conservati.

Con sentenza 4 ottobre 2025, n. 707, il Tribunale di Rimini, ha confermato il provvedimento del Garante 6 luglio 2023, n. 292 (doc. web n. 9924466) stabilendo che l'argomento difensivo relativo alla "carenza di personale" non è idoneo ad escludere la colpa della società. Ne deriva in particolare che la mancata consultazione della casella PEC integra negligenza organizzativa imputabile al datore di lavoro, non potendo costituire causa di giustificazione la carenza di organico. Sul mancato riscontro all'istanza di accesso, l'art. 12 del RGPD stabilisce che il titolare del trattamento deve rispondere all'istanza dell'interessato entro un mese, anche in caso di diniego, indicando le ragioni e i mezzi di tutela disponibili. Sul conferimento orale dell'incarico investigativo dall'istruttoria è emerso che l'incarico all'agenzia investigativa era stato conferito esclusivamente in forma orale. Ciò si palesa in contrasto con l'art. 8 delle regole deontologiche relative alle investigazioni difensive, che prescrive un incarico scritto recante l'indicazione: del diritto da esercitare o difendere; del procedimento penale o civile a cui l'indagine si riferisce; degli elementi di fatto che giustificano l'investigazione; del termine entro il quale deve concludersi. Ai sensi dell'art. 2-*quater*, comma 4 del Codice, il rispetto delle regole deontologiche costituisce condizione essenziale di liceità del trattamento. L'affidamento orale integra pertanto violazione sostanziale della normativa e determina illiceità dei dati raccolti. Infine, in merito all'asserita natura di dati biometrici di cui all'art. 9 del RGPD delle immagini fotografiche e video, tale da giustificare il trattamento per finalità difensive, il giudice ha ritenuto l'argomento infondato affermando che le fotografie costituiscono dati biometrici solo se trattate con strumenti tecnici specifici atti a consentire l'identificazione univoca. Ne deriva che la semplice fotografia, priva di elaborazione mediante software o hardware di riconoscimento facciale, non rientra nella categoria dei dati biometrici, ma resta un dato personale comune ai sensi dell'art. 4, par. 1, n. 1 del RGPD.

Il Tribunale di Milano, con sentenza 8 maggio 2025, n. 3745, ha confermato il provvedimento del Garante 11 aprile 2024, n. 205 (doc. web n. 10008076), dichiarando improponibile il ricorso proposto dalla società per essersi la stessa avvalsa del meccanismo di definizione di cui all'art. 166, comma 8, del Codice, avendo la medesima ottemperato alle prescrizioni impartite dal Garante con il provvedimento impugnato ed effettuato il pagamento in misura ridotta nel termine prescritto. Ad avviso del Tribunale, tale norma prevede un meccanismo di definizione della controversia simile a quello previsto dalla normativa sulle sanzioni amministrative di cui all'art. 16, l. n. 689/1981 – con la differenza che in tale ultimo caso non viene emessa la successiva ordinanza-ingiunzione – e all'art. 202 del codice della strada per le sanzioni conseguenti alle violazioni ivi previste. Invero, analogamente l'art. 166, comma 8, d.lgs. n. 196/2003 consente al trasgressore di corrispondere una sanzione ridotta della metà rispetto a quella irrogata nel caso in cui lo stesso effettui tale pagamento e si adegui alle eventuali prescrizioni impartite dal Garante nel termine previsto per la proposizione del ricorso, quale meccanismo premiale per la definizione anticipata del contenzioso. Con riferimento ai contenziosi sviluppatisi in relazione alla definizione agevolata prevista dalle richiamate norme, la giurisprudenza di legittimità ha rilevato come l'avvenuto pagamento della sanzione in misura ridotta comporti una incompatibilità oltre che un'implicita rinunzia a far valere qualsiasi contestazione relativa sia alla sanzione pecuniaria irrogata, sia alla violazione contestata, che della sanzione pecuniaria è il presupposto giuridico, ritenendo ammissibili in sede di ricorso doglianze che abbiano ad oggetto esclusivo le sole sanzioni accessorie, quali la mancata previsione della pena accessoria o la previsione della stessa in misura diversa (cfr. Cass. civ., sez. u., 29 luglio 2008 n. 20544, Cass. civ., sez. 2-6, 2 dicembre 2021 n. 37999). Il Tribunale meneghino, pertanto, ha ritenuto tali princìpi applicabili anche nel caso di specie, posto che la scelta della ricorrente di conformarsi alle prescrizioni del Garante e di procedere al contestuale pagamento della sanzione in misura ridotta ha configurato un'acquiescenza al provvedimento e ha determinato, in conformità alla citata previsione normativa e all'avviso su tale facoltà reso nello stesso provvedimento impugnato, la definizione anticipata della controversia, in quanto tale incompatibile con la proposizione di successive contestazioni sulla sussistenza dei presupposti della violazione e dell'applicazione delle sanzioni.

Degne di nota appaiono alcune pronunce emanate da diversi tribunali di merito che hanno confermato alcuni provvedimenti di archiviazione, posti a conclusione dell'esame di istruttoria preliminare di reclami presentati al Garante.

Segnatamente, con sentenza 15 luglio 2025, n. 1138, il Tribunale di Treviso ha confermato un provvedimento del Garante, notificato il 15 marzo 2023, con cui era stato archiviato un reclamo concernente la produzione in un giudizio di documenti relativi a procedimenti penali a carico del reclamante, avvenuta nella cornice dettata dall'art. 160-*bis* del Codice, affermando l'applicabilità alla specie dell'art. 37, comma 6, d.lgs. n. 51/2018.

Con sentenza 3 ottobre 2025, n. 13820, il Tribunale di Roma ha dichiarato, in via pregiudiziale, inammissibile il ricorso presentato da un reclamante avverso un provvedimento di archiviazione per non aver lo stesso chiamato in causa il titolare del trattamento nel termine ex art. 10, comma 3, d.lgs. n. 150/2011; nel merito, ha dichiarato l'infondatezza del ricorso attesa l'applicabilità dell'art. 160-*bis* del Codice. La sentenza è stata impugnata dinanzi alla Corte di cassazione.

Con sentenza 18 aprile 2025, n. 841, il Tribunale di Velletri ha confermato il provvedimento del Garante 6 agosto 2021 di archiviazione del reclamo concernente le comunicazioni intercorse tra l'amministrazione, datrice di lavoro del reclamante, e il

medesimo, in relazione a talune istanze presentate da quest'ultimo con riguardo ad infermità riconosciute per causa di servizio e contenenti anche dati relativi alla salute, avvenute in asserita violazione della disciplina in materia di protezione dei dati personali. Sotto il profilo dei termini procedimentali, il Tribunale ha rilevato che l'art. 143 del Codice non correla al superamento del termine un effetto decadenziale, né qualifica espressamente tale termine come perentorio, richiamando quei principi giurisprudenziali per cui il carattere della perentorietà del termine può essere attribuito ad una scadenza temporale solo da una espressa norma di legge. Pertanto, in assenza di specifica disposizione che espressamente preveda il termine come perentorio, comminando la perdita della possibilità di azione da parte dell'amministrazione al suo spirare o la specifica sanzione della decadenza, il termine va inteso come meramente sollecitatorio o ordinatorio, sicché il suo superamento non determina l'illegittimità dell'atto (cfr. C.d.S. sez. V, 7 marzo 2023). Il Tribunale ha, altresì, affermato che il procedimento del Garante, a seguito di reclamo, non ha, di per sé, natura esclusivamente sanzionatoria, ma solo eventualmente sanzionatoria, atteso che la procedura avviata a seguito di un reclamo ha principalmente una funzione di accertamento e di tutela dei diritti dell'interessato. Pertanto, considerato che il provvedimento impugnato non aveva natura sanzionatoria, essendo stata peraltro disposta l'archiviazione del reclamo, il Tribunale non ha ritenuto sussistenti esigenze di rilievo pubblico, sicché ha valutato applicabili i principi consolidati della giurisprudenza amministrativa, secondo cui il termine di conclusione del procedimento riveste, di regola, natura ordinatoria, con la conseguenza che il mancato rispetto del medesimo non vizia l'atto adottato tardivamente (cfr. C.d.S., sez. VI, 25 maggio 2020, n. 3307 e C.d.S., sez. VI, 08 luglio 2015, n. 3401).

Con sentenza 8 maggio 2025, n. 241, il Tribunale di Sulmona ha confermato il provvedimento di archiviazione 16 aprile 2024 in relazione ad un reclamo proposto innanzi al Garante, rigettando il motivo di ricorso relativo all'asserita violazione dell'art. 10-*bis*, l. n. 241/1990. In particolare, il Tribunale ha rilevato la specialità del procedimento su reclamo disciplinato dal reg. del Garante n. 1/2019, evidenziandone la natura di procedura a struttura solo eventualmente bifasica, in cui alla prima parte nella quale si svolge una istruttoria endoprocedimentale improntata a celerità e speditezza non necessariamente segue un vero e proprio procedimento amministrativo avente funzione sanzionatoria della violazione come accertata in istruttoria. La sentenza è stata impugnata dinanzi alla Corte di cassazione.

Con sentenza 8 luglio 2025, n. 18583, la Suprema Corte ha cassato con rinvio, in accoglimento del ricorso proposto dal Garante, la sentenza n. 2615/2023 del Tribunale di Roma, che aveva annullato il provvedimento del 16 dicembre 2021, n. 443 (doc. web n. 9735672). La questione afferisce al tema relativo alla natura del termine procedimentale di 120 giorni per la notifica delle presunte violazioni ex art. 166, comma 5 del Codice. Sul punto, la Suprema Corte ha enunciato il seguente principio di diritto: "In tema di trattamento dei dati personali, la complessiva attività procedimentale dell'Autorità Garante per la protezione di questi ultimi, finalizzata all'accertamento di violazioni ed alla irrogazione delle corrispondenti sanzioni, consta di due fasi – una sanzionatoria in senso stretto ed una, precedente, investigativa o preistruttoria – logicamente e cronologicamente distinte. Il termine, da considerarsi perentorio, di centoventi giorni previsto al punto 2 dell'allegato "B" del reg. del Garante n. 2/2019 si riferisce esclusivamente alla fase sanzionatoria in senso stretto e decorre dalla conclusione della fase preistruttoria che culmina con l'effettivo accertamento delle violazioni ascritte al trasgressore e la notifica della contestazione". Il giudizio di rinvio è pendente.

20 Le relazioni comunitarie e internazionali

L'attività del Garante, nel periodo in considerazione, è stata contrassegnata da un considerevole impegno, sia in ambito europeo, sia in ambito internazionale, dettato dalla costante partecipazione ai molti tavoli e gruppi di lavoro di cui l'Autorità è parte attiva.

Nel contesto UE, il 2025 si è caratterizzato per le diverse iniziative dirette a una maggiore semplificazione e armonizzazione delle regole sulla protezione dei dati e della loro applicazione. Questa linea di tendenza è stata ravvisata sia nelle attività dello stesso CEPD, sia a livello normativo, con le proposte della Commissione europea che hanno riguardato la disciplina della protezione dei dati e le normative in materia di e-Privacy e di IA.

Gli obiettivi della semplificazione e dell'applicazione coerente del RGPD insieme al tema delle intersezioni tra diverse regolamentazioni in ambito digitale (reg. IA, DMA, DSA, *Data Act*, *Data Governance Act*, ecc.) sono stati al centro dell'incontro dei vertici delle autorità europee di protezione dati tenutosi a Helsinki il 1° e 2 luglio 2025, che ha segnato un momento di grande rilevanza nella definizione degli obiettivi del CEPD.

In conformità alla strategia per il periodo 2024-2027 (v. Relazione 2024, p. 197), con la dichiarazione di Helsinki il Comitato ha stabilito di dar vita ad una serie di azioni volte a migliorare l'efficienza del suo operato, con un particolare focus sull'uniformità e la chiarezza esplicativa dei propri atti, sulla pianificazione dei suoi lavori e un sempre maggiore coordinamento tra le autorità per assicurare linee di azione il più possibile coerenti (v. *infra*).

A livello normativo, la Commissione europea ha dapprima presentato una proposta di regolamento, pubblicata il 21 maggio 2025 (COM(2025) 501 final), per emendare alcuni atti legislativi, incluso il RGPD, introducendo misure di semplificazione, nonché l'estensione di alcune misure di attenuazione previste per le piccole e medie imprese (PMI) alle piccole imprese a media capitalizzazione (*Small Medium Cap* - SMC), in particolare in merito agli obblighi di tenuta del registro delle attività di trattamento prevista dall'art. 30 del RGPD. Tale iniziativa, che ha riguardato specifiche e circoscritte norme del regolamento sulla protezione dei dati, è stata seguita da una più ampia proposta, la proposta per un "Digital Omnibus", comprendente modifiche al RGPD, alla direttiva e-Privacy e al *Data acquis*, pubblicata il 19 novembre 2025, tesa invece ad apportare più incisive modifiche anche alla disciplina sulla protezione dei dati. Nello stesso giorno, la Commissione ha altresì pubblicato una proposta di regolamento che modifica i regolamenti (UE) 2024/1689 e (UE) 2018/1139 per quanto riguarda la semplificazione dell'attuazione delle norme armonizzate sull'intelligenza artificiale (di seguito Omnibus digitale sull'IA), introducendo alcuni emendamenti all'AI Act che attengono alla protezione dei dati.

La necessità di rafforzare la cooperazione fra autorità nella gestione dei casi transfrontalieri è stata inoltre al centro dei lavori per un regolamento sulle norme procedurali aggiuntive per l'applicazione del RGPD che, adottato il 12 dicembre 2025 e applicabile dal 2027, introduce un altro tassello significativo per la sistematizzazione dell'attività delle autorità

di protezione dei dati, concernente specifici procedimenti nei casi riguardanti un trattamento transfrontaliero e la composizione delle controversie da parte del CEPD durante tali procedimenti.

A livello internazionale, il Garante ha continuato a seguire i lavori dei diversi forum in materia di protezione dei dati, ed in particolare il Consiglio d'Europa, l'OCSE, la *Global Privacy Assembly* e il G7 delle autorità di protezione dati.

20.1. *La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dei dati*

Nel corso del 2025 la plenaria del CEPD si è riunita quattordici volte. 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.

Come già accennato, il 1° e 2 luglio 2025 i vertici delle autorità che compongono il CEPD si sono riuniti a Helsinki, in un apposito *High Level Meeting*, per discutere di alcune questioni strategiche, e in particolare: il tema della semplificazione del RGPD e degli strumenti per renderne più agevole l'implementazione; l'applicazione coerente del RGPD; le intersezioni tra le regolamentazioni UE in ambito digitale e la conseguente cooperazione tra le autorità competenti nei diversi settori.

Dichiarazione di Helsinki

All'esito del Meeting, il CEPD ha adottato una dichiarazione nella quale vengono delineate le nuove iniziative che si intende intraprendere per rendere la compliance del RGPD più semplice, in particolare per le piccole e medie imprese, rafforzare la coerenza e la cooperazione inter-regolatoria, ponendo la tutela dei diritti fondamentali al centro dell'innovazione digitale e della competitività.

Tra le attività del Comitato annunciate dalla dichiarazione di Helsinki si segnalano:

- l'elaborazione di modelli per le organizzazioni e le imprese e di un modello comune per le notifiche di *data breach* alle autorità di protezione dei dati;
- la raccolta di decisioni e linee guida adottate dalle autorità che compongono il CEPD su questioni prioritarie al fine di facilitarne la comprensione da parte degli attori interessati;
- l'allineamento delle linee guida e delle posizioni assunte dalle autorità per assicurarne efficacia e coerenza con le decisioni del Comitato;
- lo sviluppo di strumenti e metodologie per promuovere azioni comuni anche laddove non si applichi il meccanismo dello sportello unico;
- l'elaborazione, ove appropriato, di linee guida congiunte con altri regolatori (quali le linee guida sull'interazione tra RGPD e DMA elaborate dal CEPD e dalla Commissione europea, adottate il 9 ottobre 2025 nella loro prima versione, poi sottoposta a consultazione pubblica, v. *infra*);
- il rafforzamento della cooperazione con altre autorità di regolazione, anche attraverso lo scambio di informazioni su argomenti di comune interesse e l'invito, indirizzato alle stesse, a partecipare alle plenarie del Comitato;
- l'intensificazione del dialogo con gli stakeholder dei diversi settori interessati dal lavoro del CEPD.

Lo *statement* è stato seguito da una serie di azioni operative promosse dalla presidente e dal segretariato del Comitato. Infatti, con l'adozione di un documento contenente il piano applicativo di Helsinki nella plenaria dell'11 settembre, il CEPD si è impegnato ad implementare una serie di misure, in particolare con riferimento all'organizzazione delle sue attività, la pianificazione dei lavori e la necessità di un sempre maggiore coordinamento tra le autorità volto ad assicurare linee di azione il più possibile coerenti.

20

Nell'ottica di promuovere iniziative finalizzate ad una più agevole compliance, il CEPD ha avviato una consultazione pubblica (conclusasi il 3 dicembre 2025) funzionale a raccogliere i suggerimenti delle parti interessate sulle tipologie di modelli (ad es., un modello per le informative sulla privacy o per i registri delle attività di trattamento dei dati) più utili a facilitare la conformità al RGPD.

Con riferimento invece alle attività concernenti l'efficienza del proprio operato, il CEDP ha aggiornato le migliori pratiche per l'organizzazione delle riunioni plenarie, ne ha adottate di nuove su come preparare e redigere le proprie linee guida, predisposto un modello (*quality check*) per assicurare la qualità e la leggibilità dei propri documenti, nonché un modello per la realizzazione dei rapporti volti a riassumere ed a esaminare i contributi pervenuti nel corso delle consultazioni pubbliche cui i documenti del Comitato come le linee guida sono sottoposti.

Proposta sulla semplificazione per le piccole e medie imprese

Con il parere 1/2025 adottato l'8 luglio 2025, il CEPD si è pronunciato sulla proposta di regolamento della Commissione, pubblicata il 21 maggio 2025, volta a modificare alcune normative, incluso il RGPD, introducendo l'estensione di alcune misure di attenuazione previste per le piccole e medie imprese (PMI) alle piccole imprese a media capitalizzazione (*Small medium cap* - SMC), oltre ad ulteriori misure di semplificazione.

Con specifico riferimento al RGPD, la proposta mira sostanzialmente a modificare l'esenzione di cui all'art. 30, par. 5, RGPD prevedendo che l'obbligo di tenuta del registro di trattamento non si applichi a un'impresa o organizzazione che impieghi meno di 750 persone, a meno che il trattamento effettuato non possa comportare un alto rischio per i diritti e le libertà delle persone interessate, ai sensi dell'art. 35 RGPD. Attualmente l'obbligo di tenuta del registro delle attività di trattamento di cui all'art. 30, par. 5, RGPD non si applica alle imprese o organizzazioni con meno di 250 dipendenti "a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'art. 9, par. 1, o i dati personali relativi a condanne penali e a reati di cui all'art. 10".

Con il parere il CEPD supporta l'obiettivo generale della proposta di ridurre l'onere amministrativo per le PMI e le SMC, purché ciò non comporti una diminuzione della protezione dei diritti fondamentali degli individui. Il parere accoglie con favore che le modifiche proposte quanto all'obbligo di mantenere un registro dei trattamenti siano mirate e limitate e non impattino sui principi fondamentali e gli altri obblighi previsti dal RGPD; fornisce infine suggerimenti per meglio chiarire alcuni passaggi della proposta.

Omnibus digitale sull'IA

Con il parere 1/2026 adottato il 20 gennaio 2026, CEPD e GEPD hanno affrontato gli aspetti della proposta che rivestono particolare importanza per la protezione dei dati. Anche in questo caso, il parere sostiene l'obiettivo generale della proposta di ridurre gli oneri amministrativi per le imprese, le amministrazioni e il pubblico in generale, purché ciò non comporti una riduzione della tutela dei diritti fondamentali ed in particolare della protezione dei dati. Nella consapevolezza, tuttavia, che già durante la stesura iniziale del reg. IA sono stati introdotti diversi emendamenti per contribuire a ridurre gli oneri amministrativi, il parere sottolinea la necessità di mantenere un attento equilibrio tra la semplificazione e la salvaguardia dei diritti fondamentali e mette quindi in guardia i co-legislatori dal ridurre le garanzie attualmente offerte dal reg. IA in assenza di un'attenta considerazione della tutela dei diritti delle persone.

Digital Omnibus

Con il parere congiunto 2/2026, adottato il 10 febbraio 2026, CEPD e GEPD si sono espressi sulla proposta di un testo di Digital Omnibus comprendente significative modifiche al RGPD, alla direttiva e-Privacy e al *Data acquis*. Il parere, che in termini generali supporta gli obiettivi di semplificare la compliance, rafforzare l'esercizio dei diritti e facilitare la competitività, contiene alcune considerazioni critiche sull'efficacia

di specifiche misure proposte dalla Commissione.

In questa ottica, appaiono dunque positive le modifiche al RGPD volte in particolare a prevedere: una definizione di ricerca scientifica; una nuova deroga al divieto di trattare categorie particolari di dati ai fini dell'autenticazione biometrica ove i mezzi per la verifica rimangano sotto il solo controllo dell'interessato; l'innalzamento della soglia per la notifica delle violazioni dei dati (limitando il relativo obbligo al caso di violazione dei dati personali che possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche); l'estensione dei termini per la stessa notifica; modelli comuni per la notifica di *data breach* e per le DPIA.

Molto critico il parere, invece, nei riguardi delle modifiche suscettibili di alterare l'impianto di tutela previsto dalla normativa sulla protezione dei dati. È il caso degli emendamenti alla nozione di dato personale, elemento chiave di tutta la disciplina che, lungi dal costituire una mirata modifica migliorativa, è suscettibile di restringere il concetto stesso di dato personale e con esso l'intero sistema di tutela fornito dal RGPD, rendendolo incerto, legato a parametri soggettivi e disattendendo pertanto gli obiettivi di certezza giuridica che la proposta intende perseguire.

Altre proposte di emendamento al RGPD, pur in linea generale supportate dal CEPD e GEPD, meriterebbero miglioramenti ulteriori, in particolare con riferimento al legittimo interesse come base giuridica dei trattamenti nel contesto dell'IA, alla previsione di una deroga per i trattamenti incidentali e residuali di categorie particolari di dati sempre nel contesto IA, ad alcune limitazioni al diritto di accesso, alle deroghe agli obblighi di trasparenza e alle modifiche sulle decisioni automatizzate sottolineando l'importanza di mantenere il principio del loro divieto, salve specifiche deroghe.

Con riferimento alle proposte di emendamento relative alla direttiva e-Privacy, è accolto con favore l'obiettivo della proposta di fornire soluzioni dirette ad attenuare pratiche per la richiesta di consenso onerose per l'interessato e la proliferazione di cookie banner, così come, in linea generale e salvi necessari aggiustamenti del testo, a fornire ulteriori limitate eccezioni al divieto di archiviazione e di accesso alle informazioni archiviate nell'apparecchiatura terminale di un abbonato o di un utente, nonché l'attribuzione alle sole autorità di protezione dati della supervisione anche in questo settore.

Riguardo alle proposte di modifica relative al *Data acquis*, il parere supporta gli obiettivi di semplificazione perseguiti attraverso l'integrazione nel regolamento sui dati (reg. (UE) 2023/2854, di seguito *Data Act*), del regolamento sulla *governance* dei dati (reg. (UE) 2022/868) e della direttiva sui dati aperti e il riutilizzo dell'informazione del settore pubblico (direttiva (UE) 2019/1024).

Cionondimeno, in merito all'accesso alle informazioni del settore pubblico a fini di riutilizzo, il CEPD e il GEPD raccomandano di mantenere la chiarezza offerta dall'attuale quadro giuridico, specificando che questo non obbliga gli enti del settore pubblico a consentire il riutilizzo di dati personali, né fornisce una base giuridica per l'accesso a questi ultimi. Per quanto riguarda le emergenze pubbliche, il CEPD e il GEPD esortano il legislatore europeo a ribadire che i dati personali possono essere condivisi con gli enti del settore pubblico solo in forma pseudonimizzata, nei casi in cui non siano sufficienti dati anonimi per rispondere all'emergenza pubblica di volta in volta invocata. Rispetto ai servizi di intermediazione dei dati e alle organizzazioni per altruismo dei dati, il parere sottolinea l'importanza di una condivisione dei dati affidabile e responsabile e raccomanda al legislatore europeo di mantenere talune specifiche garanzie, previste dall'attuale quadro giuridico, utili a favorire la trasparenza e la supervisione.

In materia di *enforcement*, il parere raccomanda, in particolare, l'introduzione di specifiche disposizioni volte a consentire lo scambio di informazioni tra le autorità competenti ai sensi del *Data Act* e le autorità regolatorie, incluse quelle di protezione dei

20

dati, ed esorta il legislatore europeo a chiarire le responsabilità e le competenze di queste ultime nella supervisione del RGPD.

Il CEPD e il GEPD accolgono anche con favore la conferma del ruolo del Comitato europeo per l'innovazione dei dati (EDIB) a sostegno della coerente attuazione del *Data Act*. In particolare, raccomandano di conferire alla Commissione europea il potere di emanare linee guida su qualsiasi argomento relativo al *Data Act* e di chiarire il ruolo dell'EDIB nel fornire assistenza alla Commissione in questo processo.

Norme procedurali aggiuntive per l'applicazione del RGPD

In data 12 dicembre 2025 è stato pubblicato il reg. 2025/2518 che stabilisce norme procedurali aggiuntive relative all'applicazione del RGPD. Il nuovo regolamento – che è entrato in vigore il 1° gennaio 2026 e troverà applicazione a partire dal 2 aprile 2027 – integra il RGPD e introduce norme relative allo svolgimento dei procedimenti da parte delle autorità di controllo nei casi riguardanti un trattamento transfrontaliero e da parte del CEPD in sede di composizione delle controversie.

Le nuove norme nascono dall'esigenza di potenziare la cooperazione fra autorità nella gestione dei casi transfrontalieri, con particolare riguardo agli aspetti procedurali e, anche alla luce dei suggerimenti elaborati dal CEPD in occasione del vertice di Vienna fra i presidenti delle autorità di protezione dati del SEE, tenutosi nel mese di aprile 2022 (v. Relazione 2022, p. 177), introducono diversi elementi procedurali volti ad armonizzare la trattazione dei casi transfrontalieri ovviando, per quanto possibile, alle divergenze esistenti nelle normative nazionali che, come è noto, possono rimanere impregiudicate purché non ostacolino l'implementazione della norma sovranazionale (in ottemperanza ai principi di effettività ed equivalenza).

In linea con la proposta originale della Commissione – sulla quale il CEPD ed il GEPD si erano espressi attraverso il parere congiunto (1/2023) del 19 settembre 2023 (v. Relazione 2023, p. 211) e la dichiarazione 4/2024 (v. Relazione 2024, p. 200) –, il nuovo regolamento, senza modificare il quadro di cooperazione previsto dal Capo VII del RGPD, lo integra prevedendo, in particolare: disposizioni sui criteri (formali) di ammissibilità dei reclami relativi a trattamenti transfrontalieri che dovranno essere valutati dall'autorità ricevente e trasmessi, da quest'ultima, all'autorità di controllo capofila (art. 4(1) e 5); una procedura di "risoluzione rapida" dei reclami (*early resolution*), attivabile sia dall'autorità che riceve un reclamo sia dall'autorità capofila (art. 5); una procedura di cooperazione semplice (art. 6) e una più dettagliata procedura di cooperazione nell'ambito dello sportello unico, aggiungendo ulteriori passaggi necessari a quanto già previsto dall'art. 60 del RGPD (artt. 10-11, 16, 19-20); la creazione di un fascicolo di cooperazione dedicato a ogni reclamo o indagine (art. 9), "non direttamente accessibile alle parti sottoposte a indagine, ai reclamanti o a terzi" (art. 26(2)) e di un fascicolo amministrativo dell'indagine su una presunta violazione del RGPD destinato a favorire la trasparenza nei confronti dei soggetti sottoposti alle indagini e dei reclamanti (artt. 24(3) e(4) e 25).

Il regolamento contiene alcuni termini ordinatori (art. 15) e numerose disposizioni che mirano a disciplinare l'esercizio del diritto di reclamanti e parti sottoposte alle indagini di essere ascoltati prima dell'adozione delle decisioni da parte delle autorità di controllo e, a seconda dei casi, del CEPD; inoltre, introduce disposizioni concernenti la procedura di risoluzione delle controversie dinanzi al Comitato ex art. 65 RGPD (artt. 27-30) e le procedure ex art. 66 RGPD (artt. 31-33), delimitando anche l'ambito delle "obiezioni pertinenti e motivate" che possono essere presentate dalle autorità competenti ai progetti di decisione predisposti dall'autorità capofila (art. 23).

Al fine di armonizzare la raccolta di informazioni circa l'attività svolta dalle

autorità e dal CEPD in questo ambito, il nuovo regolamento indica anche le informazioni di natura statistica che devono essere contenute nella relazione che il CEPD è tenuto a presentare annualmente ai sensi dell'art. 71 RGPD.

Migliori pratiche relative ai pareri ex art. 64, par. 2, RGPD

Al fine di rendere più agevole la cooperazione tra le autorità quando le stesse sono chiamate da una di esse o dalla Commissione europea ad esprimere un parere ai sensi dell'art. 64, par. 2, RGPD (parere che non costituisce un atto di per sé vincolante nei confronti dei terzi, come statuito dall'ordinanza del Tribunale dell'Unione europea del 29 aprile 2025, nella causa T-319/24), il CEPD ha aggiornato il proprio documento interno 3/2019 e ha allegato allo stesso alcune indicazioni di migliori prassi – che rappresentano un'intesa comune tra le autorità – su come razionalizzare il processo da seguire per la presentazione delle richieste di parere e la redazione degli stessi.

Il documento prevede che, prima di presentare una richiesta di parere, il soggetto proponente avvii discussioni informali in seno al CEPD per valutare la necessità e l'opportunità della richiesta, raccogliere indicazioni da parte delle altre autorità, valutare l'eventuale avvio di una consultazione pubblica (a livello nazionale o di CEPD), identificare le risorse per la predisposizione del parere.

La parte finale fornisce alcune migliori pratiche per la formulazione, la struttura e lo stile di tali pareri, nonché indicazioni per la loro predisposizione.

Linee guida relative all'interazione tra DSA e RGPD

Nel 2025 il CEPD ha adottato linee guida sull'interazione tra il *Digital Services Act* (DSA) e il RGPD, con l'obiettivo di favorire un'interpretazione coerente dei due strumenti nei casi in cui le disposizioni del DSA incidono sul trattamento di dati personali da parte dei fornitori di servizi intermediari.

Le linee guida chiariscono, in particolare, le basi giuridiche del trattamento connesse alle attività di moderazione dei contenuti illegali, evidenziando le condizioni in cui possono trovare applicazione le lett. c) o f) dell'art. 6, par. 1, RGPD. Vengono inoltre analizzati i meccanismi di *notice and action* e di gestione dei reclami, sottolineando l'esigenza di limitare la raccolta di dati personali allo stretto necessario e di garantire il rispetto dei diritti degli interessati.

Il documento affronta anche il tema dei *dark patterns*, chiarendo il rapporto tra il divieto previsto dal DSA e la disciplina RGPD, nonché le disposizioni in materia di pubblicità online, con particolare riguardo al divieto di utilizzo di categorie particolari di dati per finalità di *targeting*.

Ulteriori indicazioni riguardano i sistemi di raccomandazione, che possono comportare rischi significativi per i diritti degli interessati, anche in relazione all'art. 22 del RGPD, nonché la tutela dei minori sulle piattaforme online, con richiami alla necessità di soluzioni di *age assurance* proporzionate e rispettose della privacy.

Le linee guida evidenziano inoltre le implicazioni in materia di valutazioni d'impatto per i fornitori di piattaforme di grandi dimensioni e sottolineano l'importanza della cooperazione tra autorità di protezione dei dati, coordinatori dei servizi digitali e Commissione europea per garantire un'applicazione coerente dei due quadri normativi.

Le linee guida sono state sottoposte a consultazione pubblica, conclusasi il 31 ottobre 2025 e verranno riviste alla luce degli esiti della stessa.

Si segnala che, sempre con riferimento alla protezione dei minori online nell'ambito del DSA, il CEPD ha adottato il contributo (11 giugno 2025), in risposta alla consultazione pubblica avviata dalla Commissione europea il 13 maggio 2025 sulle proprie linee guida in merito alle misure per assicurare un alto livello di protezione della privacy e della sicurezza dei minori online in base all'art. 28(4) del DSA.

Concorrenza e tutela dei consumatori

Si è ulteriormente accresciuto l'impegno profuso dal Comitato nella riflessione sul rapporto tra protezione dei dati, diritto della concorrenza e tutela dei consumatori, questione sempre più rilevante a fronte delle crescenti sinergie tra questi diversi ambiti

20

(cfr. anche la sentenza della Corte di giustizia *Bundeskartellamt*, causa C-252/21).

Con il *Position Paper* sull'interazione tra protezione dei dati e diritto della concorrenza adottato il 16 gennaio 2025, il CEPD ha richiamato il ruolo significativo della cooperazione tra le autorità per la protezione dei dati personali e le autorità per la concorrenza nel sistema di protezione delle persone.

Il documento mette in evidenza la promozione di sinergie tra autorità per la protezione dei dati personali e della concorrenza allo scopo di migliorare la capacità di entrambi i regimi di proteggere interessati e utenti. Considerata la crescente importanza, per modelli di business delle aziende, dei dati personali, le norme applicabili al loro trattamento diventano sempre più centrali, così come le strategie per aumentare la coerenza di regolamenti che, seppur distinti, si collocano in rapporto sinergico. Tale evoluzione richiederà una migliore comprensione della relazione tra i concetti utilizzati nella normativa sulla protezione dei dati ed in quella sulla concorrenza, al fine di rafforzare la capacità delle rispettive autorità di tenere conto del contesto economico attuale, e, viceversa, di considerare profili di protezione dei dati rilevanti nelle loro valutazioni e decisioni.

Linee guida relative all'interazione tra DMA e RGPD

Nell'ambito delle attività che hanno riguardato le intersezioni inter-regolatorie, di particolare rilevanza sono state le linee guida sull'interazione tra la legge sui mercati digitali (DMA) e RGPD (v. Relazione 2024, p. 200). In linea con la strategia del Comitato per gli anni 2024-2027 e con gli obiettivi della dichiarazione di Helsinki, volti a semplificare la conformità al RGPD e a rafforzarne la coerenza, queste linee guida rappresentano il primo esercizio congiunto tra CEPD e Commissione europea. Approvate il 9 ottobre 2025, mirano ad agevolare l'applicazione coerente del DMA e del RGPD e ad accrescere la certezza del diritto per le grandi piattaforme digitali che forniscono servizi di base (come motori di ricerca online, app store e servizi di messaggistica, cd. *gatekeeper*) agli utenti commerciali e ai singoli individui.

Tali linee guida mettono in luce come sia il DMA che il RGPD tutelano gli individui nel panorama digitale, ma i loro obiettivi sono complementari: i diritti individuali e la protezione dei dati nel caso del RGPD e l'equità e la contendibilità dei mercati digitali ai sensi del DMA. Diverse attività regolate dal DMA comportano il trattamento di dati personali da parte dei *gatekeeper* e, in diverse diposizioni, il DMA fa esplicito riferimento a definizioni e concetti propri del RGPD. Le linee guida chiariscono come i *gatekeeper* possono attuare le previsioni del DMA in conformità con il diritto dell'UE in materia di protezione dei dati. In particolare, sono enucleati gli elementi che i *gatekeeper* devono tenere in considerazione per conformarsi all'obbligo di consentire agli utenti finali di effettuare una scelta libera ed esprimere un consenso valido per i trattamenti finalizzati a fornire servizi pubblicitari online, nonché per combinare o utilizzare i loro dati personali nei servizi principali della piattaforma. Le linee guida attengono anche ad altre disposizioni del DMA, tra cui quelle relative alla distribuzione di app e app store di terze parti, alla portabilità dei dati, alle richieste di accesso ai dati e all'interoperabilità dei servizi di messaggistica. Il Comitato e la Commissione hanno avviato una consultazione pubblica congiunta sul testo in parola, dando così l'opportunità alle parti interessate di fornire osservazioni e contributi.

Oltre a queste prime linee guida congiunte con la Commissione europea, il Comitato ha avviato quest'anno altri lavori di collaborazione e, in particolare, con l'ufficio per l'intelligenza artificiale (*AI Board*, previsto dal reg. sull'IA), in vista della stesura di linee guida congiunte sull'interazione tra il regolamento stesso e il diritto dell'UE in materia di protezione dei dati. L'obiettivo è quello di chiarire il nuovo quadro normativo europeo in materia di intelligenza artificiale mantenendo garanzie coerenti e uniformi per la protezione dei dati personali.

Sempre con riferimento al DMA, il CEPD ha continuato a seguire i lavori dell'*High Level Group* (HLG) istituito ai sensi dell'art. 40 del DMA, che riunisce trenta membri nominati da diversi regolatori e reti europee tra cui il GEPD e il CEPD, con l'obiettivo di fornire alla Commissione consulenza e competenze per garantire l'attuazione coerente e complementare della legge sui mercati digitali e degli altri regolamenti settoriali applicabili ai *gatekeeper* (v. Relazione 2023, p. 210).

DMA *High Level Group*

Tra le attività dell'HLG, cui il CEPD ha fornito specifico contributo, si segnala in particolare il documento di sintesi contenente una mappatura delle problematiche normative sollevate dall'IA in tutti i quadri regolatori supervisionati dai membri del Gruppo di alto livello, adottato il 12 dicembre 2025.

È proseguita l'attività interpretativa del CEPD relativa a concetti chiave del regolamento, volta a facilitarne l'applicazione coerente. In particolare con le linee guida 1/2025, il Comitato ha chiarito il concetto, l'applicabilità e i vantaggi della pseudonimizzazione che, definita dall'art. 4, par. 5, RGPD, costituisce una misura tecnica di mitigazione del rischio nel trattamento dei dati personali.

Linee guida 1/2025 su pseudonimizzazione

Le linee guida sottolineano che i dati pseudonimizzati, attribuibili a una persona fisica mediante l'uso di informazioni aggiuntive, costituiscono informazioni relative a una persona fisica identificabile e sono pertanto ancora dati personali. Inoltre, la pseudonimizzazione può ridurre i rischi per gli interessati facilitando dunque la possibilità di ricorrere alla base giuridica del legittimo interesse ai sensi dell'art. 6, par. 1, lett. f), RGPD, purché siano soddisfatti tutti gli altri requisiti del regolamento. Analogamente, la pseudonimizzazione può contribuire a garantire la compatibilità con la finalità originaria del trattamento (art. 6, par. 4, RGPD).

Le linee guida spiegano, tra l'altro, in che modo la pseudonimizzazione possa aiutare i titolari a soddisfare gli obblighi relativi all'attuazione dei principi di protezione dei dati, in particolare quelli di *privacy by design* e *by default* (art. 25) nonché gli obblighi di sicurezza (art. 32) e analizzano le misure tecniche e le garanzie che devono essere adottate per assicurare la riservatezza e impedire l'identificazione non autorizzata delle persone ove si utilizzino dati pseudonimizzati.

Sempre in linea con l'impegno adottato ad Helsinki di un maggiore coinvolgimento delle parti interessate, il Comitato ha organizzato un evento sui temi dell'anonimizzazione e della pseudonimizzazione, a seguito della sentenza della CGUE 4 settembre 2025 nel caso GEPD contro SRB (Caso C-413/23 P). L'evento, tenutosi online il 12 dicembre 2025, ha offerto l'opportunità di raccogliere i contributi di associazioni di settore, ONG, aziende, accademici e studi legali al fine di informare e supportare il lavoro in corso del Comitato su questi temi. È disponibile sul sito istituzionale del Comitato una relazione che riassume le principali questioni discusse nel corso dell'evento.

Stakeholders' event su anonimizzazione e pseudonimizzazione

Con riferimento ai trattamenti dei dati nell'ambito delle nuove tecnologie, l'8 aprile 2025, il CEPD ha adottato le linee guida 2/2025 in materia di *blockchain*, segnando un significativo passo avanti nel chiarire come le soluzioni basate sulla *blockchain* possano essere conformi al RGPD.

Linee guida 2/2025 sulle tecnologie *blockchain*

La natura distribuita dell'architettura di elaborazione dati tipica delle *blockchain* e i complessi concetti matematici coinvolti implicano un elevato grado di incertezza e sfide specifiche quanto al trattamento dei dati personali.

Le linee guida forniscono un quadro di riferimento per le organizzazioni che stanno valutando l'utilizzo della tecnologia *blockchain*, delineando le principali considerazioni di conformità al RGPD per le attività di trattamento previste. Forniscono una panoramica dei principi fondamentali della tecnologia *blockchain*, valutando le diverse architetture possibili e le loro implicazioni per il trattamento dei dati personali. Inoltre, chiariscono che i ruoli e le responsabilità dei diversi attori devono essere valutati in sede di

progettazione di un trattamento nel contesto della *blockchain* ed evidenziano la necessità di una protezione dei dati *by design* e *by default* nonché di misure organizzative e tecniche adeguate. Forniscono inoltre esempi di diverse tecniche per la minimizzazione dei dati e per il trattamento e la conservazione dei dati personali.

Come regola generale, la memorizzazione di dati personali su una *blockchain* dovrebbe essere evitata se in conflitto con i principi di protezione dei dati. Le linee guida illustrano in dettaglio gli aspetti tecnici e le modalità di implementazione delle diverse tecniche in conformità ai principi di protezione dati, evidenziandone i punti di forza e di debolezza per aiutare le organizzazioni a scegliere le misure più appropriate.

Infine, le linee guida evidenziano l'interazione tra gli aspetti tecnici della *blockchain* e i principi di protezione dei dati di cui all'art. 5 del RGPD, l'importanza dei diritti degli interessati (in particolare alla trasparenza, rettifica e cancellazione) nonché l'importanza della valutazione d'impatto sulla protezione dei dati (DPIA) prima di implementare un trattamento che utilizzi la tecnologia *blockchain*.

Age assurance

Il CEPD ha concluso il lavoro concernente i sistemi di verifica dell'età, tema centrale della tutela dei minori online. La dichiarazione 1/2025, adottata l'11 febbraio 2025, si propone di fornire un quadro generale dei principi di protezione dati che devono essere rispettati nei trattamenti relativi all'approntamento di sistemi di *age assurance*.

L'intento della dichiarazione – che si rivolge ai diversi attori coinvolti – è di fornire indicazioni che promuovano soluzioni non intrusive, anche tenendo conto della proliferazione dei forum attualmente impegnati a discutere di questa tematica e delle molte soluzioni proposte dall'industria, sovente non in linea con un approccio rispettoso della protezione dei dati.

Meccanismi nazionali di certificazione della protezione dati

Nel 2025 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 3/2025 sul progetto di decisione dell'autorità di controllo francese di approvazione dei criteri di certificazione Lexing, applicabili in Francia per la certificazione di trattamenti effettuati da titolari e responsabili; il parere 15/2025 sul progetto di decisione dell'autorità di controllo austriaca di approvazione dei criteri di certificazione predisposti da BDO Consulting GmbH, consentendone così il loro utilizzo in Austria sempre per la certificazione di titolari e responsabili nonché il parere 34/2025 sul progetto di decisione dell'autorità di controllo greca di approvazione dei criteri per la certificazione di conformità al RGPD delle operazioni di trattamento di dati dei dipendenti redatti dal Centro di diritto costituzionale europeo (CECL). Questi ultimi sono applicabili in Grecia per la certificazione di trattamenti effettuati da titolari in ambito lavorativo.

Codice mondiale antidoping

Su richiesta della Commissione europea, il CEPD è tornato ad esprimersi sul trattamento dei dati personali a fini antidoping (v. lettera inviata dal presidente del CEPD alla presidenza del Consiglio dell'UE il 9 ottobre 2019) con le raccomandazioni 1/2025 sulla revisione del codice mondiale antidoping e dei suoi standard internazionali per il 2027 condotta dall'agenzia mondiale antidoping (WADA). Nelle raccomandazioni, il CEPD sottolinea come in tale ambito sia essenziale tutelare i dati personali degli atleti considerato in particolare che, in molti casi, tali trattamenti coinvolgono dati personali sensibili e, tra questi, dati sanitari concernenti i campioni biologici prelevati agli atleti. Il codice e gli standard antidoping si propongono di assoggettare le organizzazioni nazionali antidoping (NADO) a uno standard equivalente a quello del RGPD nel trattamento dei dati personali a fini antidoping. In tale contesto, l'obiettivo perseguito dalle raccomandazioni è quello di valutare la compatibilità con il CEPD del codice antidoping della WADA e, in particolare, dello standard internazionale per la protezione dei dati (ISDP). Le raccomandazioni del CEPD analizzano i principi fondamentali della

protezione dei dati, come la necessità di una base giuridica appropriata per il trattamento dei dati personali degli atleti, mettendo in dubbio che questa possa essere rappresentata dal consenso, nonché la limitazione delle finalità e della conservazione. Le raccomandazioni sottolineano poi che gli atleti devono essere pienamente informati sul trattamento dei propri dati personali, inclusa la raccolta di informazioni grezze e di intelligence a fini antidoping, e debbono poter esercitare efficacemente i propri diritti.

Trasferimenti di dati - adeguatezza dell'OEB

Larga parte dell'attività svolta dal CEPD nel 2025 in materia di trasferimenti di dati all'estero è stata dedicata alla predisposizione e adozione dei pareri sulle proposte di decisione di adeguatezza presentate dalla Commissione europea ai sensi dell'art. 45 del RGPD.

Nel parere 7/2025 adottato sulla proposta di decisione relativa all'Organizzazione europea dei brevetti (OEB), il CEPD ha sottolineato che tali decisioni "costituiscono un solido strumento di trasferimento per garantire che i diritti dell'interessato siano tutelati quando i dati personali sono trasferiti al di fuori del SEE" non solo verso paesi terzi ma anche verso organizzazioni internazionali. Ed è proprio nei confronti dell'OEB che, con decisione di esecuzione 2025/1382 del 15 luglio 2025, la Commissione europea ha adottato la sua prima decisione relativa ad un'organizzazione internazionale, riconoscendo che il suo quadro giuridico – ampiamente allineato con quello dell'UE – fornisce un livello di protezione adeguato. In particolare, il CEPD, nel condividere larga parte della proposta di decisione della Commissione, aveva chiesto alla stessa di meglio chiarire il regime di *governance* in materia di protezione dei dati interno all'organizzazione, le garanzie in caso di trasferimento ulteriore dei dati verso paesi terzi, i poteri investigativi e correttivi previsti nell'ambito del sistema di sorveglianza sul rispetto delle regole di protezione dati e l'accesso del governo ai dati personali trasferiti dall'UE.

Rispetto a questo ultimo aspetto, è stata sottolineata la peculiarità della valutazione effettuata in relazione all'adeguatezza relativa a un'organizzazione internazionale e le garanzie previste anche alla luce della interazione tra le regole sui privilegi e le immunità dell'Organizzazione nonché l'obbligo di cooperare con gli Stati contraenti. Al riguardo il CEPD ha invitato la Commissione a monitorare se tali richieste saranno ricevute in futuro e in che modo le norme pertinenti saranno applicate.

Trasferimenti di dati - adeguatezza del Regno Unito in ambito RGPD e LED

Sempre in tema di adeguatezza, il CEPD è stato chiamato a fornire i propri pareri a norma dell'art. 70, par. 1, lett. s), RGPD e dell'art. 51, par. 1, lett. g), LED (direttiva 2016/680 - *Law Enforcement Directive*), sui progetti relativi alla proroga della validità delle decisioni di adeguatezza del Regno Unito adottate dalla Commissione europea il 28 giugno 2021. Per verificare se il livello di protezione dei dati nel Regno Unito possa ancora essere considerato "adeguato", la Commissione ha rivalutato l'ordinamento britannico alla luce delle numerose modifiche normative intervenute a seguito della Brexit e della modifica, a giugno 2025, della disciplina specifica in materia di protezione dei dati. Dopo l'adozione, il 24 giugno 2025, di due decisioni volte a prorogare di sei mesi la durata delle precedenti (per consentire la definizione del quadro giuridico rilevante), il 22 luglio dello stesso anno la Commissione europea ha pubblicato due ulteriori proposte di modifica delle precedenti decisioni di adeguatezza volte a prorogare di sei anni la clausola di caducità ivi contenuta.

Nel parere adottato ai sensi del RGPD (26/2025), il CEPD si è concentrato sia sulla valutazione del quadro giuridico e delle norme sulla protezione dei dati applicabili nel Regno Unito, sia sulle regole relative all'accesso da parte delle autorità pubbliche britanniche ai dati personali trasferiti dal SEE e sui mezzi di ricorso a disposizione delle persone fisiche.

Il parere accoglie con favore il perdurante allineamento tra il quadro giuridico britannico in materia di protezione dei dati e quello dell'UE, e si sofferma, in particolare,

20

sugli aspetti per i quali ritiene necessario un chiarimento da parte della Commissione europea (quali le norme che disciplinano il trasferimento dei dati personali e quelle che hanno determinato la ristrutturazione dell'ufficio del commissario per l'informazione nonché riformato la nomina e la revoca dei suoi membri) o un monitoraggio sull'applicazione della nuova normativa. Attenzione è stata richiesta in merito alle modifiche introdotte dal *Retained EU Law (Revocation and Reform*) Act 2023 (REUL Act), con cui il Regno Unito ha rivisto il quadro giuridico generale "ereditato" dall'UE, eliminando il principio del primato del diritto dell'UE (anche se con talune garanzie per alcune disposizioni del RGPD) e l'applicazione diretta dei principi del diritto dell'UE. Analoga cura dovrà essere prestata rispetto a quei settori nei quali la nuova normativa prevede la possibilità di introdurre modifiche attraverso l'adozione di regolamenti adottati dal *Secretary of State* (soggetti ad un minore controllo parlamentare), nonché in merito all'applicazione dei poteri correttivi e all'efficacia delle sanzioni e dei mezzi di ricorso per le parti interessate.

In materia di accesso delle autorità governative ai dati personali trasferiti dal SEE al Regno Unito, il parere nota che il nuovo assetto normativo prevede esenzioni estese per la sicurezza nazionale e chiede che la Commissione svolga una più attenta valutazione al riguardo e monitori l'applicazione di tali esenzioni, con particolare riguardo al rispetto del principio di proporzionalità, nonché all'obbligo di trattare i dati personali per una finalità legittima.

Nel parere adottato in ambito LED (27/2025), il CEPD esamina le modifiche normative intervenute dopo l'adozione della precedente decisione di adeguatezza. In particolare, oltre al tema dei trasferimenti ulteriori e delle deroghe per motivi di sicurezza nazionale a favore delle autorità di contrasto, invita la Commissione a valutare criticamente l'impostazione più permissiva delle disposizioni in materia di processo decisionale automatizzato. Tale disciplina, infatti, attribuisce nuovi poteri al *Secretary of State*, riconoscendogli un ampio margine discrezionale nella definizione di ciò che debba intendersi per "intervento umano significativo" e per "decisione significativa con effetti analogamente rilevanti". Il parere invita, inoltre, la Commissione a monitorare affinché il regime di protezione dei dati previsto per i trattamenti connessi alla sicurezza nazionale non venga indebitamente esteso a contesti estranei a tale ambito. Alcune disposizioni del nuovo quadro normativo consentono, in taluni casi, di ricondurre le attività di trattamento svolte dalle autorità competenti in materia di *law enforcement* nell'ambito delle norme applicabili alle autorità di sicurezza nazionali, ossia, in pratica, di limitare l'applicazione della normativa in materia di protezione dei dati personali.

Trasferimenti di dati - adeguatezza del Brasile

Nel 2025, la Commissione ha anche presentato un progetto di decisione volto a riconoscere l'adeguatezza del quadro giuridico brasiliano. Al riguardo, il CEPD, con parere 28/2025, ha rilevato con soddisfazione che la disciplina in materia di protezione dei dati, insieme ai decreti presidenziali e ai regolamenti vincolanti emanati dall'autorità brasiliana per la protezione dei dati è fortemente allineata ai requisiti in materia di protezione dei dati contenuti nel RGPD. Il parere individua pochi ambiti nei quali fare maggiore chiarezza e tra questi le tipologie di trattamenti per cui richiedere la valutazione d'impatto sulla protezione dei dati e il ruolo del consiglio nazionale per la protezione dei dati personali e la privacy (uno degli organismi di cui fa parte l'autorità brasiliana) e la sua interazione con l'autorità di protezione dei dati (ANPD). Per quanto riguarda l'accesso da parte delle autorità pubbliche brasiliane ai dati personali trasferiti dall'UE per finalità di *law enforcement* e sicurezza nazionale, il CEPD rileva positivamente che la Corte suprema federale del Brasile, nella sua giurisprudenza, ha interpretato la legge in materia di protezione dei dati in modo da ampliarne l'applicabilità parziale al trattamento dei dati personali effettuato per le indagini penali e il mantenimento dell'ordine pubblico

e invita la Commissione a chiarire ulteriormente l'applicabilità della disciplina in caso di trattamento di dati personali a fini di *law enforcement* in ambito penale, compresi i poteri investigativi e correttivi dell'autorità, nonché a prendere attentamente in considerazione qualsiasi sviluppo pertinente del quadro giuridico esistente a tale riguardo.

Trasferimenti di dati - incontro con le autorità dei paesi adeguati

Dopo la prima riunione con i commissari e i rappresentanti delle autorità di protezione dei dati dei paesi terzi che beneficiano di una decisione di adeguatezza da parte della Commissione svoltasi nel 2024 (v. Relazione 2024, p. 204), il CEPD ha rafforzato la propria cooperazione con tali autorità condividendo informazioni e raccogliendo esperienze sulla cooperazione internazionale in materia di *enforcement* delle discipline di protezione dei dati. In questo contesto, il 3 dicembre 2025 si è tenuta la seconda riunione che ha visto anche la partecipazione dei rappresentanti dell'Organizzazione europea dei brevetti e ha offerto a tutti i partecipanti l'opportunità di condividere opinioni sulle attività passate e aggiornamenti sulle prossime priorità in materia di *enforcement*.

Trasferimenti di dati - linee guida art. 48 del RGPD

All'esito della consultazione pubblica è stato adottato il testo definitivo delle linee guida 2/2024 sull'art. 48 del RGPD che chiariscono le condizioni alle quali i titolari e i responsabili del trattamento possono rispondere alle richieste di dati personali provenienti da autorità di paesi terzi (v. Relazione 2024, p. 201). Il testo rivisto specifica, tra l'altro, che non rientra nell'ambito di applicazione dell'art. 48 del RGPD il caso in cui la richiesta da parte delle autorità di un paese terzo raggiunga la capogruppo stabilita nel medesimo paese terzo e quest'ultima, per poter rispondere alla richiesta, chieda i dati in questione ad una sua controllata nel SEE. In tale situazione, la società controllata, in quanto società esportatrice, deve conformarsi al RGPD e potrà trasferire i dati in questione solo dopo aver individuato un'idonea base giuridica ai sensi dell'art. 6 e un idoneo strumento di trasferimento ai sensi degli artt. 45 e ss. del RGPD.

Trasferimenti di dati - BCR

Rispetto agli anni precedenti, il 2025 ha visto un incremento dell'attività del CEPD per la verifica della conformità ai requisiti previsti dall'art. 47 del RGPD delle norme vincolanti d'impresa (BCR) presentate per approvazione alle autorità competenti. Nel rispetto di quanto previsto dall'art. 64, par. 1, lett. f), RGPD, sono stati adottati diciotto pareri in merito a BCR per titolari del trattamento (valutate alla luce delle raccomandazioni 1/2022 riviste nel 2023) e sette BCR per responsabili del trattamento (valutate ancora alla luce del WP 257.rev.01). Tenuto conto dell'esperienza maturata a partire dall'applicazione del RGPD, il 13 marzo 2025, il CEPD ha inoltre rivisto la procedura di cooperazione per l'approvazione delle BCR.

Seconda dichiarazione sull'attuazione della direttiva PNR

Con la dichiarazione sull'attuazione della direttiva (UE) 2016/681 adottata il 14 marzo 2025, alla luce della sentenza della CGUE C-817/19, il CEPD fornisce alle Unità d'informazione sui passeggeri nazionali ulteriori raccomandazioni sui necessari adeguamenti e limitazioni al trattamento dei dati del codice di prenotazione, in aggiunta a quelle già espresse nella dichiarazione del 15 dicembre 2022. Le raccomandazioni riguardano alcuni aspetti chiave della sentenza PNR, tra cui: le categorie di dati rientranti nell'ambito di applicazione della direttiva PNR, specie con riferimento ai terzi non passeggeri; il collegamento oggettivo tra i reati e i viaggi aerei; il modo in cui i paesi europei dovrebbero selezionare i voli da cui vengono raccolti i dati del codice di prenotazione; l'informativa da fornire agli interessati sui rimedi disponibili; il controllo preventivo per le richieste di comunicazione dei dati PNR e il periodo di conservazione di questi ultimi. Secondo il CEPD, il periodo di conservazione di tutti i dati PNR non dovrebbe superare un periodo di sei mesi. Trascorso tale periodo, i paesi europei possono conservare i dati del codice di prenotazione solo per il tempo necessario e proporzionato agli obiettivi della direttiva PNR. Il CEPD registra una sostanziale mancanza di sforzi di attuazione normativa delle indicazioni della Corte di giustizia. Pertanto, sottolinea l'urgente necessità di implementare le modifiche legislative necessarie per

adeguare gli ordinamenti nazionali all'orientamento espresso nella sentenza PNR, richiamando, da un lato, la responsabilità della Commissione europea nel monitorare tale processo di adeguamento e, dall'altro, il diritto delle autorità di controllo di adottare misure adeguate in caso di persistente contrasto giuridico.

Nel corso del 2025 le autorità di protezione dei dati dello SEE (tra cui il Garante) hanno avviato indagini coordinate sulla conformità dei titolari del trattamento alle disposizioni del RGPD in materia di diritto alla cancellazione.

CEF 2025 diritto alla cancellazione

Il *Coordinated Enforcement Framework* (CEF) 2025 ha coinvolto complessivamente 764 titolari del trattamento, tra piccole, medie e grandi imprese operanti in tutta Europa. Nove autorità hanno avviato o proseguito attività istruttorie, mentre le restanti 23, tra cui il Garante, hanno condotto indagini conoscitive. L'iniziativa mirava a verificare l'effettivo esercizio del diritto alla cancellazione da parte dei cittadini europei e a valutare le modalità con cui i titolari ne garantiscono l'attuazione. Al termine dell'attività, il CEPD ha individuato buone pratiche e principali criticità, tra le quali meritano di essere segnalati:

- la carenza di procedure interne adeguate alla gestione delle richieste;
- l'insufficienza delle informazioni fornite agli interessati;
- il ricorso a tecniche di anonimizzazione non efficaci come alternative alla cancellazione;
- difficoltà nell'individuazione dei tempi di conservazione dei dati e nella gestione della cancellazione, in particolare nel contesto dei backup;
- criticità nell'effettuare i necessari bilanciamenti con altri diritti, atteso che il diritto alla cancellazione non ha carattere assoluto.

Affari finanziari

L'attività del CEPD è proseguita 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. Merita ricordare, in tale ambito, i lavori volti alla predisposizione di un documento concernente l'art. 75 del reg. 2024/1624, che prevede lo scambio di informazioni nel quadro di partenariati tra diversi soggetti istituzionali e privati ai fini dell'adempimento degli obblighi in materia di antiriciclaggio e contrasto al finanziamento del terrorismo (AML/CFT), nonché di uno specifico documento concernente le cd. *watchlist*, database che contengono informazioni sulle attività economico finanziarie di diversi soggetti, di cui si avvalgono i cd. soggetti obbligati (*obliged entities)*, per adempiere agli obblighi di monitoraggio previsti dalla normativa AML/CFT.

Account nelle piattaforme di e-commerce

Si segnala l'adozione, avvenuta il 3 dicembre 2025, delle raccomandazioni 2/2025 concernenti la base giuridica necessaria alla creazione di account da parte di utenti nelle piattaforme di e-commerce, oggetto anche di una consultazione pubblica chiusasi il 12 febbraio 2026.

Il documento risponde all'esigenza di offrire chiarimenti riguardo ad una prassi, piuttosto comune, consistente nel richiedere agli utenti la creazione di account per poter accedere alle offerte o acquistare beni e servizi. Pur riconoscendo l'interesse commerciale di tale prassi nel settore dell'e-commerce, il CEPD la ritiene foriera di rischi ulteriori ai danni degli interessati.

Sono state pertanto fornite raccomandazioni sulle condizioni in base alle quali i titolari che operano nel settore possono legittimamente richiedere ai propri utenti di creare un account ai sensi degli artt. 5, par. 1, lett. a) e 6 RGPD. In particolare, il documento fornisce esempi in cui la creazione "obbligatoria" di un account può o meno essere ritenuta necessaria per l'esecuzione di un contratto (art. 6, par. 1, lett. b), RGPD) o per il rispetto di un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, par. 11, lett. c), RGPD) o per il perseguimento di un interesse legittimo del titolare del trattamento o di un terzo (art. 6, par.1, lett. f), RGPD). Il CEPD rileva che imporre la

creazione di un account può essere giustificato solo per un insieme molto limitato – sebbene non esaustivo – di finalità, come offrire un servizio in abbonamento o fornire accesso a offerte esclusive. Fornire agli utenti la facoltà di creare un account oppure di continuare a navigare e acquistare come "ospite" (*guest mode*) appare il modo più efficace per garantire il corretto trattamento dei dati personali sui siti di e-commerce, in conformità con l'obbligo di protezione dei dati fin dalla progettazione e per impostazione predefinita ai sensi dell'art. 25 del RGPD.

È proseguita l'attività del CEPD in materia di euro digitale, già oggetto del parere congiunto CEPD/GEPD 2/2023. Nella consapevolezza che le decisioni riguardanti il design della moneta digitale hanno implicazioni significative per i diritti e le libertà degli individui europei, il Comitato ha richiesto a un esperto, nell'ambito del progetto "*Support Pool of Experts* - SPE", di effettuare una valutazione approfondita sulla fattibilità pratica della "modalità offline basata su token", già supportata dal CEPD. Il rapporto, pubblicato sul sito del CEPD, esplora le limitazioni intrinseche, gli approcci possibili e le considerazioni sulla sicurezza relative allo sviluppo di una modalità offline per l'euro digitale che sia simile al contante, anonima e resistente al doppio utilizzo.

20.2. *La cooperazione delle autorità di protezione dati nel settore libertà, giustizia e affari interni*

Nel periodo considerato la trattazione di affari a carattere sovranazionale, anche in relazione all'attività dei gruppi di lavoro in sede europea di interesse per l'attività di polizia e di cooperazione in ambito giudiziario, ha visto un crescente impegno dell'Autorità.

20.2.1. Comitato di controllo coordinato (CSC)

Il CSC, come è noto, è costituito dai rappresentanti delle autorità di controllo nazionali e del GEPD e garantisce la vigilanza coordinata dei sistemi IT su larga scala e degli organi, uffici e agenzie dell'UE, in conformità all'art. 62 del reg. (UE) 2018/1725 (EUDPR).

Il mandato del Comitato, oltre alle competenze di supervisione già assegnate riguardo a IMI, EUROJUST, EPPO, EUROPOL, SIS, Prüm II, VIS, EES ed ETIAS, è stato esteso, per via del richiamo al predetto art. 62 del EUDPR, anche a diversi sistemi informativi, non strettamente legati a questioni di sicurezza, frontiere e immigrazione e giustizia, quali quelli previsti dal regolamento recante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (reg. (UE) 2023/2854, cd. *Data Act*), il regolamento di esecuzione sugli obblighi di comunicazione ai fini del meccanismo di adeguamento del carbonio alle frontiere durante il periodo transitorio (reg. (UE) 2023/1773), il reg. di esecuzione sull'istituzione e il funzionamento degli spazi di sperimentazione normativa per l'interoperabilità (reg. di esecuzione (UE) 2025/1420).

Su invito del Comitato, la Commissione ha presentato un quadro d'insieme degli atti normativi europei istitutivi di sistemi informativi che forniscono la base giuridica del controllo coordinato a opera del CSC, precisando che per tali sistemi si prevedono meccanismi di supervisione condivisa tra istituzioni europee e autorità nazionali di controllo in relazione al trattamento dei dati nonché l'obbligo di consultazione del GEPD. In proposito, è stato richiesto alla Commissione di fornire specifiche informazioni con particolare riguardo ai trattamenti di dati effettuati attraverso i suddetti sistemi informativi, dal momento che tale ampliamento di competenze del Comitato ha dirette ripercussioni sulle risorse da impiegare sia a livello nazionale che a livello europeo tramite il Segretariato.

EES

Il sistema EES (*Entry/Exit System*) – istituito dal reg. (UE) 2017/2226 e finalizzato a registrare gli ingressi e le uscite dei cittadini di paesi terzi ai confini esterni dell'area Schengen – è entrato in funzione, in modo graduale, a partire dal 12 ottobre 2025 con l'obiettivo di migliorare la gestione delle frontiere e supportare l'attività di contrasto al terrorismo ed alla criminalità organizzata.

L'operatività del sistema di ingressi/uscite, a causa di ritardi da parte di alcuni Stati membri a livello tecnico, è stata posticipata rispetto a quella originariamente prevista stabilendo un'introduzione graduale ai valichi di frontiera, in conformità al reg. (UE) 2025/1534 del 18 luglio 2025, su cui il GEPD ha reso il parere 3/2025. La piena attuazione del sistema informativo dovrà avvenire entro il 10 aprile 2026 (cfr. al riguardo il par. 8.3 della presente Relazione in merito al parere reso dal Garante sul decreto interministeriale per l'attuazione del sistema EES a livello nazionale).

L'avvio del sistema è stato accompagnato da una campagna informativa dedicata della quale si è occupata la Commissione, in collaborazione con le autorità di controllo e il GEPD in conformità all'art. 51 del reg. EES. A tal riguardo, i membri del Comitato hanno avuto diverse interlocuzioni con la Commissione e, anche tramite l'attività di input da parte del gruppo di lavoro specifico del CSC su EES (di cui fa parte anche il Garante), hanno provveduto a rivedere i materiali informativi (sia cartacei sia quelli pubblicati sul sito web della Commissione, Travel4EES).

Nel quadro del coordinamento interno delle attività di supervisione, i rappresentanti delle autorità si sono confrontati sullo stato di attuazione del sistema EES a livello nazionale, nell'ottica di attenzionare elementi di criticità ed elaborare una risposta coerente. In proposito, a titolo esemplificativo, i membri hanno deciso di sviluppare una guida per l'esercizio dei diritti degli interessati in EES, dandone mandato al gruppo di lavoro su EES.

ETIAS

L'autorizzazione ai viaggi ETIAS (sistema dell'UE di informazione e autorizzazione ai viaggi, istituito dal reg. (UE) 2018/1240) è un requisito d'ingresso per i cittadini esenti dall'obbligo di visto che viaggiano nello spazio Schengen o a Cipro, per soggiorni di norma non superiori a 90 giorni su un periodo di 180 giorni. L'entrata in funzione del sistema è prevista per l'ultimo trimestre del 2026.

Con riguardo a tale sistema informativo, il Comitato ha proseguito la riflessione avviata nel corso del 2024 relativa all'interpretazione della nozione di "destinatario" dei dati ai sensi dell'art. 4(9) del RGPD, nell'ambito del riscontro a una eventuale richiesta di accesso ex art. 15 RGPD formulata da parte degli interessati ai dati trattati in ETIAS, in particolare nella misura in cui le autorità competenti che abbiano avuto accesso a tali dati debbano essere ritenute "destinatarie" dei dati stessi. È stato approfondito a tale riguardo il ruolo del punto di accesso centrale rispetto alle richieste di consultazione dei dati ETIAS e la questione del regime giuridico di riferimento (RGPD o la direttiva 2016/680).

È inoltre continuato l'approfondimento della questione relativa alla titolarità del trattamento dei dati in ETIAS, quale contributo al lavoro di FRONTEX sulla valutazione di impatto (DPIA) e sulla gestione delle istanze di esercizio da parte degli interessati, allo scopo di chiarire la ripartizione di responsabilità tra l'Unità centrale e le Unità nazionali ETIAS ai sensi dell'art. 57 del reg. ETIAS. In particolare, il gruppo di lavoro specifico su ETIAS ha presentato al CSC una nota nella quale vengono valutati gli argomenti a favore e quelli contrari all'ipotesi di una co-titolarità del trattamento ovvero di una titolarità successiva. I membri del Comitato hanno deciso di proseguire il lavoro tramite un'analisi dettagliata dei flussi di dati e la preparazione di una dichiarazione che riflette la posizione del CSC sul concetto di "titolarità retroattiva" del trattamento, ipotizzata dalla Commissione a cui FRONTEX ha specificamente rivolto un quesito.

FRONTEX ha inoltre presentato una soluzione tecnica per lo scambio di informazioni tra le Unità (centrale o nazionali ETIAS) e le autorità di protezione dei dati nazionali in attuazione dell'art. 64(6) del reg. ETIAS secondo il quale le Unità ETIAS devono tenere un registro scritto relativo alle istanze di esercizio dei diritti degli interessati ricevute e ai relativi esiti da mettere a disposizione delle autorità di controllo.

È stato avviato un progetto pilota relativo a tale applicativo per testarne la funzionalità ed evidenziare eventuali criticità, a cui i membri del Comitato sono stati invitati a partecipare.

EUROPOL

È proseguita l'attività di supervisione congiunta relativa al trattamento dei dati di minori (under 15) sospettati di aver commesso un reato di competenza di EUROPOL. Il report finale è stato infine adottato dal Comitato.

Nel corso delle riunioni del CSC, i membri sono stati altresì periodicamente aggiornati dal GEPD sui pareri resi e sull'attività di supervisione condotta relativa ad EUROPOL. In particolare, si segnalano, tra gli altri: il parere reso sulla proposta di regolamento sul potenziamento del sostegno di EUROPOL e sul rafforzamento della cooperazione di polizia per prevenire e combattere il traffico di migranti e la tratta di esseri umani (reg. (UE) 2025/2611); il parere reso, dietro consultazione preventiva, sullo sviluppo e l'uso di modelli di *machine learning* per le analisi operative; il parere reso sull'attuazione di ETIAS in merito alle procedure per inserire i dati nell'elenco di controllo (cd. *watchlist*).

Il GEPD ha inoltre riferito in merito all'attività di ispezione annuale di EUROPOL relativa al 2025, che si è tenuta nel mese di luglio, con la partecipazione di due rappresentanti delle autorità di controllo e che ha riguardato l'utilizzo del SIS, il trattamento di dati di riconoscimento facciale e il trasferimento di dati ai paesi terzi ed organizzazioni internazionali.

È stato infine deciso di istituire un apposito gruppo di lavoro, interno al Comitato al pari di quelli già avviati per EES ed ETIAS, per approfondire le tematiche legate alla cooperazione giudiziaria e di polizia ed in particolare fornire una prima analisi delle informazioni rese dal GEPD nell'ambito dei pareri resi in sede di consultazione preventiva per identificare punti di comune interesse.

EUROJUST

È proseguita l'attività di raccolta di informazioni tramite il questionario relativo alle difficoltà registrate dalle autorità di controllo nella supervisione delle autorità giudiziarie nazionali in relazione a EUROJUST. È stato sottolineato che le modalità di trasposizione a livello nazionale dell'art. 45 della direttiva (per l'Italia: art. 37, comma 6, d.lgs. n. 51/2018) impattano sull'attività di supervisione. In particolare è stato al riguardo deciso di veicolare le criticità rilevate nell'ambito dell'esercizio di valutazione della direttiva lanciato dalla Commissione e rispetto al quale il CEPD fornirà il suo contributo. Successivamente, è stato predisposto un nuovo questionario per ricomprendere alcuni profili che non erano stati inseriti nel precedente, di cui verranno analizzate le risposte una volta che tutte le autorità di supervisione avranno fatto pervenire le rispettive osservazioni.

I membri del Comitato hanno inoltre preso contatti con il RPD di EUROJUST che, invitato a una delle riunioni, ha fornito alcuni aggiornamenti principalmente in merito alle clausole di protezione dei dati inserite negli accordi sulle squadre di investigazione comuni o *Joint Investigation Teams* (cd. JITs) e al ruolo di EUROJUST come punto di contatto rispetto al sistema informativo sui casellari giudiziari o ECRIS-TCN, in particolare sulle finalità connesse all'accesso di EUROJUST a tale database e la necessità di maggiore chiarezza circa gli strumenti e le procedure utilizzate, con il possibile supporto della Commissione e di eu-LISA. Su quest'ultimo tema, nell'ambito della discussione che ne è seguita, il GEPD ha presentato il proprio parere sul ruolo di EUROPOL come punto di contatto nel contesto del sistema ECRIS-TCN che ruota intorno all'interpretazione dell'art. 17 del reg. (UE) 2019/816.

20

Il GEPD ha inoltre aggiornato i membri del Comitato sulle conclusioni raggiunte attraverso l'attività ispettiva sulla banca dati delle prove di crimini internazionali fondamentali (*Core International Crimes Evidence Database* - CICED), con particolare riferimento al trattamento di categorie particolari di dati e all'esercizio dei diritti degli interessati.

SIS

Si è discusso ampiamente in ambito CSC circa la modalità di gestione delle attività di verifica dei log di cui all'art. 12 del reg. SIS (*Schengen Information System*) al fine di uniformare gli approcci utilizzati dalle autorità di controllo e identificare alcune *best practice*. Il documento adottato dai membri costituirà la base di un dialogo con la Commissione. Al contempo è stato deciso di predisporre linee guida per il controllo dei log ai sensi del predetto art. 12 per le autorità competenti nazionali, secondo un approccio pratico. È stata altresì predisposta una raccomandazione sul calcolo del ciclo temporale per condurre gli audit nell'ambito dei sistemi informativi europei su larga scala, che ha un ruolo centrale anche nell'ambito delle valutazioni periodiche Schengen. Il documento approvato dal CSC è stato inoltrato alla Commissione ed è consultabile sul sito del CEPD.

Il Garante ha poi contribuito all'elaborazione del *Joint Report of Schengen Information System 2024* raccogliendo sia i dati nazionali di competenza dell'Autorità che quelli messi a disposizione dal Ministero dell'interno, in ottemperanza all'obbligo recentemente introdotto per gli Stati membri di comunicare al CEPD entro il 31 marzo di ogni anno le statistiche sull'esercizio dei diritti degli interessati relative al SIS. In particolare sono state rendicontate le richieste di accesso, rettifica e cancellazione.

Nel periodo considerato, in relazione alle attività di controllo riservate all'Autorità sui trattamenti effettuati sui dati personali registrati nel SIS, il Garante ha continuato a curare il monitoraggio del periodico flusso di istanze e comunicazioni provenienti dagli interessati e dalle autorità coinvolte (Dipartimento della PS - Servizio informativo interforze - Divisione NSIS), al fine di verificare che l'elaborazione e l'utilizzazione dei dati inseriti negli archivi SIS non leda i diritti delle persone ai sensi degli artt. 52, 53 e 54 del reg. (UE) 2018/1861, e 67 e 68 del reg. (UE) 2018/1862, in relazione alle disposizioni nazionali pertinenti del d.lgs. n. 51/2018.

Infine, con riguardo agli aspetti di comunicazione istituzionale di competenza, l'Autorità ha provveduto alla predisposizione ed alla pubblicazione sul proprio sito istituzionale dei contenuti descrittivi del SIS e delle corrette modalità di esercizio dei diritti di accesso, rettifica e cancellazione relativi ai dati personali contenuti in tale sistema da parte degli interessati. Poiché i diritti in questione sono esercitati mediante richieste indirizzate al Ministero dell'interno - Dipartimento della pubblica sicurezza (autorità centrale competente sulla sezione nazionale del SIS), sono state avviate proficue interlocuzioni tra l'Autorità e tale Dicastero al fine di definire modelli condivisi, in linea con le indicazioni rese a livello europeo.

EURODAC

Con riferimento al Sistema informativo EURODAC – dal 2026 anch'esso ricompreso nell'attività di supervisione del CSC – il gruppo di supervisione ha seguito lo stato di attuazione del nuovo reg. EURODAC (reg. (UE) 1358/2024), in vigore dal 12 giugno 2026; tale regolamento rappresenta un elemento centrale nell'attuazione del pacchetto Dublino e del nuovo Patto per l'immigrazione. In particolare, è stato rappresentato che l'implementazione del regolamento in parola costituisce una responsabilità condivisa fra Stati membri, Commissione ed eu-LISA. È stato fatto riferimento al regolamento di esecuzione della Commissione 2055 del 2 ottobre 2025, il cui all. XI contiene un opuscolo informativo sul trattamento dei dati in EURODAC, parte di un modello per i richiedenti asilo "Cosa bisogna sapere su EURODAC" (realizzato utilizzando anche i commenti ricevuti dal GEPD). È stato ribadito che eu-LISA si occuperà della formazione degli Stati per il sistema centralizzato e che questi a loro volta saranno tenuti a formare il proprio staff.

I membri del gruppo di supervisione hanno inoltre ricevuto un aggiornamento da parte di eu-LISA sui dati statistici relativi ai dati registrati in EURODAC, rilevando tra i vari aspetti una diminuzione sia delle transazioni tra il 2023 e il 2024 relative a tutte le categorie di dati sia delle registrazioni di dati nel sistema centrale dovuta allo spirare dei termini di conservazione.

È proseguito il lavoro di approfondimento del rapporto tra il regolamento cosiddetto screening (reg. 2024/1356) e il reg. EURODAC che si concentrerà sullo studio delle seguenti tematiche: i) differenze nelle definizioni relative alla protezione dei dati (es. soggetto vulnerabile) e i rischi che comportano; ii) differenze sul principio di limitazione delle finalità e categorie di dati; iii) categorie di soggetti interessati. Infine, è stata avviata una riflessione sull'esercizio dei diritti degli interessati, evidenziando criticità relative agli obblighi di informazione e all'utilizzo di modelli predefiniti.

20.3. *La partecipazione dell'Autorità in seno al Consiglio d'Europa, all'OCSE e ad altri gruppi di lavoro internazionali*

20.3.1. Consiglio d'Europa

Il Comitato consultivo della Convenzione 108/1981 (T-PD), composto da 55 parti, si è riunito due volte in plenaria (17-19 giugno e 3-5 novembre 2025) e due volte nella sua composizione ristretta (cd. T-PD *Bureau*, 19-20 marzo e 29-30 settembre 2025) di cui una rappresentante del Garante è parte per l'Italia.

Convenzione 108+

Il raggiungimento del numero sufficiente di ratifiche per consentire l'entrata in vigore del protocollo emendativo della Convenzione 108 (cd. Convenzione 108+) è rimasto uno degli obiettivi cui l'attività del Comitato tende. Tale protocollo, adottato già nel 2018 al fine di rafforzare la tutela approntata dalla Convenzione 108 anche rispetto alle molte sfide per la protezione dei dati provenienti dal mutato scenario tecnologico e globale, necessita di un numero di ratifiche (trentotto) inusualmente alto per poter entrare in vigore.

Le ratifiche hanno raggiunto il numero di 33 nel corso dell'anno, con quella di Grecia (5 marzo 2025) e del Principato di Monaco (6 marzo 2025), e la Convenzione modernizzata necessita dunque di un ulteriore sforzo per poter garantire la realizzazione di uno strumento internazionale particolarmente significativo, soprattutto per la sua vocazione globale, essendo aperto all'accessione anche di paesi che non sono parte del Consiglio d'Europa.

Linee guida sull'art. 11 della Convenzione 108+

Sono state adottate, all'esito di un lungo lavoro di elaborazione, le linee guida sull'interpretazione dell'art. 11 della Convenzione 108+ che stabilisce i requisiti cui devono attenersi le parti nel prevedere eccezioni ai principi della Convenzione 108+ in specifici ambiti (in particolare *law enforcement* e sicurezza nazionale).

Le linee guida (cfr. Relazione 2024, p. 220) forniscono indicazioni sui requisiti ai quali le normative nazionali devono attenersi nella previsione di eccezioni ai principi della Convenzione al fine di garantire che tali eccezioni siano rispettose dell'essenza dei diritti fondamentali tutelati dalla Convenzione stessa.

Trasferimenti di dati verso paesi terzi

Nel corso delle due plenarie il Comitato ha discusso delle future attività riguardo ai trasferimenti di dati verso paesi terzi ed ha concordato con gli obiettivi proposti dal Segretariato in uno specifico documento di lavoro, concernente in particolare: la promozione dei modelli di clausole contrattuali (*Model Contractual Clauses* - MCC: *controller to controller, processor to processor, controller to processor*) già adottati dal Comitato nel corso del 2024 (cfr. Relazione 2024, p. 202) favorendone, ove possibile, l'adozione da parte degli Stati; la predisposizione di un *action plan,* con la cooperazione delle autorità

nazionali di protezione dei dati, per garantire l'approvazione delle MCC entro il 2029, e l'elaborazione di materiali divulgativi che possano promuoverne l'uso.

Il Comitato ha altresì supportato le ulteriori proposte contenute nel documento che consistono, in particolare, nell'avvio di un lavoro interpretativo sull'art. 14 della Convenzione 108+, nella creazione di un inventario degli strumenti di trasferimenti dati da rendere disponibile sul sito web del Comitato, in un'attività di promozione degli standard del Consiglio d'Europa nei forum globali, nonché nell'elaborazione di studi e report sulla convergenza dei diversi strumenti di trasferimenti dati disponibili a livello globale.

Neurotecnologie

È proseguita la discussione per la predisposizione di linee guida in materia di protezione dei dati nell'ambito delle neurotecnologie, anche attraverso la collaborazione con gli esperti scientifici autori del report disponibile online sul sito web del Comitato. Le neurotecnologie possono infatti comportare rischi molto significativi per i diritti fondamentali delle persone, compresa la protezione dei dati, in quanto consentono forme di sorveglianza degli ambiti più intimi della vita individuale quali il pensiero e gli stati emotivi. Obbligano pertanto ad una lettura ragionata degli strumenti giuridici in uso, anche se già interpretati in via evolutiva dalla stessa Corte EDU, nonché ad una riflessione sulla necessità di apportare regole specifiche per un settore tanto sensibile.

***Large Language Models* (LLM)**

Il Comitato ha discusso il tema dei *Large Language Models* (LLM) e delle loro implicazioni sulla protezione dei dati. Nella consapevolezza che tali modelli sono in grado di svolgere sempre più sofisticate attività di predizione anche psicologica degli individui che se ne servono, anticipando desideri ed indirizzando le loro scelte, il Comitato ha avviato una discussione in vista della predisposizione di specifiche linee guida.

Elezioni del *Data Protection Commissioner*

Allo scadere del lungo mandato di Jean Philippe Walter, nel corso della plenaria di giugno si sono svolte le elezioni per il ruolo di *Data Protection Commissioner* del Consiglio d'Europa, assunto da Tamar Kaldani, ex presidente dell'autorità di protezione dati della Georgia.

20.3.2. G7 DPA

Nel corso del 2025 il Garante ha proseguito il lavoro il seno al forum G7 DPA che vede riunite le autorità per la privacy dei sette paesi membri del G7. Durante l'anno l'Autorità ha partecipato a tutte le riunioni da remoto dei tre gruppi di lavoro del G7 DPA (*Data Free Flow with Trust* - DFFT, *Emerging Technologies Working Group* - ETWG, *Enforcement Cooperation Working Group Cooperation* - ECWG) che hanno approfondito le tematiche relative rispettivamente alla protezione dei dati e ai flussi transfrontalieri di dati, alle tecnologie emergenti e alla cooperazione tra autorità.

***Roundtable* di Ottawa**

Si è tenuta in Canada (Ottawa) la quinta Tavola rotonda delle G7 DPA dal 17 al 19 giugno 2025 presso la *Willson House* (lago Meech). Il vertice è stato coordinato, nell'ambito della presidenza di turno del Canada, da Philippe Dufresne, Presidente della Commissione canadese per la protezione della privacy. Alla Tavola rotonda hanno partecipato le autorità di Canada, Francia, Germania, Giappone, Italia, Regno Unito, Stati Uniti, oltre alla Presidente del Comitato europeo per la protezione dati, Anu Talus, e al Garante europeo, Wojciech Wiewiórowski. Il Garante ha partecipato con il Presidente Pasquale Stanzione, la Vicepresidente Ginevra Cerrina Feroni e i componenti Agostino Ghiglia e Guido Scorza. Al centro dei lavori tematiche cruciali come la promozione della libera circolazione dei dati, il rafforzamento della cooperazione transfrontaliera, le sfide alla privacy derivanti dagli attacchi alla cybersicurezza e l'impatto delle nuove tecnologie emergenti, a partire dall'intelligenza artificiale. L'obiettivo dell'incontro è stato quello di consolidare ulteriormente la cooperazione tra le autorità privacy dei paesi del G7. Il documento principale, portato in adozione il 19 giugno, è stato lo *Statement* G7 DPA dal titolo *Prioritising Privacy* che guarda alla privacy quale

strumento di sviluppo economico e di innovazione, evidenziando che dovrà essere dedicata particolare attenzione alla tutela dei minori. È stato altresì adottato il *Communiqué*, che, in sintesi, riporta le intenzioni di lavoro delle autorità che partecipano alla Tavola rotonda annuale G7.

Il 16 e 17 giugno, inoltre, a margine della Tavola rotonda si è svolto un workshop organizzato da Canada, Giappone e OCSE sull'utilizzo delle nuove tecnologie e dell'IA nei settori della sanità e della finanza (*Expert workshop and High Level Roundtable on PETs and AI*). Per il Garante è intervenuta la Vicepresidente Ginevra Cerrina Feroni, mentre gli altri componenti hanno portato il loro contributo al dibattito delle varie sessioni.

Al temine dei lavori del G7, il 20 giugno si è tenuto il *Privacy Symposium*, un seminario dedicato al tema della privacy dei giovani nell'era digitale al quale ha partecipato, come relatore, l'Avv. Guido Scorza.

Nella stessa giornata, il Presidente Pasquale Stanzione, la Vicepresidente Ginevra Cerrina Feroni e il componente Agostino Ghiglia sono intervenuti in un dibattito pubblico presso la McGill University di Montréal.

Nel corso dei mesi successivi, partendo dai risultati del G7 del Canada, i membri del G7 hanno approfondito alcuni temi specifici, quali l'evoluzione del ruolo delle autorità di protezione dei dati nella *governance* dell'intelligenza artificiale; l'IA generativa; l'uso etico dei dati sanitari; il contributo dell'IA nella ricerca medico-scientifica; cloud computing e cybersicurezza; l'importanza dell'educazione civica digitale.

Tale lavoro di approfondimento è stato quindi portato a sintesi nella Tavola rotonda virtuale di dicembre.

***Roundtable* virtuale**

Il secondo incontro delle autorità della privacy dei paesi del G7 si è tenuto da remoto il 9 e 10 dicembre. In tale circostanza, la delegazione italiana è stata guidata nel corso della prima giornata da Guido Scorza e nella seconda dalla Vicepresidente Ginevra Cerrina Feroni.

Le discussioni si sono concentrate sui progressi compiuti nel corso dell'anno nell'ambito dei richiamati pilastri del Piano d'azione 2025, ossia circolazione transfrontaliera dei dati sicura e responsabile (DFFT), rafforzamento della fiducia nelle nuove tecnologie, cooperazione internazionale in materia di applicazione delle norme di protezione dati:

- trasferimento dei dati transfrontalieri in modo sicuro e responsabile: l'*Information Commissioner's Office* (ICO) del Regno Unito e l'autorità federale per la protezione dei dati tedesca hanno co-diretto il Gruppo DFFT, che ha lavorato nell'ottica di contribuire al raggiungimento di un elevato livello di protezione dei dati, facilitando al contempo i flussi internazionali;
- rafforzare la fiducia nelle nuove tecnologie: sotto la guida dell'ICO, l'*Emerging Technologies Working Group* ha esaminato come promuovere lo sviluppo e l'utilizzo di nuove tecnologie in modo da rafforzare la fiducia e rispettare i principi di privacy e protezione dei dati. Ciò include il progresso del lavoro sull'intelligenza artificiale, sui fornitori di servizi terzi, sulla tecnologia di tracciamento online nei dispositivi domestici connessi e sulla privacy dei minori;
- cooperazione per l'attuazione delle normative: co-presieduto dalla *Federal Trade Commission* degli Stati Uniti e dalla *Personal Information Protection Commission* del Giappone (PPC), *l'Enforcement Cooperation Working Group* ha progettato meccanismi e metodi pratici per migliorare la cooperazione nelle azioni di applicazione delle normative tra le diverse giurisdizioni.

La Tavola rotonda si è conclusa con l'adozione di:

- un *Position Paper* sul DFFT;
- una dichiarazione (*Statement*) relativa all'utilizzo di tecnologie di tracciamento (*tracking technologies*) nell'ambito dei dispositivi domestici connessi utilizzati dai minori;

- un documento (ad uso interno) per il format per lo scambio di informazioni;
- il Piano d'azione per il 2026, in base al quale le autorità si impegnano a continuare a promuovere la fiducia e a sostenere l'innovazione a tutela della privacy, in particolare dei minori.

Le autorità hanno anche accolto con favore la dichiarazione ministeriale G7 2025 su industria, digitale e tecnologia per un approccio all'intelligenza artificiale che metta la persona al centro e per "una IA che stimoli innovazione e crescita a beneficio delle persone, mitighi le esternalità negative, rafforzi la sicurezza economica e nazionale, rispetti i quadri giuridici applicabili, compresi i diritti umani".

Questa Tavola rotonda ha rappresentato l'evento conclusivo della presidenza canadese. L'incontro ha visto pertanto il passaggio di consegne alla presidente della Commissione nazionale per l'informatica e le libertà francese (CNIL), che ospiterà la prossima Tavola rotonda del G7 DPA (23-26 giugno 2026).

20.3.3. OCSE

DGP

È proseguita l'attività dell'Autorità in ambito OCSE, in particolare attraverso la partecipazione al DGP (*Working Party on Data Governance and Privacy*), del quale l'Autorità è membro con un proprio rappresentante, al quale sono state confermate nel 2025 le funzioni di ViceChair che svolge dal 2012 (già nel WPSPDE - *Working Party on Security and Privacy in Digital Economy*).

Le due riunioni plenarie del DGP (7 e 8 aprile 2025 e 17 e 18 novembre 2025), cui si sono come di consueto aggiunte diverse riunioni del *Bureau*, il gruppo ristretto del *Board*, sono state anche per il 2025 caratterizzate da un'altissima partecipazione delle delegazioni dei paesi membri.

Si riportano i principali temi trattati nel corso dell'anno:

- intelligenza artificiale: il Gruppo si è confrontato sui recenti progressi tecnologici dell'IA, tema sul quale l'OCSE si sta concentrando da più angolature e sotto la spinta di diversi Comitati. *In primis*, il Gruppo ha seguito le recenti attività del partenariato globale sull'IA (GPAI) dell'OCSE (di cui l'Italia è parte dal 2020), ossia l'iniziativa internazionale e multidisciplinare che ha come obiettivo la promozione, lo sviluppo e l'utilizzo responsabile dell'intelligenza artificiale, "fondata sui diritti umani, l'inclusione, la diversità, l'innovazione e la crescita economica". Il GPAI sta accelerando i lavori per avvicinare teoria e pratica nell'IA, sostenendo "attività applicate" relative ad essa. Gli esperti di IA provenienti dall'industria, dalla società civile, dal settore pubblico e dal mondo accademico hanno lavorato su quattro tematiche principali: intelligenza artificiale responsabile; *governance* dei dati; futuro del lavoro; innovazione e commercializzazione. In tale contesto il DGP ha preso atto degli sviluppi delle recenti attività e fornito il proprio contributo al correlato Gruppo di esperti GPAI su IA, dati e privacy di cui due rappresentanti del Garante sono membri dal 2024 (v. *infra*). Si è inoltre lavorato per la redazione di un documento programmatico su "Meccanismi di raccolta dati per la formazione sull'IA: implicazioni sulla privacy e sulla *governance* dei dati"; il documento è stato elaborato per promuovere una discussione strategica all'interno del DGP sulla futura direzione degli sforzi dell'OCSE in materia di *governance* dei dati e privacy nel contesto dell'IA e si presta a divenire un importante riferimento per il futuro lavoro del DGP su IA. Attraverso l'esame dell'intera gamma di meccanismi utilizzati per raccogliere dati per l'apprendimento automatico, dalle informazioni fornite dagli utenti e dalle donazioni volontarie di dati alle licenze commerciali di dati, ai set di dati aperti e al *web scraping* su larga scala, il documento evidenzia le implicazioni di ciascun metodo per la protezione dei dati e la proprietà intellettuale, sottolineando che il modo in cui i dati vengono raccolti può essere deter-

minante tanto quanto il modo in cui vengono sviluppati gli algoritmi. Il documento rileva inoltre un crescente contenzioso giudiziario sull'utilizzo di dati raccolti online per addestrare modelli linguistici di grandi dimensioni, nonché crescenti richieste di trasparenza sulle origini dei set di dati di addestramento. Elemento centrale dello studio è una tassonomia che classifica la raccolta dati in due fonti principali: la raccolta diretta da individui e organizzazioni e i dati ottenuti da terze parti. In proposito, il DGP ha sostenuto che, sebbene i set di dati aperti e condivisi siano essenziali, per quanto riguarda l'innovazione, è necessario bilanciare queste misure con misure di tutela della privacy e di responsabilizzazione, in coerenza con il lavoro svolto sull'*accountability* di cui parimenti il DGP negli anni si è fatto messaggero. Infine il documento indica le tecnologie di tutela della privacy e i dati sintetici come strumenti che potrebbero ridurre i rischi nei futuri processi di raccolta dati;

- flusso libero dei dati con fiducia (DFFT): è proseguito il lavoro della comunità di esperti di *data flows* - (DFFT *Community* istituita dall'OCSE nel 2024) per sostenere il processo di creazione di fiducia sui dati e sul loro utilizzo oltre confine. La comunità riunisce esperti provenienti da governi, mondo accademico, società civile, imprese e organizzazioni internazionali e ha condotto il lavoro sui tre principali progetti individuati nel 2024: pagamenti transfrontalieri; rafforzamento della trasparenza regolatoria; PETs (*Privacy Enhancing Technologies*). In tale contesto, particolare impegno è stato profuso per il progetto relativo ai pagamenti transfrontalieri, che 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. In particolare, è stata avviata la partecipazione del Segretariato del DGP al forum di Basilea ospitato dal *Financial Stability Board* (FSB), e la relativa collaborazione con la *Financial Action Task Force* (GAFI). Si tratta del forum sui dati sui pagamenti transfrontalieri dell'FSB, voluto per l'attuazione delle raccomandazioni 2024 dell'FSB per promuovere l'allineamento e l'interoperabilità tra i *framework* di dati relativi ai pagamenti transfrontalieri, in supporto della roadmap del G20 per il miglioramento dei pagamenti transfrontalieri;

- neurotecnologie: il DGP ha proseguito il lavoro sul delicato tema della neurotecnologia, ed è stato rinnovato un interesse generale per l'analisi dei temi di protezione dei dati legati alla natura transfrontaliera delle neurotecnologie e alla conseguente necessità di politiche che promuovano la cooperazione internazionale a fronte di una rapida evoluzione tecnologica e di un mutevole panorama geopolitico. Su tale impulso è stato organizzato l'11 giugno un workshop sulle implicazioni della privacy dei dati nelle neurotecnologie, nonché sui progressi di uno studio di mappatura dei dati con le aziende del settore neurotecnologico e sui piani futuri per un report congiunto sul rafforzamento della *governance* dei dati per le neurotecnologie emergenti in sinergia con il Gruppo di lavoro su biotecnologie, nanotecnologie e tecnologie convergenti (BNCT) del Comitato per la politica scientifica e tecnologica (CSTP). Il workshop ha aperto la strada ad altre iniziative internazionali al fine di sviluppare standard per governare l'innovazione neurotecnologica che siano in linea con i principi condivisi in materia di protezione dei dati;

- accesso affidabile dei governi ai dati dei privati: altro tema dominante 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 conferenza ministeriale OCSE di Gran Canaria nel mese di dicembre 2022. Nelle plenarie del 2025 il DGP ha preso atto dei progressi compiuti attraverso la dichiarazione e si è concentrato su come rafforzarne l'attuazione. È stato ribadito che l'emanazione dei principi OCSE non esaurisce le opportunità di lavoro multilaterale sull'accesso

dei governi ai dati personali. La dichiarazione stessa "rileva" la necessità di ulteriori lavori su altre tipologie di accesso ai dati, tra cui l'acquisto da parte dei governi di banche dati commerciali del settore privato, il ricorso a dati personali accessibili al pubblico ed a comunicazioni volontarie alle forze dell'ordine e alle autorità di sicurezza nazionale.

Gruppo di esperti su IA, dati e privacy

Il 2025 ha visto l'intensificarsi del lavoro del Gruppo di esperti dell'OCSE su IA, dati e privacy di cui il Garante è parte. Il Gruppo di lavoro si caratterizza per riunire in un forum le diverse *expertise* in materia di privacy e protezione dati nonché nel settore dell'IA al fine di effettuare approfondimenti sulle aree di intersezione tra i due ambiti e fornire contributi sulle scelte di policy da adottare in chiave prospettica e all'interno della cornice sovranazionale. Il Gruppo, in collaborazione con il DGP, ha partecipato all'organizzazione di due tavole rotonde di alto livello (11 febbraio 2025) sulla *governance* internazionale dei dati e la privacy nel contesto dell'IA, come evento collaterale dell'*Artificial Intelligence Action Summit* e in collaborazione con la *Personal Information Protection Commission* (PIPC) della Corea e l'autorità francese per la protezione dei dati (CNIL).

La prima tavola rotonda si è concentrata sulla necessità di migliorare l'accesso e la condivisione dei dati per l'intelligenza artificiale, proteggendo al contempo i diritti individuali, tra cui la privacy, ma anche altri diritti o interessi quali i diritti di proprietà intellettuale. In tale contesto sono state messe le basi per la seconda tavola rotonda evidenziando, ad esempio, l'importanza dell'accesso e della condivisione dei dati per l'intelligenza artificiale, esplorando le strategie nazionali sui dati per l'intelligenza artificiale e analizzando approcci tecnici o organizzativi quali le tecnologie per il miglioramento della privacy (PET) o le *sandbox* normative come strumenti utili a integrare i quadri di *governance* dei dati e privacy in tali contesti. La prima tavola rotonda ha condotto alla pubblicazione di un documento dal titolo "Migliorare l'accesso e la condivisione dei dati nell'era dell'intelligenza artificiale", che integra la raccomandazione dell'OCSE sul miglioramento dell'accesso e della condivisione dei dati.

Nella seconda tavola rotonda su "*Trustworthy and Accountable Data Governance in the Age of AI*", si è discusso dell'applicazione dei principi di privacy e protezione dei dati all'IA, con l'obiettivo di promuovere un'innovazione responsabile e condivisa. Fra i temi affrontati si ricordano l'individuazione delle basi giuridiche per il trattamento dei dati personali, l'implementazione di un approccio basato sul rischio e il ruolo delle autorità di controllo nella *governance* dei dati dell'IA.

20.4. *Le conferenze internazionali ed europee delle autorità di protezione dati e privacy*

Global Privacy Assembly

Il Garante ha partecipato alla 47ª sessione annuale della *Global Privacy Assembly* (GPA), ospitata dalla *Personal Information Protection Commission* della Corea del Sud (dal 15 al 19 settembre) che ha avuto come tema centrale l'IA e le sue implicazioni per la tutela dei diritti e la protezione dei dati personali.

I lavori si sono articolati in *open sessions*, aperte al pubblico, in *closed sessions* riservate alle autorità per il confronto regolatorio e l'adozione di risoluzioni, e in *side event* paralleli, dedicati a questioni emergenti come l'*open source* e la protezione dei minori. La delegazione del Garante, in particolare, ha contribuito al *side event* dedicato all'IA *open source*, alla sessione dedicata a "*Redress and Interoperability of Data Protection: the consumer perspective*", e alla *closed session* nel panel relativo al *targeted advertising*.

Nel corso delle *open sessions* sono stati affrontati i principali temi relativi all'IA. In tale sede sono stati evidenziati i rischi connessi all'integrazione degli agenti di IA nei sistemi operativi e al possibile indebolimento della crittografia (citando casi riferiti ad alcune

piattaforme) i quali compromettono la riservatezza e la cifratura *end-to-end*, rafforzando modelli economici basati sulla raccolta massiva di dati personali.

In un panel si è approfondito il ruolo della pseudonimizzazione e dei dati sintetici come strumenti di innovazione sicura: misure capaci di rafforzare la protezione e abilitare la ricerca, pur con limiti legati al rischio di reidentificazione e alla mancanza di standard condivisi.

Le applicazioni dell'IA in sanità hanno suscitato interesse: l'IA può migliorare diagnosi precoci, ridurre errori clinici e accelerare la ricerca di nuovi farmaci, ma restano sfide cruciali in materia di trasparenza, consenso dinamico e fiducia dei pazienti. Sono emerse proposte volte a promuovere un uso mirato dei dati sintetici e maggiori responsabilità delle strutture sanitarie nella valutazione degli algoritmi.

Il panel sulle basi giuridiche per l'uso dei dati personali nell'IA ha evidenziato approcci divergenti tra ordinamenti: se il consenso esplicito e la disciplina dei dati sensibili restano indiscussi, persistono incertezze sul ricorso al legittimo interesse per il *training* e sui limiti tra dati pseudonimizzati e anonimizzati. Sono state illustrate esperienze di dialogo con Big Tech sull'uso dei dati per l'addestramento degli LLM, provvedimenti di blocco (Irlanda), linee guida flessibili (Corea del Sud) e richiami etici e coerenti con i principi fondamentali, nonostante la diversità dei sistemi giuridici (Argentina).

Infine, il panel sui trasferimenti internazionali di dati ha mostrato come, nell'era dell'IA e della geopolitica, i flussi transfrontalieri non siano più un tema solo tecnico ma una questione centrale per i diritti, la sicurezza e la sovranità. L'Europa ha ribadito che senza stato di diritto non vi possono essere trasferimenti sicuri; dagli Stati Uniti è venuto un richiamo alla cooperazione tra democrazie per affrontare le minacce digitali; dai Paesi africani la richiesta di riequilibrare il sistema e rafforzare le capacità locali; dal Giappone il rilancio del concetto di *Data Free Flow with Trust*, da tradurre in strumenti concreti.

Un ulteriore approfondimento è stato dedicato alla *digital education*, con particolare attenzione all'impatto delle tecnologie educative e dell'IA sui minori. UNICEF ha richiamato l'esigenza di un'EdTech inclusiva e sicura, accessibile anche alle comunità più marginali. Il dibattito ha evidenziato criticità comuni: asimmetria di potere tra scuole e piattaforme, consenso spesso inefficace, bisogno di regole chiare e di un approccio multistakeholder per garantire equità e inclusione.

Nel corso della *closed session* la GPA ha approvato tre risoluzioni che riguardano:

- dati personali e intelligenza artificiale: tale risoluzione, presentata dal garante australiano e co-sponsorizzata dal Garante italiano insieme ad altre autorità, affronta i rischi legati all'uso dei dati personali per l'addestramento dei modelli di IA. Il testo riafferma che le norme sulla protezione dati si applicano pienamente all'IA e richiama cinque principi fondamentali: base giuridica corretta, limitazione delle finalità, minimizzazione, trasparenza e accuratezza. Le autorità si impegnano a sensibilizzare sviluppatori e decisori, a rafforzare il coordinamento nell'enforcement e a condividere esperienze sull'IA generativa;

- supervisione umana delle decisioni automatizzate: la risoluzione, proposta dal garante canadese, ribadisce che le decisioni basate su sistemi di IA devono prevedere un controllo umano effettivo, non meramente formale. La supervisione deve essere reale, con supervisori dotati di un ruolo chiaro, competenze e risorse adeguate, e con organizzazioni che restano pienamente responsabili. Vengono promosse misure pratiche come formazione, meccanismi di escalation e test periodici, nonché l'impegno a sviluppare una definizione comune e condividere buone pratiche;

- educazione digitale e cittadinanza responsabile: la terza risoluzione, proposta dal Messico e dalla Georgia, sottolinea l'urgenza di integrare la protezione dei dati nell'educazione digitale, dall'infanzia all'università. L'obiettivo è contrastare fenomeni

come cyberbullismo, deepfake e furti d'identità, promuovendo programmi di alfabetizzazione, politiche inclusive, materiali accessibili e formazione per docenti e genitori.

Nell'ambito dei GPA *Awards*, l'Autorità, con soddisfazione, ha visto anche premiata la sua iniziativa "Privacy Tour", categoria "*Education and Public Awareness*".

Il Garante, inoltre, ha aderito, insieme ad altre venti autorità, al *Joint Statement on Building Trustworthy Data Governance Frameworks for Artificial Intelligence*, già proposto da alcune autorità di protezione dati nell'ambito dell'*AI Action Summit* di Parigi del 10-11 febbraio 2025. Il documento promuove lo sviluppo di sistemi di IA innovativi e rispettosi della privacy, sottolineando l'importanza di principi di protezione dei dati *by design*, *governance* trasparente e cooperazione tra autorità per affrontare i rischi legati a discriminazione, disinformazione e violazioni della privacy.

Si deve menzionare, infine, il *side event* organizzato dal Garante in collaborazione con l'Ambasciata d'Italia dal titolo "*Privacy in the face of the challenges posed by artificial intelligence*", che ha offerto un'opportunità molto apprezzata di confronto con un pubblico prevalentemente coreano.

Conferenza di primavera *(Spring Conference)*

Si è tenuta a Batumi (Georgia) dal 6 al 9 maggio, ospitata dall'autorità georgiana, la 33ª Conferenza di primavera delle autorità europee di protezione dati, cd. *Spring Conference*.

Diversi i temi trattati nelle sessioni a porte chiuse, riservate alle sole autorità di protezione dei dati. In particolare, nel panel sull'*interplay* di diversi regimi giuridici sulla regolamentazione della tecnologia, la Vicepresidente Cerrina Feroni ha presentato un intervento dal titolo "*Safeguarding Fundamental Rights in the Age of AI: The Role of Data Protection Authorities*", sottolineando la funzione cruciale delle autorità privacy, ancore di responsabilità istituzionale, nel contesto dell'intelligenza artificiale. Di seguito, nel panel sui minori, il dott. Ghiglia è intervenuto sul tema "*Building Trustworthy AI for Children: Advancing Digital Civic Education and Risk Governance within the EU AI Act*", sottolineando l'importanza di investire in un'efficace educazione digitale e nell'adozione di una prospettiva incentrata sul minore nella progettazione e nella *governance* dei sistemi di IA.

Oltre ai temi affrontati nel corso dei lavori, tra cui i dati sanitari e il ruolo del RPD (con gli interventi dei due RPD di EUROJUST ed EUROPOL), sono stati presentati due *side events*: uno sulla protezione dei dati personali in Georgia e l'altro sulla valutazione d'impatto per i diritti fondamentali nel contesto del reg. IA.

Nel corso dei lavori sono altresì stati approvati due risoluzioni di accreditamento come membri della Conferenza delle autorità dell'Andalusia e della Repubblica del Kosovo e la risoluzione "*on the Action Plan for Further Collaboration Activities*".

20.5. *Rinvii pregiudiziali ex art. 267 TFUE*

L'attività internazionale del Garante ha riguardato altresì le cause pregiudiziali proposte dinanzi alla CGUE dai giudici degli Stati membri, ai sensi dell'art. 267 del TFUE, in materia di protezione dei dati personali.

In proposito, si rammenta che, a seguito del trasferimento parziale di competenze dalla Corte al Tribunale dell'UE avvenuto nel 2024, la materia della protezione dei dati personali è rimasta di esclusiva competenza della Corte.

Si conferma, nel corso del 2025, la tendenza all'incremento del numero di tali cause principalmente in rapporto all'interpretazione di disposizioni del RGPD, anche se non sono mancate questioni connesse alla direttiva 2016/680/UE e alla direttiva 2002/58/CE.

Qui di seguito le sentenze adottate dalla CGUE nel corso del 2025, oggetto di domande pregiudiziali istruite anche dal Garante:

- sentenza 9 gennaio 2025, causa C-416/23, sull'interpretazione della nozione di

«richieste eccessive» di cui all'art. 57, par. 4, RGPD;

- sentenza 9 gennaio 2025, causa C-394/23, sul trattamento dei dati personali relativi all'appellativo dei clienti avente la finalità di personalizzare la comunicazione commerciale fondata sulla loro identità di genere, e sulle basi legittimanti dell'esecuzione del contratto e del legittimo interesse del titolare del trattamento o di terzi;
- sentenza 13 febbraio 2025, causa C-383/23, sull'art. 83 del RGPD sulle sanzioni amministrative pecuniarie e sul termine "impresa";
- sentenza 27 febbraio 2025, causa C-638/23, sulla titolarità del trattamento da parte di un'entità amministrativa ausiliaria senza personalità giuridica;
- sentenza 27 febbraio 2025, causa C-203/22, sulla portata del diritto di accesso e sulla nozione di "informazioni significative sulla logica utilizzata" in relazione allo *scoring* creditizio;
- sentenza 13 marzo 2025, causa C-247/23, sui dati personali relativi all'identità di genere e diritto di rettifica;
- sentenza 3 aprile 2025, causa C-710/23, sulla titolarità del trattamento e designazione da parte della normativa nazionale di un'entità amministrativa ausiliaria priva di personalità giuridica e di capacità giuridica propria;
- sentenza 30 aprile 2025, cause riunite C-313/23, C-316/23 e C-332/23, in materia di divulgazione a un organo giudiziario di dati personali protetti dal segreto bancario;
- sentenza 5 giugno 2025, causa C-541/24, in materia di accesso agli atti di causa da parte di un avvocato estraneo al processo;
- sentenza 4 settembre 2025, causa C-655/23, in relazione al diritto alla cancellazione dei dati personali e al risarcimento del danno immateriale;
- sentenza 13 novembre 2025, causa C-654/23, con riguardo ai trattamenti di dati personali per finalità di *direct marketing* (in particolare, il cd. soft spam) e direttiva 2002/58/CE;
- sentenza 20 novembre 2025, causa C-57/23, in materia di raccolta e conservazione di dati biometrici e genetici da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (direttiva 2016/680/UE);
- sentenza 2 dicembre 2025, causa C-492/23, in materia di responsabilità del gestore di un mercato online per la pubblicazione dei dati personali contenuti in annunci collocati nel suo mercato online da parte di utenti inserzionisti;
- sentenza 18 dicembre 2025, causa C-422/24, in materia di informazioni da fornire all'interessato con riguardo ad un trattamento di dati operato tramite una *bodycam* indossata da controllori nei trasporti pubblici.

20.6. *I progetti per l'applicazione del RGPD finanziati dall'Unione europea*

Nel quadro del progetto di gemellaggio (*twinning*) finanziato dall'Unione europea, che ha visto il Garante impegnato in qualità di partner (cfr. Relazione 2024, p. 227), sono stati organizzati dal 9 al 12 giugno, presso la sede del Garante, quattro seminari con una delegazione di esperti dalla Bosnia-Erzegovina dell'agenzia IDDEA (responsabile per i documenti d'identificazione e lo scambio dati) e dell'agenzia per la protezione dei dati personali su alcuni temi chiave, tra cui *privacy by design* e *by default*, gestione dei *data breach*, utilizzo di banche dati e call center, e il ruolo del *Data Protection Officer* (DPO/(RPD).

L'evento ha segnato la conclusione della fase operativa del progetto, che mira a sostenere la modernizzazione dell'amministrazione pubblica in Bosnia-Erzegovina migliorando i servizi al cittadino. La Bosnia-Erzegovina è paese candidato dal 2022 all'adesione all'Unione europea.

21 Trattamenti transfrontalieri di dati personali e cooperazione europea

21.1. T*rattamenti transfrontalieri e società dell'informazione*

I trattamenti transfrontalieri, ovverosia i trattamenti di dati personali che, secondo la definizione dell'art. 4, n. 23, RGPD, hanno luogo nell'ambito delle attività di più stabilimenti di un titolare o di un unico stabilimento ma che incidono in modo sostanziale su interessati in più di uno Stato membro, costituiscono una percentuale rilevante in termini sia quantitativi che qualitativi delle procedure di cooperazione (cd. procedure IMI) che interessano i fornitori di servizi della società dell'informazione.

Il meccanismo dello sportello unico (*One-Stop-Shop*), come noto, si fonda sui principi di cooperazione (tra autorità di controllo) e di coerenza (tra autorità di controllo e Comitato europeo), i quali congiuntamente danno vita ad un sistema amministrativo paneuropeo, che si prospetta ulteriormente rafforzato e consolidato dal reg. (UE) 2025/2518 (di seguito nuovo regolamento procedurale), pubblicato sull'*Official Journal* della UE in data 26 novembre 2025, che stabilisce norme procedurali aggiuntive sull'applicazione del RGPD e che si applicherà a far data dal 2 Aprile 2027.

Nell'anno 2025 il numero delle procedure di cooperazione nel settore delle comunicazioni elettroniche è risultato sostanzialmente stabile rispetto al 2024, dopo un costante aumento rilevato a partire dal 2022.

In termini generali, si conferma l'aumento delle procedure di vera e propria cooperazione (artt. 60 e ss. RGPD, aumentate di circa il 20% rispetto al 2024), mentre sono risultate sostanzialmente stabili le procedure preliminari ex art. 56 del RGPD, ovverosia le procedure relative alla fase iniziale di determinazione, su ogni singolo caso, aperto d'ufficio od originato da un reclamo, dei ruoli rispettivamente di autorità capofila (*Lead Supervisory Authority* - LSA) e autorità interessata (*Concerned Supervisory Authority* - CSA). 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 all'autorità capofila irlandese (DPC). I reclami in argomento vengono spesso trattati e definiti dalla DPC mediante procedure di composizione amichevole (*amicable settlement*), un sistema di risoluzione bonaria delle controversie che persegue il duplice obiettivo di garantire una tutela celere e soddisfacente degli interessati e una maggiore efficienza dell'azione amministrativa mediante la deflazione del carico di lavoro che grava sulle autorità di controllo. Tale procedura viene applicata anche da altre autorità di controllo sulla scorta della legislazione nazionale nella cornice normativa di cui all'art. 57, par. 1, lett. f), RGPD. Come sopra rappresentato, il nuovo regolamento procedurale 2025/2518 costituirà la base legislativa per la definizione bonaria dei reclami anche laddove non prevista negli ordinamenti nazionali, al fine "di porre rapidamente fine alle violazioni […] e di fornire una rapida risoluzione ai reclamanti" (cfr. cons. 21), mediante l'introduzione della cd. risoluzione rapida (cfr. art. 5) che permetterà, alle autorità interessate che ricevono reclami aventi ad

oggetto trattamenti transfrontalieri e sussistendo determinate condizioni, di definire tali reclami senza sottoporli al meccanismo di cooperazione.

Come ormai noto e consolidato, le procedure di cooperazione consentono all'Autorità di prendere parte alle istruttorie condotte nei confronti, principalmente, dei primari *players,* delle piattaforme online e dei servizi di social networking. In tale contesto vengono, infatti, affrontate tematiche transnazionali di estrema attualità e rilevanza nella società dell'informazione fra le quali l'interpretazione e l'applicazione dei principi generali in materia di trattamento dei dati personali, l'individuazione della corretta base giuridica di specifiche attività di trattamento e le modalità per garantire l'esercizio dei diritti degli interessati.

Si è già dato conto del lavoro svolto dall'Autorità nel corso del 2025 relativamente alle attività di valutazione preliminare di compliance condotte dalla DPC in merito alle iniziative di due grandi società statunitensi che offrono servizi di social networking nell'area SEE e intendevano trattare determinati dati personali degli utenti (cd. *first party data*) per finalità di addestramento dei modelli e dei servizi di intelligenza artificiale generativa (cfr. par. 12.2).

Negli ultimi anni si è altresì assistito ad un incremento delle procedure cd. di assistenza reciproca volontaria (VMA), sia sotto il profilo numerico, sia sotto il profilo della rilevanza dei contenuti condivisi che spesso sono relativi ad aggiornamenti, anche di impatto, circa il trattamento dei dati personali da parte dei principali *player* mondiali. In particolare, nel 2025 l'autorità irlandese, in veste di autorità capofila, ha fatto ampio uso di tale strumento di cooperazione per condividere con le autorità interessate gli aggiornamenti ricevuti dai grandi titolari statunitensi stabiliti in Irlanda in materie di particolare interesse ed attualità, come i trattamenti di dati personali sottesi all'addestramento dei modelli di intelligenza artificiale generativa o a servizi ad essi connessi, ovvero l'implementazione di nuove *feature* da parte delle principali società del settore tecnologico.

L'Autorità ha anche adottato due progetti di decisione ex art. 60, par. 3, RGPD in qualità di autorità capofila (LSA) nei confronti di due titolari del trattamento stabiliti in Italia. In entrambi i casi il Garante ha ritenuto di proporre l'archiviazione dei reclami presentati avverso i due titolari e, a seguito dell'assenza di obiezioni pertinenti e motivate da parte dell'autorità di controllo che aveva ricevuto tali reclami, ha comunicato formalmente i progetti di decisione per i seguiti di competenza (adozione della decisione finale a opera dell'autorità ricevente il reclamo, ex art. 60, par. 8, RGPD).

L'Autorità ha adottato due decisioni finali, ai sensi dell'art. 60, par. 8, RGPD, concernenti l'archiviazione dei rispettivi reclami proposti nel 2024 da due cittadini italiani nei confronti di una società che gestisce note piattaforme di social network. Tali reclami erano stati presentati a seguito dell'annuncio da parte del titolare dell'intenzione di avviare una attività di trattamento sui cd. *first party data*, vale a dire i dati pubblici condivisi dagli utenti sui propri social network, per finalità di addestramento del proprio modello di IA generativa, in asserita violazione degli artt. 6, 12, 13, 17, 18, 19, 21 e 25 del RGPD.

I due reclami erano stati trasmessi, in forza del meccanismo dello sportello unico, all'autorità di controllo irlandese, ai sensi e per gli effetti dell'art. 56 del RGPD. Nell'agosto 2025, dopo una serie di interlocuzioni, l'autorità capofila irlandese ha adottato due progetti di decisione di archiviazione, ai sensi dell'art. 60, par. 3, RGPD, in quanto il trattamento dei dati personali lamentato non era mai stato effettuato dal titolare a seguito del rinvio del progetto. L'Autorità ha conseguentemente adottato le due decisioni finali di archiviazione, ai sensi dell'art. 60, per. 8, RGPD (provv.ti 13 novembre 2025, nn. 693 e 694, doc. web nn. 10198751 e 10198779).

Si è, infine, conclusa l'attività di cooperazione rafforzata dell'Autorità sullo *strategic*

case Smart TV, a cui il Garante aveva partecipato congiuntamente alle autorità olandese, ungherese e del Liechtenstein. L'analisi dei dati emersi dall'accertamento tecnico (raccolta e analisi del flusso telematico di dati prodotti dalle Smart TV selezionate), svolto simultaneamente, sulla base di un *Joint Operation Action Plan* (JOAP), redatto ai sensi dell'art. 62 del RGPD, le risultanze emerse dai riscontri forniti dai tre titolari coinvolti e la valutazione giuridica preliminare delle autorità coinvolte sono confluiti in un *final investigation report* che è stato sottoposto ed approvato dalla plenaria del CEPD di giugno 2025 (https://www.autoriteitpersoonsgegevens.nl/documenten/rapport-verkennend-onderzoek-smart-tvs).

21.2. *Trattamenti transfrontalieri in ambito economico-produttivo*

La partecipazione al sistema IMI previsto dal reg. (UE) 1024/2012, per la gestione dei meccanismi di cooperazione e coerenza di cui al Capo VII del RGPD 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. Si segnala in proposito il notevole incremento nel numero di queste procedure rispetto agli anni precedenti.

Per quanto riguarda l'ambito economico, le procedure IMI riguardano casistiche eterogenee riferite ad una variegata pluralità di titolari e responsabili del trattamento, considerata la granularità del settore di riferimento.

Si conferma nel 2025 la prevalenza delle procedure IMI ai sensi dell'art. 56 del RGPD volte all'identificazione dell'autorità capofila (LSA) e delle autorità interessate (CSA) che rappresentano circa il 54% della totalità delle procedure pervenute nel corso dell'anno. Nel periodo di riferimento, l'Autorità si è dichiarata "interessata", ai sensi dell'art. 4, n. 22, RGPD, in 172 casi assumendo invece la posizione di "autorità capofila" in un numero limitato di casi (10) riguardanti società con stabilimento unico o principale in Italia.

Al tal riguardo, si segnala il notevole aumento delle procedure IMI rispetto all'anno 2024, in specie con riguardo a quelle ex art. 56 RGPD.

Sono, inoltre, molto aumentate, rispetto allo scorso anno, 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 sollevare solo commenti o richieste di chiarimenti.

Riguardo ai casi in cui l'Autorità si è dichiarata capofila 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, 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.

Non sono stati predisposti progetti di decisione in relazione a trattamenti transfrontalieri.

In relazione a un reclamo presentato da un cittadino svedese nei confronti di un società sportiva dilettantistica con cui aveva lamentato il mancato riscontro alla richiesta di accesso ai dati – e riguardo al quale il Garante aveva formulato nel 2024, con progetto di decisione, la proposta di adottare una decisione ai sensi dell'art. 60 par. 8, al fine di chiudere il procedimento, con archiviazione del relativo reclamo, non

essendo stata provata la violazione degli artt. 12 e 15 – l'autorità svedese, a cui era stato presentato il reclamo, dopo aver dichiarato di aderire alla proposta del Garante, tenuto altresì conto che nessun ulteriore sollecito o contestazione era pervenuto da parte dell'interessato, ha adottato la decisione finale ex art. 60.8 del RGPD, poi notificata al titolare da questa Autorità.

Nel 2025 sono state adottate le seguenti decisioni finali:

- provv. 10 aprile 2025, n. 207 (doc. web n. 10160922) che ha avuto origine dal reclamo di un cittadino tedesco il quale aveva lamentato il mancato riscontro, da parte della società italiana (titolare di una piattaforma di e-commerce per l'acquisto di capi di abbigliamento), a una richiesta di accesso ai dati personali ai sensi dell'art. 15 RGPD. Tenendo conto di tutte le circostanze del caso e, in particolare delle giustificazioni addotte per il mancato (iniziale) riscontro alla prima richiesta di accesso, nonché dei riscontri forniti dal titolare a seguito della richiesta di accesso, il Garante ha proposto la chiusura del procedimento con decisione ex art. 60, par. 7, RGPD, senza l'adozione di misure correttive o sanzionatorie nei confronti del titolare ritenendo che quest'ultimo si fosse conformato a quanto richiesto e che dunque l'interessato potesse ritenersi soddisfatto; al riguardo, si evidenziava che il medesimo interessato – al quale tramite l'autorità ricevente il reclamo (l'autorità tedesca di Renania Settentrionale-Vestfalia) era stata data la possibilità di essere sentito – non aveva fatto pervenire obiezioni o commenti. Si è ritenuto pertanto che ricorressero i presupposti per un *amicable settlement* previsti dal Comitato nelle linee guida 6/2022 sull'attuazione pratica delle composizioni amichevoli. Pertanto – spirato il termine di quattro settimane previsto dall'art. 60, par. 6, RGPD, senza che venissero sollevate obiezioni da parte delle autorità interessate – è stata adottata dal Garante una decisione finale ex art. 60, par. 7, RGPD, con provvedimento collegiale poi notificato al titolare;
- provv. 23 ottobre 2025, n. 617 (doc. web n. 10196127) con cui si è concluso il procedimento relativo al reclamo nei confronti di una società italiana di e-commerce, proposto da un cittadino del Lussemburgo, il quale aveva lamentato il mancato riscontro alla richiesta di accesso ai propri dati che la società avrebbe raccolto in occasione della sua ricerca di una sistemazione alberghiera sul relativo sito web. In particolare il reclamante, a seguito della ricezione di un'e-mail (poi rivelatasi e-mail di recall/carrello abbandonato) chiedeva di conoscere i destinatari a cui i propri dati personali sarebbero stati trasmessi. A seguito dell'attività istruttoria condotta dal Garante e dopo aver condiviso la relativa proposta di decisione con le altre autorità interessate senza che fossero sollevate obiezioni pertinenti e motivate, è stato adottato un ammonimento, tenuto conto, oltre che delle violazioni accertate (artt. 12 e 15 per inadeguato riscontro alla richiesta di esercizio del diritto di accesso; art. 13 per informativa inadeguata e lacunosa; art. 30 per mancata tenuta del registro dei trattamenti), di tutte le circostanze del caso e in particolare del fatto che la società aveva soddisfatto le richieste dell'interessato in corso di procedimento, aveva aggiornato l'informativa e istituito il registro dei trattamenti.

Per quanto riguarda l'assistenza reciproca fra le autorità di controllo, sempre con riferimento all'ambito economico, si conferma l'utilizzo della relativa procedura IMI allo scopo di ottenere informazioni sulle normative nazionali in tema di protezione dei dati o su questioni relative all'applicazione di particolari disposizioni del RGPD. Fra le questioni trattate, si menzionano le seguenti: il recepimento in Italia della direttiva (UE) 2015/849, al fine di conoscere in quale misura le banche siano autorizzate a verificare le attività finanziarie di persone politicamente esposte e dei loro familiari stretti (PEP); il trattamento dei dati biometrici per l'identificazione a

21

distanza dei clienti da parte di banche ed istituti di pagamento; il trattamento dei dati nell'ambito della centrali dei rischi della Banca d'Italia; l'utilizzo di sistemi di riconoscimento automatico delle targhe dei veicoli nei parcheggi gestiti da compagnie di parcheggio private; il trattamento dei dati personali nel settore della sanità privata e nel settore *beauty*, e l'eventuale approvazione di codici di condotta in tali settori.

Anche nel 2025 sono stati presentati al Garante reclami ai sensi degli artt. 143 e ss. del Codice e 77 RGPD nei confronti di società con sede in altro Stato membro per i quali si è reso necessario avviare le procedure di cooperazione, provvedendo a trasmettere la relativa documentazione alla competente autorità capofila.

22 Attività di normazione tecnica internazionale e nazionale

Il Garante ha proseguito la collaborazione in tema di elaborazione di norme tecniche internazionali nell'ambito del Working Group 5 del sottocomitato SC27, che si occupa della sicurezza delle informazioni all'interno del comitato tecnico JTC1 dell'Organizzazione internazionale per la normazione (ISO). Il gruppo di lavoro segue gli aspetti di sicurezza nella gestione delle identità relativamente alle tecnologie biometriche e alla protezione dei dati personali. Armonizzando la propria posizione con quelle delle altre autorità di protezione dati tramite il CEPD, che ha un collegamento in proposito con ISO, l'Autorità ha seguito lo sviluppo delle seguenti norme tecniche:

- ISO 27701:2019 - *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*, revisione a seguito della pubblicazione della ISO 27002:2022 (pubblicato a ottobre 2025);
- 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 27706 - *Requirements for bodies providing audit and certification of privacy information management systems,* che definisce requisiti aggiuntivi alla ISO 17021 per gli organismi di certificazione che svolgono audit e rilasciano certificazioni secondo la ISO 27701:2025 (*Privacy Information management System*) (pubblicato a ottobre 2025);
- ISO/IEC 10267 - *Methods to quantify the amount of personal information in a dataset*, che intende fornire una guida sui metodi per calcolare la quantità di informazioni personali in un data set;
- ISO/IEC 27555 - revisione prevalentemente editoriale delle linee guida pubblicate nel 2021 per la cancellazione dei dati personali che includono la classificazione dei dati, la definizione dei tempi di cancellazione/periodi di mantenimento, di classi di cancellazione, di requisiti di implementazione nonché processi e responsabilità (*Guidelines on personally identifiable information deletion*);
- 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 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 ISO 27002:2022 (pubblicato ad agosto 2025);

- ISO 27574 - *Privacy in brain-computer interface* (BCI) *applications*, che ha l'obiettivo di fornire requisiti e linee guida in materia di protezione dei dati per le *Brain Computer Interface* (BCI) *Applications* e individuare specifici controlli;
- ISO 27503 - *Guidelines on Privacy Protection of Intelligent Travel Services*, che si propone di analizzare gli *Intelligent travel service system*, considerandone gli attori (es. *driver*, passeggeri, service provider), le loro relazioni e i flussi di dati scambiati;
- 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 di sicurezza e protezione dei dati dei portatori di interesse;
- 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, ecc.), i diversi tipi di avatar (*realistic*, *iconic*, *fantasy*), gli elementi di protezione della privacy che intervengono durante le interazioni dei medesimi;
- ISO 27575 - *Privacy for Metaverse Frameworks*, che intende analizzare il panorama degli elementi, informazioni, minacce e misure a protezione dei dati nel metaverso;
- ISO 27091 - *Cybersecurity and privacy - Artificial intelligence - Privacy protection* che fornisce una guida alle organizzazioni che utilizzano o sviluppano sistemi di intelligenza artificiale e modelli di *machine learning* per indirizzare i rischi privacy identificando i rischi nel ciclo di vita dei sistemi AI 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 RGPD basato sulla norma tecnica EN 17926;
- CWA 18016 - *Age appropriate design*, il progetto intende trasformare in una norma tecnica europea il documento CWA che propone una metodologia e buone pratiche per tener conto delle esigenze dei minori nello sviluppo di servizi e prodotti, *by design*, integrandolo laddove necessario.

Del pari è proseguita la collaborazione con le diverse commissioni tecniche UNINFO, l'Ente di normazione federato con UNI (Ente nazionale italiano di unificazione).

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

23.1. *La comunicazione del Garante: profili generali*

Nel 2025 l'attività comunicativa del Garante ha accompagnato in modo coerente e continuativo le iniziative dell'Autorità in settori particolarmente sensibili e caratterizzati da una rapida evoluzione tecnologica. La strategia comunicativa si è concentrata nel rendere accessibili e comprensibili ai cittadini i temi più rilevanti emersi nel corso dell'anno, con particolare attenzione all'IA, ai fenomeni di trattamento illecito dei dati e alla tutela della dignità delle persone, soprattutto nei casi di diffusione non autorizzata di contenuti privati.

Attraverso i comunicati stampa, la Newsletter istituzionale, le attività di sensibilizzazione (come podcast e iniziative divulgative) e i contenuti dedicati sui canali social, l'Autorità ha perseguito l'obiettivo di informare in modo tempestivo, trasparente e orientato alla prevenzione, rafforzando la consapevolezza pubblica sui rischi e sulle opportunità connessi al trattamento dei dati personali.

Le attività di comunicazione strategica

Le attività di comunicazione del Garante hanno avuto un focus particolare su alcuni temi che riguardano il rapporto tra nuove tecnologie, protezione dei dati e tutela dei diritti fondamentali delle persone. L'attenzione si è quindi rivolta ad ambiti come quelli dell'IA, della tutela dei minori online e dell'educazione digitale di base.

Il lancio del podcast "A proposito di privacy", avvenuto nell'aprile del 2025, risponde alla scelta di affiancare ai canali istituzionali tradizionali uno strumento capace di raggiungere utenze più ampie e diversificate e di favorire una fruizione continuativa dei contenuti, veicolando messaggi istituzionali in una forma dialogica e accessibile. Nel corso dell'anno sono state pubblicate quattro puntate, dedicate a temi di particolare impatto sociale (accessi illeciti alle banche dati, oblio oncologico, *sharenting*, scuola), in tre episodi con la partecipazione di un componente del Collegio: è stato cioè utilizzato un modulo comunicativo funzionale alla valorizzazione della viva voce dell'Autorità e al rafforzamento dell'immagine di un'istituzione autorevole ma vicina ai cittadini, collegando in modo chiaro la tutela dei diritti a situazioni concrete della vita quotidiana.

Una delle iniziative più rilevanti del 2025 è stato l'evento formativo "La Privacy in salute", un ciclo di incontri dedicati alla gestione dei dati personali nel settore sanitario, rivolto in particolare ai responsabili della protezione dei dati delle regioni, delle province autonome e delle strutture sanitarie pubbliche e private. Il ciclo di quattro incontri si è svolto da aprile a novembre e ha impegnato nelle attività di informazione e divulgazione dirigenti e funzionari dell'Autorità, oltre che decisori ed esperti dei vari settori coinvolti. L'iniziativa è stata supportata attraverso attività di comunicazione a vari livelli (web, social media, comunicati stampa) e con la ideazione e la realizzazione di materiali di grafica e multimediali.

Sono state ideate e realizzate – totalmente *in house* – due campagne informative in tema di educazione digitale e sicurezza digitale di base, con la produzione di infografiche,

pagine informative sul sito web istituzionale del Garante, clip multimediali e post sui social media. La prima, "Per una privacy da paura anche ad Halloween", ha mirato ad aumentare la consapevolezza sui possibili rischi del digitale in un momento dell'anno caratterizzato dalla volontà di esporsi online per mostrare festeggiamenti e costumi e da un proliferare di offerte commerciali che possono a volte nascondere insidie e tentativi di truffa. La campagna ha sensibilizzato l'utenza sulla necessità di riflettere attentamente prima di pubblicare o condividere immagini sui social network, in particolare nel caso di minori; un altro aspetto essenziale ha riguardato la necessità di esaminare attentamente le offerte straordinarie, regali e consegne di prodotti che possono celare tentativi di truffa o possono esporre dispositivi e dati personali ad azioni malevole. La seconda campagna è stata promossa in occasione delle festività natalizie, con la versione aggiornata di "La privacy sotto l'albero" attraverso la quale il Garante ha ricordato, con un Vademecum ricco di casistiche e indicazioni, i pochi, semplici, ma se ben applicati, efficaci consigli per vivere le festività evitando brutte sorprese per la privacy e la sicurezza digitale.

23.2. *I prodotti informativi*

Nel corso del 2025 sono stati diffusi 59 comunicati stampa e 11 Newsletter.

La Newsletter del Garante è una pubblicazione periodica, registrata presso il Tribunale di Roma, giunta al XXVII anno di diffusione. È inviata in via telematica a redazioni, professionisti, amministrazioni pubbliche, imprese e semplici cittadini che ne fanno esplicita richiesta o si iscrivono online alla Newsletter sul sito dell'Autorità.

La Newsletter è da anni uno strumento conosciuto ed apprezzato che l'Autorità utilizza fornendo un vasto panorama di questioni e problematiche 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 che vengono rielaborati in chiave giornalistica.

Sul sito è sempre possibile consultare l'archivio tematico della pubblicazione che raccoglie, divise per categorie, i 27 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 11 numeri del GPDPDigest, il magazine online 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.

23.3. *Il sito istituzionale, i prodotti multimediali e le pubblicazioni*

Il 2025 ha confermato e rafforzato l'impegno dell'Ufficio per incrementare la quantità, varietà e qualità dei prodotti di comunicazione digitale destinati alla diffusione tramite il sito web e i canali social media del Garante, con una produzione di contenuti integrata e multicanale. Sono stati pubblicati circa 1.226 contenuti sui profili social media (LinkedIn, Instagram, X, Telegram e YouTube), con una presenza articolata e spesso differenziata per piattaforma. I follower totali dei profili social media e di messaggistica hanno toccato la quota complessiva di 110.867, con un incremento di circa l'8% rispetto al 2024 (102.529). La piattaforma professionale LinkedIn continua

a rappresentare il canale più seguito, con 75.225 follower. Instagram e X hanno raggiunto rispettivamente 13.040 e 11.530 follower, mentre la pagina YouTube si è attestata a 5.371 iscritti. L'attività di social media *engagement* ha prodotto complessivamente circa 118.000 interazioni nel corso dell'anno.

Il portale istituzionale si è arricchito di nuove sezioni, mentre le altre sono state rinnovate nella grafica, nell'usabilità e nei contenuti. Complessivamente sono 43 le sezioni e pagine tematiche coinvolte da interventi, tra cui le nuove sezioni dedicate a blockchain, deepfake, podcast, cyberbullismo, biometria, trasporti e la versione in lingua inglese del sito.

La produzione video si è mantenuta su livelli significativi, con 55 prodotti realizzati nell'arco dell'anno tra video istituzionali, contributi dei componenti del Collegio, *teaser* promozionali per i social media e montaggi degli eventi.

Sul fronte editoriale si segnalano due importanti pubblicazioni aggiornate nel secondo semestre: "Social privacy. Come tutelarsi nell'era dei social media", aggiornamento della guida pubblicata per la prima volta nel 2009, e "La scuola a prova di privacy", nuova versione di 98 pagine del Vademecum che affronta le tematiche connesse al trattamento dei dati personali nelle istituzioni scolastiche, anche alla luce dei nuovi strumenti di intelligenza artificiale. A supporto di entrambe le pubblicazioni sono stati ideati segnalibri cartacei istituzionali con QR code per favorirne la diffusione.

Merita di essere segnalato che su tutte le questioni sulle quali il Garante è intervenuto i media hanno posto sempre una costante attenzione. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali, delle testate online e blog che hanno trattato i temi legati alla privacy sono state 7.023, quelle relative all'attività del Garante 5.791. Gli articoli aventi per oggetto le interviste, interventi e dichiarazioni del Garante sono state 113 su stampa e web, mentre 58 su Radio e TV. Si contano, infine, 1.698 articoli relativi ai comunicati stampa e 625 relativi agli argomenti delle Newsletter.

23.4. *Le manifestazioni e i convegni*

A partire dal 2007, promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le autorità europee per la privacy, il 28 gennaio di ogni anno, viene celebrata in tutta Europa la Giornata europea per la protezione dei dati personali, che ha lo scopo di sensibilizzare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali.

Il Garante ha organizzato il convegno "Le sfide dell'I.A. La protezione dei dati nell'era del cambiamento", in occasione della 19ª edizione della Giornata europea. L'evento si è svolto il 29 gennaio presso la Sala del Refettorio di Palazzo San Macuto a Roma e ha consentito di approfondire l'impatto dell'IA in settori cruciali come lavoro, sanità, giustizia e sicurezza, evidenziando il ruolo centrale della protezione dei dati nel governo di queste tecnologie. I lavori, aperti dalla Vicepresidente della Camera Anna Ascani, hanno visto gli interventi del Presidente del Garante, di rappresentanti del Governo e delle principali istituzioni nazionali.

Il Collegio del Garante ha incontrato il 23 giugno l'Ambasciatore d'Italia a Ottawa, Alessandro Cattaneo, per un confronto sui principali esiti della tavola rotonda "G7 Privacy" ospitata nei giorni immediatamente precedenti in Canada. L'incontro, svoltosi in un clima di collaborazione, ha permesso di approfondire i temi centrali del vertice: trasferimento internazionale dei dati, tecnologie emergenti ed *enforcement*, ambiti nei quali Italia e Canada intrattengono consolidate relazioni istituzionali.

Sono state richiamate in proposito le iniziative che hanno preceduto e seguito il G7, tra cui l'evento OCSE dedicato all'innovazione e il *Privacy Symposium* organizzato dal Commissario canadese per la privacy, sottolineando la rilevanza della tutela dei minori nell'ambiente digitale.

Il 15 luglio, presso la Sala della Regina della Camera dei deputati, alla presenza delle istituzioni di Camera e Senato, di ministri, di rappresentanti del Parlamento, del mondo dell'impresa e delle associazioni di categoria si è svolta la cerimonia della presentazione della Relazione per l'anno 2024. La Relazione ha illustrato 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, l'intero evento è stato trasmesso in diretta TV ed in streaming sul sito web istituzionale.

Nel corso dell'anno, il Presidente e i componenti del Collegio hanno infine partecipato a numerosi eventi, convegni e giornate di studio, di rilievo nazionale ed internazionale.

23.5. *L'attività internazionale*

L'Autorità ha fornito, nel corso di riunioni a distanza e attività intermedie di coordinamento, un rilevante contributo alle attività del gruppo di comunicatori istituito presso il CEPD, tramite la revisione dei comunicati stampa del Comitato agli esiti delle riunioni plenarie e in occasione della pubblicazione di linee guida e altri documenti.

Il Garante ha contribuito fattivamente all'alimentazione della sezione *National news* del sito del CEPD, segnalando alcune delle notizie e comunicati nazionali di maggior interesse, oltre a condividere con il gruppo i comunicati stampa di una qualche rilevanza per le altre autorità.

Per tutto il 2025 è stata inoltre data visibilità alle diverse attività internazionali del Garante: lancio dell'azione e dei relativi risultati nell'ambito del *Coordinated enforcement framework* (CEF), che vede impegnate ogni anno la gran parte delle autorità europee in una verifica tematica sull'attuazione del RGPD; copertura della partecipazione alla Conferenza di primavera delle autorità europee (*Spring conference*); copertura della partecipazione al "G7 Privacy", svoltosi in Canada a luglio e conclusosi con una riunione da remoto in dicembre.

23.6. *L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi*

Nel corso del 2025, l'Autorità ha continuato a curare, attraverso il Servizio per le relazioni con il pubblico, l'informazione sulle disposizioni in materia di protezione dei dati personali e sulle relative modalità di tutela, sia mediante il servizio di ascolto telefonico, sia attraverso la posta elettronica, riscontrando quotidianamente quesiti di varia natura provenienti da enti pubblici e privati e da singoli cittadini. Quanto al ricevimento del pubblico presso la sede di Piazza Venezia, lo si è riservato ai soli casi più delicati, secondo prassi ormai consolidate.

Il Servizio per le relazioni con il pubblico, oltre a fungere come sempre da punto essenziale di contatto dei cittadini con l'Autorità, ha svolto anche una funzione di filtro curando, laddove possibile, il diretto riscontro delle richieste pervenute, ove necessario con il supporto dei singoli dipartimenti e servizi dell'Autorità. Sono state prontamente trattate anche molteplici richieste concernenti fascicoli assegnati ad altre unità organizzative, garantendo l'opportuno raccordo con il lavoro dell'Ufficio nel suo complesso.

Significativi risultano i dati numerici relativi ai contatti con il Servizio, che ammontano a poco più di 13.000, di cui circa 8.400 e-mail e quasi 5.000 contatti telefonici; inoltre, sono stati riscontrati più analiticamente 177 fascicoli e sono state ricevute presso la sede 13 persone (cfr. parte IV, tab.15).

Oltre a fornire consulenza giuridica all'utenza, il Servizio ha continuato a riscontrare direttamente le richieste di informazioni o chiarimenti 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*).

Nel 2025 il Servizio ha altresì proseguito nell'aggiornamento delle note-tipo di riscontro su tematiche ricorrenti nelle interazioni con l'utenza (ad es. per la videosorveglianza, il condominio, il fascicolo sanitario elettronico, i trattamenti di dati in ambito scolastico, il Sistema informativo Schengen). Nella stessa ottica di semplificazione amministrativa, sono state predisposte nuove note dedicate a specifici temi quali i termini dei procedimenti davanti al Garante, le assenze per malattia in ambito lavorativo, le richieste di accesso alle progressioni economiche orizzontali. In tutti questi casi, si è cercato di fornire agli utenti riscontri chiari e sintetici, indicando comunque tutti i riferimenti normativi utili a consentire adeguate tutele.

Tra le tematiche di carattere generale esaminate direttamente, si segnalano, in primo luogo, quelle concernenti gli strumenti di tutela dinanzi al Garante e gli adempimenti previsti dal RGPD. Molte 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 diffuso interesse hanno riguardato i trattamenti di dati personali nei seguenti settori: lavoro, videosorveglianza, sanità e ricerca scientifica, scuola, utilizzo di tecnologie digitali nonché i trattamenti in ambito giornalistico, con particolare riferimento alle richieste di deindicizzazione dei dati personali dai motori di ricerca (cfr. parte IV, grafico 16).

III

L'UFFICIO DEL GARANTE

24 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 oggetto di particolare attenzione da parte 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, nonché contributi di letteratura cosiddetta grigia o provenienti da altri organismi e istituzioni. Tale aggiornamento è stato garantito anche 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 2025, tenendo conto anche delle fattispecie più frequentemente esaminate. Al riguardo, menzioniamo in primo luogo le applicazioni connesse all'intelligenza artificiale, nelle sue molteplici connotazioni, anche alla luce della promulgazione della l. 23 settembre 2025, n. 132 - Disposizioni e deleghe al Governo in materia di intelligenza artificiale; inoltre la pseudonimizzazione (alla luce della sentenza della CGUE nel caso C-413/23 P, e delle proposte di modifica del quadro normativo UE in materia di protezione dati contenute nel Digital Omnibus); l'eredità digitale (compreso il tema più ampio della persistenza della persona digitale *post-mortem*); il regolamento procedurale che integra il RGPD quanto alla gestione di casi relativi a trattamenti transfrontalieri (reg. (UE) 2025/2518), con particolare riguardo ad alcuni aspetti problematici quali la risoluzione precoce di controversie, i termini procedimentali, e l'accesso delle parti al fascicolo del procedimento. L'attenzione si è concentrata, inoltre, sulle tematiche del diritto di accesso, nelle sue molteplici declinazioni, sulle implicazioni della normativa in materia di whistleblowing, e su altre questioni quali l'utilizzo del riconoscimento facciale in rapporto alla crescente diffusione di tecnologie biometriche in contesti di viaggio e il bilanciamento fra libertà di espressione e protezione della vita privata, con particolare riguardo al criterio della essenzialità delle informazioni.

Approfondimenti sono stati realizzati con riguardo a domande di rinvio pregiudiziale, rivolte alla Corte di giustizia dell'Unione europea, che hanno investito la materia della protezione dei dati; grazie a questi contributi, 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 2024. 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. È stata a tale scopo inserita nella Relazione un'apposita infografica per sintetizzare in modo efficace i principali risultati e ambiti di lavoro.

In conformità a quanto previsto dall'art. 22, d.l. n. 90/2014 convertito in l. 11 agosto 2014, n. 114, la Relazione annuale del Garante (non diversamente da quella delle altre autorità amministrative indipendenti) è stata altresì trasmessa alla Corte dei conti.

25 La gestione amministrativa

25.1. *Il bilancio e la gestione economico-finanziaria*

La gestione amministrativa dell'Autorità è stata improntata al rispetto dei principi di una prudente valutazione delle entrate e all'osservanza dei vincoli di spesa contenuti nelle disposizioni legislative e regolamentari applicabili anche al Garante.

Le risorse finanziarie per assicurare il funzionamento dell'Ufficio sono state previste dalla l. 30 dicembre 2024, n. 207 e hanno consentito di espletare i compiti e le attività istituzionali sulla base degli obiettivi programmatici approvati dal Collegio.

Riguardo alle specifiche esigenze di contenimento delle spese, l'Autorità ha continuato a porre in essere tutti gli opportuni accorgimenti funzionali alla gestione dei propri servizi nel rispetto di criteri di economicità.

L'Autorità non detiene immobili adibiti ad abitazione o foresteria e nel corso dell'esercizio non ha sostenuto spese per incarichi di studio e di consulenza.

La gestione amministrativa del Garante è stata assoggettata agli ordinari e periodici controlli che l'organo preposto alla verifica della regolarità amministrativo-contabile ha ritenuto di effettuare.

Sotto il profilo più strettamente contabile, il risultato finanziario dell'esercizio ha fatto registrare un sostanziale equilibrio tra entrate ed uscite, con un lieve avanzo finanziario di amministrazione, pari a 0,1 milioni di euro, in significativa riduzione rispetto al corrispondente risultato del precedente esercizio finanziario che aveva fatto registrare un avanzo di oltre 9,2 milioni di euro.

Dal raffronto tra le due annualità, infatti, emerge che i trasferimenti erariali si sono ridotti di oltre 3 milioni di euro mentre le esigenze di spesa sono cresciute di 6,8 milioni di euro.

Nel corso del 2025, al netto delle partite di giro, le entrate complessivamente acquisite dall'Autorità sono state pari a 48,0 milioni di euro a fronte delle quali sono stati registrati impegni di spesa per 47,9 milioni di euro.

Le risorse finanziarie acquisite al bilancio del Garante sono rappresentate, per la quasi totalità, da trasferimenti erariali disposti nell'ambito della pertinente legge di bilancio, in coerenza con quanto previsto dall'art. 156, comma 8, d.lgs. n. 196/2003.

L'importo complessivamente trasferito dal MEF per le complessive esigenze di funzionamento dell'Autorità è stato pari a 46,6 milioni di euro comprensivi di una quota di 2,7 milioni di euro di entrate da ascrivere a somme riassegnate dallo stesso Ministero in ragione dei proventi che l'erario aveva stimato di incassare nell'anno di riferimento a titolo di sanzioni irrogate dal Garante.

L'art. 166, comma 7, ultimo periodo, del Codice, infatti, prevede che i proventi delle sanzioni, derivanti dai provvedimenti adottati dal Garante nella misura del 50%, sono riassegnati alla stessa Autorità per lo svolgimento delle proprie attività istituzionali.

Nel corso dell'anno 2025 risultano acquisiti al bilancio dello Stato importi derivanti dai provvedimenti sanzionatori per complessivi 37,7 milioni di euro, in significativa crescita rispetto al precedente esercizio finanziario nel quale le entrate affluite all'erario erano state di 24,4 milioni di euro.

Di queste somme, riassegnabili *ex lege* al Garante in misura pari alla metà, solo una minima parte, corrispondente alla quota compresa nell'ambito dello stanziamento iniziale, è stata effettivamente trasferita.

Le ulteriori entrate acquisite nell'anno risultano di entità meno significativa e i relativi importi sono imputabili a trasferimenti per progetti specifici, anche in conto capitale, e a titolo di rimborsi da parte di altre amministrazioni.

Dalla tabella 24 si evince dalle due annualità poste a raffronto, da un lato, la consistente riduzione di entrate correnti e, dall'altro lato, l'incremento delle spese imputabile in misura largamente prevalente a quelle per il funzionamento dell'Autorità.

Sotto il profilo delle entrate, quelle correnti fanno registrare una contrazione rispetto al corrispondente valore del precedente esercizio finanziario (-3,0 milioni di euro, pari a -5,99%), ascrivibile ad una significativa contrazione dei trasferimenti erariali.

La spesa complessiva, di contro, fa registrare un significativo incremento rispetto ai valori del precedente esercizio (+6,8 milioni di euro, pari a +16,71%).

Tale incremento è ascrivibile in massima parte alla spesa per il personale, cresciuta per effetto dell'ampliamento della pianta organica autorizzata dal legislatore e della conseguente immissione in ruolo di numerose unità di personale, assunte in prossimità della fine dell'anno 2024.

L'ampliamento dell'organico è stato determinato dalla necessità di fare fronte alle sempre più crescenti incombenze che il Garante è chiamato ad affrontare e che ha reso indispensabile, quindi, un primo potenziamento della struttura.

In generale, la spesa complessiva si caratterizza, come per la generalità di analoghi soggetti pubblici, per una significativa incidenza degli oneri del personale, le cui risorse, tuttavia, rappresentano per esperienza, competenza e professionalità un fattore di primaria importanza nello svolgimento delle innumerevoli funzioni attribuite all'Autorità in ambito nazionale ed eurounitario.

L'indennità di carica dei componenti del Garante viene determinata nel rispetto delle vigenti disposizioni contenute nel Codice e in coerenza con i prescritti limiti di legge.

Con riferimento, infine, agli oneri strettamente connessi alle esigenze gestionali, nel corso dell'anno risultano rispettati i limiti di spesa dettati dalle specifiche disposizioni legislative applicabili anche all'Autorità.

25.2. *L'attività contrattuale e le procedure di affidamento*

In linea generale, nell'anno 2025 l'attività contrattuale è stata caratterizzata da due particolari evenienze, una esterna ed una interna al contesto organizzativo dell'Autorità. Il riferimento riguarda in particolare, nell'ordine, l'emanazione del cosiddetto decreto correttivo al codice dei contratti pubblici (d.lgs. n. 209/2024) e la scadenza del periodo di qualificazione che consentiva l'inserimento dell'Autorità nell'elenco delle stazioni appaltanti autorizzate ad operare per appalti di servizi e forniture fino a un valore di 5 milioni di euro (categoria "SF2").

Nel corso dell'anno è stato quindi necessario proseguire nell'aggiornamento dei processi lavorativi alle nuove procedure, anche alla luce delle ulteriori competenze tecnico-giuridiche richieste sia a seguito, nel precedente anno, dell'introduzione del nuovo codice dei contratti pubblici (d.lgs. n. 36/2023), sia in risposta alle numerose modifiche a questo apportate dal citato decreto correttivo.

Nel contempo, le innovazioni apportate al sistema di qualificazione delle stazioni appaltanti attraverso un quadro regolatorio contrassegnato da complessità legate anche al nuovo assetto normativo hanno imposto all'Autorità un serrato sforzo volto a mantenere la citata categoria "SF2", al fine di conservare l'autonomia organizzativa anche in materia di appalti pubblici, come si conviene ad una autorità indipendente.

25

L'esito è stato positivo, talché l'Autorità potrà continuare a bandire autonome procedure di gara, nei settori dei servizi e delle forniture, per importi non superiori a 5 milioni di euro, soglia del tutto compatibile con le effettive esigenze del Garante come sino ad oggi rilevate.

Per quanto attiene al profilo della normativa interna, merita di essere segnalato che nel febbraio 2025 è entrato in vigore il regolamento concernente la disciplina dei contratti di appalto del Garante aventi importo inferiore alle soglie europee al fine di disciplinare alcuni aspetti relativi a tali appalti, tenendo conto delle specifiche previsioni del codice dei contratti pubblici come, ad esempio, quella relativa al rispetto del principio di rotazione degli affidamenti (provv. 27 novembre 2024, n. 836, doc. web n. 10101560 e par. 26.2. della Relazione 2024).

In un'ottica di costante implementazione degli strumenti previsti dall'articolata disciplina dei contratti pubblici, è proseguita poi l'attività di valutazione e riscontro dei profili specificamente connessi alla corretta esecuzione degli appalti, considerando la particolare attenzione che il codice dei contratti pubblici rivolge a tale fase della vita contrattuale.

Procedure di affidamento

In merito ai contratti stipulati nell'anno in esame, deve evidenziarsi che la percentuale del numero di procedure di approvvigionamento effettuate attraverso la piattaforma CONSIP sul totale delle procedure ha superato il 90%, mentre la corrispondente proporzione dell'ammontare affidato ha superato il 96%.

Il ricorso agli strumenti messi a disposizione all'interno della piattaforma "Acquisti in rete PA" (convenzioni, accordi quadro e MEPA) ha permesso quindi di soddisfare la maggior parte delle necessità di approvvigionamento dell'Autorità; la parte residuale ha trovato prevalente esecuzione all'interno di altra piattaforma digitale certificata, a causa dell'indisponibilità all'interno dei citati strumenti CONSIP di talune categorie merceologiche. Al contempo è stata avviata l'analisi tecnica riguardante un ulteriore strumento messo a disposizione da CONSIP all'interno della piattaforma Acquisti in rete PA (sul sito Acquistinretepa.it), denominata "Gare in ASP - *Application Service Provider*", il cui utilizzo consentirebbe all'Autorità di effettuare la totalità delle negoziazioni propedeutiche all'approvvigionamento di beni e servizi su tale sistema di *e-procurement*. Ciò nondimeno, anche nell'annualità in esame si sono dovute registrare diffuse, per quanto temporanee, anomalie di funzionamento della citata piattaforma, che si auspica possa essere potenziata al fine di garantire la massima fluidità di utilizzo da parte delle stazioni appaltanti.

Tralasciando alcune disposizioni di proroga già previste nei corrispondenti contratti di affidamento (come il piano sanitario per il personale), la procedura di maggior rilievo economico registrata è stata costituita dall'adesione all'accordo-quadro CONSIP "*Facility management* grandi immobili". Nonostante alcune complessità soprattutto di carattere tecnico-amministrativo, tale adesione ha consentito all'Autorità di operare una riorganizzazione generale, sotto l'egida di un unico contratto, di servizi precedentemente regolati da autonome procedure di affidamento, realizzando così economie procedimentali e semplificazione delle catene di responsabilità.

Nella graduatoria degli affidamenti, ordinata per importo, seguono poi alcuni contratti afferenti all'area informatica, tutti stipulati all'interno della menzionata piattaforma CONSIP; tra questi, si citano l'adesione a due ulteriori accordi quadro: "Servizi di sicurezza da remoto, di *compliance* e controllo per le pubbliche amministrazioni", grazie al quale è stata implementata la sicurezza del sito internet istituzionale, e "*Microsoft Enterprise Agreement*", attraverso il quale è stata aumentata la capacità dell'Autorità di ricorrere a postazioni lavorative virtuali, caratterizzate da un più efficiente utilizzo delle risorse hardware, nonché da elevate scalabilità e flessibilità operativa. Ulteriori attività sono state poste in essere al fine di garantire la sicurezza informatica e fisica delle componenti infrastrutturali dell'Ufficio.

La sede del Garante e i contratti connessi

Esternamente all'area informatica, è interessante evidenziare che, grazie all'implementazione nella piattaforma CONSIP della categoria merceologica riguardante i servizi assicurativi, l'Autorità ha potuto farvi ricorso per affidare le proprie polizze concernenti l'ambito "*all risks*" afferente al proprio patrimonio mobiliare e immobiliare.

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.

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.

Inoltre, l'adozione degli standard di sicurezza è avvenuta anche con verifiche ambientali in stretta collaborazione con il responsabile della sicurezza e il dipartimento risorse umane e le attività di manutenzione dell'impiantistica antincendio sono state svolte con il supporto delle ditte incaricate.

25.3. *L'organizzazione dell'Ufficio*

Nell'anno di riferimento è proseguito il processo di attuazione del piano strategico dell'Autorità finalizzato al pieno raggiungimento degli obiettivi programmati. Tale attività è stata realizzata seguendo una duplice direttrice: dal lato interno, attraverso la reingegnerizzazione dei processi lavorativi; dal lato esterno, mediante la valorizzazione di forme di collaborazione con stakeholder istituzionali e sociali operanti, nei rispettivi ambiti di competenza, su tematiche attinenti anche alla protezione dei dati personali.

Rafforzamento dell'organico

È stato pressoché definito il processo di completamento della dotazione organica funzionale all'attuazione del predetto piano strategico dell'Autorità e al pieno raggiungimento degli obiettivi ad essa attribuiti a livello nazionale ed internazionale.

Il rafforzamento dell'organico è stato realizzato mediante la copertura della quasi totalità delle posizioni di ruolo previste nella dotazione organica delle varie aree professionali (dirigenti, direttivi, operativi ed esecutivi), a seguito dell'espletamento delle relative procedure di concorso pubblico e di mobilità (cfr. parte IV, tab. 23)

Lavoro agile

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 più fragili.

La percentuale del personale che ha aderito all'istituto del lavoro agile è stata molto elevata, a conferma dell'adeguatezza di tale modalità organizzativa quale strumento idoneo a conciliare le esigenze lavorative ed istituzionali con quelle personali dei dipendenti.

Relazioni sindacali

Sono state affrontate, di concerto con le organizzazioni sindacali, varie questioni negoziali, riguardanti in particolare l'individuazione di maggiori spazi per gli uffici del Garante, il welfare aziendale e le questioni previdenziali.

Sicurezza e salute dei lavoratori

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 più fragili.

25

Formazione del personale

È stato avviato e concluso il rapporto per lo stress lavoro-correlato in collaborazione con il medico competente e con il Responsabile del servizio di prevenzione e protezione, ed è stata promossa la costituzione di un gruppo sulla sicurezza e sul lavoro interno al fine di monitorare e migliorare le condizioni di lavoro in collaborazione con il Segretario generale.

Il Garante ha attuato soluzioni formative innovative per la crescita delle competenze individuali e di gruppo, coerentemente con le esigenze manifestate dalle varie unità organizzative. 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.

L'Autorità ha inoltre favorito l'utilizzo da parte del personale della piattaforma Syllabus in adesione alle indicazioni fornite con la direttiva 23 marzo 2023 del Ministro per la p.a. in materia di formazione, relativa alla crescita delle competenze funzionali alla transizione digitale, ecologica e amministrativa promosse dal PNRR.

L'adesione alla piattaforma Syllabus ha consentito di estendere la fruizione dei corsi all'intera platea del personale, indipendentemente dalla qualifica ricoperta, nonché di supportare il processo di integrazione del personale assunto nell'ultima parte dell'anno; inoltre, ha costituito una risorsa rilevante anche per rispondere alle priorità formative indicate nella direttiva 14 gennaio 2025 del Ministro per la p.a. con oggetto "Valorizzazione delle persone e produzione di valore pubblico attraverso la formazione. Principi, obiettivi e strumenti".

Si è ritenuto di adottare l'impostazione strategica della direttiva ministeriale, sebbene l'Autorità non rientri tra le amministrazioni destinatarie dell'obbligo normativo, condividendone le finalità di sviluppo professionale dei dipendenti e sostenendo una continua azione di coinvolgimento del personale nell'aderire a iniziative formative interne ed esterne, secondo le indicazioni e le *best practice* suggerite dalla richiamata direttiva.

Al fine di favorire il raggiungimento dell'obiettivo indicato dalla direttiva, sono state proposte ulteriori offerte formative su tematiche d'interesse grazie alla collaborazione con enti esterni (es. un'attività di formazione riguardante i concetti chiave e i fondamenti del funzionamento dei sistemi di IA, a cura del CINI), mentre sul lato interno è stata avviata un'attività di caricamento sulla piattaforma interna di contenuti tecnico-specialistici su questioni di interesse del Garante.

In termini di impatto, i dati rilevati dal Garante rispetto al raggiungimento degli obiettivi formativi prefissati hanno evidenziato che il 76% del personale del Garante ha aderito ad almeno un'iniziativa formativa di livello professionale.

Per la formazione obbligatoria relativa alla normativa di settore, è proseguita la formazione erogata a seguito dell'entrata in vigore del codice dei contratti pubblici (d.lgs. n. 36/2023), per i responsabili unici di progetto (RUP) 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).

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.

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, della giurisprudenza eurounitaria e nazionale e della dottrina, nonché mediante ulteriori approfondimenti funzionali a

fornire ai dipendenti periodici aggiornamenti in materia di protezione dei dati personali e privacy (cfr. par. 24).

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.*

25

Analisi dei processi

Un impegno particolare è stato dedicato all'analisi dei processi e dei sistemi esistenti presso l'Ufficio del Garante, con l'obiettivo di fornire input rilevanti al miglioramento e all'innovazione del modello organizzativo e al processo di digitalizzazione delle procedure, coerentemente con gli obiettivi strategici individuati dall'Autorità.

Tra le attività svolte in tale direzione, si segnala la partecipazione attiva nei gruppi di lavoro promossi dal Responsabile della transizione digitale per l'analisi funzionale del futuro sistema di *Business Process Management* (BPM), l'analisi di processo volta a supportare un processo continuo di ottimizzazione dei processi lavorativi, nonché il contributo attivo fornito nelle fasi di valutazione e gestione del rischio corruttivo da parte del Responsabile della prevenzione della corruzione e trasparenza (RPCT) nell'ambito di un più ampio processo di analisi organizzativa finalizzato al miglioramento continuo delle metodologie gestionali.

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 in uso, con la 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)

L'ufficio del RPD ha proseguito nel 2025 l'attività di potenziamento e razionalizzazione delle policy di protezione dei dati. In particolare, è stato aggiornato e ristrutturato il registro dei trattamenti svolti presso il Garante ex art. 30 RGPD, comprensivo del correlato documento recante le misure tecniche e organizzative di sicurezza aventi carattere generale.

È stata parzialmente ridefinita la privacy policy dei siti che costituiscono la presenza del Garante sul web, in particolare aggiornando l'elenco dei destinatari di dati personali trattati dall'Autorità.

Sono stati curati, come di consueto, i rapporti con i responsabili di trattamento designati volta per volta dall'Autorità in relazione a specifici affidamenti, attraverso interlocuzioni talora di rilevante complessità.

Durante tutto l'anno 2025 sono state istruite ed evase numerose richieste di accesso ex art. 15 RGPD, ove necessario in coordinamento con l'Ufficio al fine di assicurare approcci omogenei e coerenti.

Sono state realizzate alcune iniziative finalizzate a garantire la formazione del personale nel settore della protezione dei dati, segnatamente attraverso alcuni webinar fruibili sulla piattaforma interna di formazione. Nell'ambito della cooperazione con altre autorità amministrative, l'ufficio del RPD ha contribuito ad attività di formazione obbligatoria in materia di privacy presso l'Autorità per le garanzie nelle comunicazioni al fine di approfondire le applicazioni pratiche della normativa nelle attività di specifica pertinenza, con particolare attenzione ai procedimenti amministrativi, ai rapporti con gli utenti e alla gestione della trasparenza.

Infine, sono proseguiti i proficui incontri organizzati dalla Rete degli RPD delle autorità indipendenti, nei quali sono state affrontate questioni di interesse comune e, in particolare, alcune problematiche connesse alla comunicazione e diffusione di dati personali fra soggetti pubblici, tematiche riguardanti il reg. IA e le linee guida AgID in materia di utilizzo dell'IA nella p.a. (illustrate anche attraverso un incontro presso la sede AgID). L'annuale seminario della Rete si è tenuto il 24 novembre 2025 presso la sede di CONSOB e ha visto la partecipazione di un panel qualificato di relatori e

discussant (fra i quali il Presidente del Garante) che hanno dibattuto sul tema dell'IA e sul suo impatto, da più prospettive, con una particolare attenzione al ruolo del RPD in tale contesto.

25.4. *"Amministrazione trasparente" e adempimenti relativi alla disciplina anticorruzione*

Presso l'Autorità ha continuato a trovare attuazione la normativa in materia di trasparenza; 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 dell'Autorità), come già segnalato nella precedente Relazione (par. 26.4), l'Autorità ha innovato il processo interno di pubblicazione di dati e documenti previsto dal d.lgs. n. 33/2013, completando il processo di migrazione dei contenuti pregressi dal sito istituzionale e raggiungendo una maggiore aderenza tra quanto previsto dalla normativa di settore e la qualità delle informazioni pubblicate, in linea con quanto indicato dall'all. 4 (Istruzioni operative per una corretta attuazione degli obblighi di pubblicazione ex d.lgs. n. 33/2013) approvato con delibera ANAC 25 settembre 2024, n. 495**.**

Sempre con riguardo ai profili di trasparenza amministrativa, sulla scorta della delibera ANAC 7 maggio 2025, n. 192 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 Responsabile della prevenzione della corruzione e della trasparenza (RPCT) che ha altresì provveduto a rinnovare tale monitoraggio, rendendone pubblici gli esiti.

Inoltre, in linea con quanto previsto dall'art. 43, d.lgs. n. 33/2013, è stata svolta un'attività di controllo costante sull'adempimento da parte dell'Autorità degli obblighi di pubblicazione previsti dalla normativa vigente. Per quanto concerne il sistema di gestione del rischio, è stato adottato, con deliberazione 29 gennaio 2026, n. 27, il Piano triennale di prevenzione della corruzione e della trasparenza (PTPCT) 2026-2028. Nello specifico si è proceduto ad aggiornare la mappatura dei processi, allineandola alla nuova realtà organizzativa scaturita dalle determine 13 marzo 2025, n. 193 (doc. web n. 10121422) e 30 dicembre 2025, n. 792 (doc. web n. 10209316), con la possibilità per i vari dipartimenti interessati di rimodulare le precedenti valutazioni di rischiosità dei processi esaminati tramite la compilazione di apposite schede di rilevazione predisposte dal RPCT.

In relazione alle misure generali inserite all'interno del PTPCT, un quadro sintetico degli aspetti salienti dell'attività svolta può desumersi dalla relazione annuale del RPCT riferita al 2025, oggetto di pubblicazione nella sezione Amministrazione trasparente.

Con riguardo all'attuazione delle misure di prevenzione generali e specifiche, il monitoraggio svolto nel 2025 sull'effettiva attuazione delle misure stesse ha condotto a realizzare attività di impulso finalizzate al miglioramento/aggiornamento di alcune delle misure generali più importanti nel corso del triennio 2026-2028.

Per quanto concerne la disciplina in materia di accesso civico introdotta con il d.lgs. n. 33/2013, è stato dato tempestivo riscontro a tutte le istanze pervenute nel 2025 (pari a 14) nonché a due istanze di riesame; 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 Transizione digitale e cybersicurezza

Le attività di transizione digitale svolte nel 2025 sono state concentrate su tre direttrici: 1) consolidamento della componente infrastrutturale ICT del sistema informativo; 2) azioni di sviluppo applicativo in ottica cloud per andare incontro alle esigenze di automazione dell'Ufficio e per offrire nuovi servizi online rivolti al pubblico degli utenti; 3) iniziative per il rafforzamento della postura di sicurezza e la gestione della sicurezza delle informazioni.

Nel corso del 2025 è stata consolidata la presenza presso il Polo strategico nazionale di tutti i sistemi applicativi e di supporto al funzionamento dell'intero sistema informativo del Garante, completando all'inizio dell'anno la migrazione avviata nel dicembre 2023.

Infrastrutture e servizi ICT

A seguito del completamento della migrazione e della avvenuta rendicontazione delle attività, la richiesta di erogazione del finanziamento PNRR relativa al "Progetto 1.1 Infrastrutture digitali - Altre PAC - giugno 2023" è stata approvata dalla Presidenza del Consiglio dei ministri - Dipartimento per la trasformazione digitale - e il finanziamento previsto di euro 628.844 è stato interamente liquidato nel corso del 2025.

Relativamente al portale web ufficiale, si è proceduto all'attivazione di un nuovo contratto esecutivo dell'accordo-quadro CONSIP 2296 "Sicurezza da remoto", sulla base del Piano dei fabbisogni e del Piano operativo definiti, mentre con separata attività e diverso fornitore è stato realizzato e reso disponibile il portale tematico relativo al G7 Privacy.

Relativamente al portale per l'attività di formazione online, basato sulla piattaforma open source Moodle, si è provveduto all'*hardening* del sistema operativo e delle applicazioni di base, per consentirne l'apertura e la consultazione al personale autorizzato anche dall'esterno della rete del Garante.

Nell'ambito della gestione documentale, si è provveduto alla implementazione, tramite il sistema Archiflow, del Registro delle violazioni, con la migrazione finale dei dati, la predisposizione della manualistica, la messa in produzione del sistema, la formazione iniziale rivolta agli utenti delle nuove funzionalità.

Relativamente alle attività di integrazione di componenti software di servizi applicativi, è stata portata a termine la revisione della procedura di *file transfer* sicuro con la Guardia di finanza; si è provveduto alla configurazione della componente SAML IDP di FortiAuth e alla integrazione tra *Active Directory* e i servizi applicativi cloud.

Nell'ambito del sistema IMI si è provveduto al passaggio delle utenze esistenti al sistema europeo di *multi factor authentication* EU Login, fornendo assistenza continua agli utenti interni.

La collaborazione applicativa e operativa con gli uffici amministrativi e con l'area giuridica è stata particolarmente intensa, in particolare con l'elaborazione dei moduli di valutazione del personale a compilazione automatica in PDF e con il supporto alla comparazione delle soluzioni per la gestione degli appalti e della trasparenza.

Relativamente ad altre attività inerenti servizi e infrastrutture ICT si è provveduto all'attivazione di procedure di *multi factor authentication* (MFA) su piattaforma *Outlook Web Access* (OWA); al potenziamento della *Virtual Desktop Infrastructure* (VDI) con l'aggiornamento della piattaforma Omnissa Horizon e dei *connection server* a Windows

Server 2025 e con l'implementazione del meccanismo di collegamento tramite *gateway* che rende non necessario il previo collegamento VPN; alla migrazione dell'infrastruttura di posta a gestione *on premise* alla versione 2025 di Microsoft Exchange; all'aggiornamento dell'intera infrastruttura di rilevamento presenze; alla predisposizione del servizio *SafeZone* per la gestione degli appelli in caso di evacuazione dell'ufficio; alla attivazione e configurazione di un nuovo *bucket* S3 da 50 Terabyte per operazioni di *backup on cloud*.

Il Garante ha inoltre aderito al programma di *Enterprise Agreement* con Microsoft con un cospicuo investimento per l'acquisto di nuove licenze relative all'utilizzo di diverse componenti software applicative, sistemistiche e di base.

Sviluppi applicativi

Per quanto riguarda gli sviluppi applicativi, le principali attività svolte nel 2025 sono state la implementazione dell'applicazione per la gestione dei ticket di assistenza tecnica ICT, gestita internamente; la maggiore integrazione degli applicativi online con il sistema di gestione documentale, con l'introdotta possibilità di consultare i documenti "originali" direttamente all'interno del sistema documentale Archiflow mediante l'utilizzo delle cosiddette *cardlink*; lo sviluppo dell'applicazione "Contratti" per la registrazione delle richieste di acquisto, la gestione dell'iter di stipulazione dei contratti e per la gestione del ciclo passivo di fatturazione; l'analisi e la realizzazione di prototipi per la migrazione dei contenuti del sito Intranet, con particolare attenzione alla copiosa documentazione prodotta dal Servizio studi e documentazione; l'analisi propedeutica alla reingegnerizzazione del sito Intranet; gli interventi evolutivi sul sistema di *Identity and Access Management* (IAM) – utilizzato per l'autenticazione dei cittadini che si avvalgono dei servizi online – finalizzati ad accrescerne i livelli di sicurezza; la revisione del processo di fascicolazione archivistica relativo alle segnalazioni in materia di telefonate indesiderate; l'integrazione del processo di firma remota nel *framework* applicativo cloud Salesforce; gli sviluppi relativi alle componenti di *back-end* delle applicazioni "Notifiche *data breach*" e "Segnalazioni *revenge porn*", per la gestione dei relativi carichi di lavoro e la realizzazione di *dashboard* direzionali.

Cybersicurezza

Per quanto attiene al rafforzamento della resilenza cyber dell'Autorità, nel corso del 2025 è proseguita l'attività di valutazione e promozione degli aspetti procedurali e organizzativi della cybersicurezza iniziata nel 2024 in concorso con l'Agenzia per la cybersicurezza nazionale (ACN), 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 si è declinato su due direttrici fondamentali: la prima area di intervento ha riguardato il rafforzamento delle capacità di rilevazione e risposta agli incidenti cyber, tanto dal punto di vista tecnico, attraverso l'adozione di un Sistema di gestione degli eventi e delle informazioni di sicurezza (SIEM), quanto da quello organizzativo, con la progettazione di un modello operativo di governo della gestione degli incidenti, supportato da una mappatura delle competenze richieste e da matrici di responsabilità operative.

La seconda area di intervento ha riguardato l'incremento di consapevolezza in ambito cyber, attraverso l'erogazione di sessioni di formazione a favore di tutto il personale dell'Autorità.

Ancora, nel corso del 2025, e sempre con riferimento all'intervento di cui al citato avviso pubblico n. 7/2023, è proseguita l'attività di mappatura, aggiornamento e formalizzazione di alcuni processi rilevanti per la gestione della sicurezza, finalizzata a 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, che andrà a compimento nel primo semestre del 2026.

Particolarmente significativa in ambito cybersicurezza è stata la partecipazione al bando dell'ACN per l'assegnazione di finanziamenti a valere sul Fondo per l'attuazione della Strategia nazionale di cybersicurezza e sul Fondo per la gestione della cybersicurezza di cui alla l. 29 dicembre 2022, n. 197. La scheda intervento presentata dal Responsabile della transizione digitale e denominata "55.1 - Attività di potenziamento di cybersicurezza - GPDP" è stata ritenuta idonea a ricevere il finanziamento di euro 2.500.000 che è stato accordato al Garante con d.P.C.M. 4 luglio 2025 e consentirà di realizzare nel corso del 2026 e del 2027 gli interventi previsti per il miglioramento della postura cyber dell'Autorità, con l'implementazione delle misure e degli obiettivi previsti.

IV

I DATI STATISTICI

Tabella 1.
Sintesi delle principali attività dell'Autorità

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	807
Partecipazione a consultazioni pubbliche	2
Audizioni del Presidente del Garante o memorie scritte trasmesse al Parlamento	13
Pareri su norme di rango primario statale, delle regioni e delle autonomie e su atti regolamentari e amministrativi	61
Pareri ai sensi dell'art. 36, par. 1, RGPD (valutazione d'impatto sulla protezione dati)	4
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	33
Approvazione regole deontologiche	0
Provvedimenti collegiali a seguito di reclamo	253
Provvedimenti collegiali a seguito di segnalazione	95
Provvedimenti collegiali a seguito di notifica di violazione di dati	12
Misure correttive e sanzionatorie (art. 58, par. 2, RGPD)	506
Ricorsi giurisdizionali trattati ex art. 152, d.lgs. n. 196/2003	89
Opposizioni (trattate) a provvedimenti del Garante	87
Pagamenti derivanti dall'attività sanzionatoria (euro)	37.760.961
Comunicazioni di notizia di reato all'autorità giudiziaria	65
Delibere dirigenziali in materia di *revenge porn* (adottate ai sensi dell'art. 33-*bis*, reg. Garante n. 1/2019) e ratificate dal Collegio	514
Provvedimenti di approvazione di codici di condotta	0
Violazioni di dati personali notificate	2.415
Accertamenti e controlli effettuati *in loco* (artt. 157-158, d.lgs. n. 196/2003)	130
Riscontri a reclami (art. 11, reg. Garante n. 1/2019)	4.288
Riscontri a segnalazioni (art. 11, reg. Garante n. 1/2019)	145.846
Riscontri a quesiti (art. 11, reg. Garante n. 1/2019)	423
Contatti Servizio relazioni con il pubblico	13.557
Reclami transfrontalieri e procedure di cooperazione ("sportello unico" - ex art. 60 del RGPD)	583
Procedure di coerenza (ex artt. 65-66 del RGPD)	0
Riunioni del Comitato europeo per la protezione dei dati personali	14
Partecipazione a sottogruppi di lavoro del Comitato europeo per la protezione dei dati personali	181
Riunioni Comitato di controllo coordinato (CSC)/organismi di supervisione	8
Riunioni presso il CoE	10
Riunioni presso l'OCSE	10
Conferenze internazionali	23
Altre conferenze e incontri	14
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	14
Istanze di riesame a seguito di diniego all'accesso civico presentate al RPCT e riscontrate ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	2

Tabella 2.
Pareri su norme di rango primario statale, delle regioni e delle autonomie

Pareri su norme di rango primario statale, delle regioni e delle autonomie	
Temi	**Riscontri resi nell'anno***
Giustizia	4
Sanità	3
Trasporti/traffico	1
Totale	**8**

Tabella 3.
Pareri su atti regolamentari e amministrativi resi al Governo, alle regioni e alle autonomie

Pareri su atti regolamentari e amministrativi resi al Governo, alle regioni e alle autonomie	
Temi	**Riscontri resi nell'anno***
Ambiente	1
Digitalizzazione p.a.	5
Fisco/riciclaggio	2
Funzioni di interesse pubblico	2
Giustizia	4
Imprese	1
Istruzione	2
Lavoro	5
Sanità	16
Sicurezza	1
Totale	**39**

Tabella 4.
Pareri su atti regolamentari e amministrativi resi ad altre istituzioni

Pareri su atti regolamentari e amministrativi resi ad altre istituzioni	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	1
Diritti fondamentali	3
Fisco	3
Funzioni di interesse pubblico	4
Giustizia	1
Statistica	2
Totale	**14**

(*) inerenti anche ad affari pervenuti anteriormente al 2025

Pareri ex art. 36, par. 1, RGPD (valutazione d'impatto sulla protezione dati)	
Temi	**Riscontri resi nell'anno***
Sicurezza	4
Totale	**4**

Tabella 5.
Pareri ex art. 36, par. 1, RGPD (valutazione d'impatto sulla protezione dati)

(*) inerenti anche ad affari pervenuti anteriormente al 2025

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))	16
Ammonimenti a titolare/responsabile del trattamento per violazioni RGPD (art. 58, par. 2, lett. b))	91
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))	11
Ingiunzioni a titolare/responsabile del trattamento di conformare i trattamenti alle disposizioni del RGPD (art. 58, par. 2, lett. d))	72
Ingiunzioni a titolare del trattamento di comunicare all'interessato una violazione dei dati personali (art. 58, par. 2, lett. e), RGPD)	4
Imposizioni di limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento (art. 58, par. 2, lett. f), RGPD)	69
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	14
Sanzioni amministrative pecuniarie ex art. 83 (art. 58, par. 2, lett. i), RGPD)	229
Totale	**506**

Tabella 6.
Misure correttive e sanzionatorie (art. 58, par. 2, RGPD)

Pagamenti derivanti dall'attività sanzionatoria	
Pagamenti spontanei dei contravventori	31.933.566
Riscossione coattiva	5.827.395
Totale	**37.760.961**

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.)	2
Associazione per delinquere (art. 416, c.p.) e comunicazione e diffusione illecita su larga scala (art. 167-*bis* del Codice)	1
Estorsione (art. 629, c.p.) nella forma di reato tentato ai sensi dell'art. 56, c.p.	1
Ipotesi di reato rinvenute in occasione dell'attività svolta ai sensi dell'art. 144-*bis*, d.lgs. n. 196/2003 (artt. 629, 609-*bis* e 600-*ter,* c.p.)	54
Violazioni in materia di controlli a distanza dei lavoratori (art. 171, d.lgs. n. 196/2003)	7
Totale	**65**

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	514
Soggetti privati	1.901
Totale	**2.415**

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	915
Preliminare	1.500
Integrativa*	2.112
Totale	**4.527**

Grafico 11.
Notifiche di violazioni di dati ricevute (per natura della violazione)

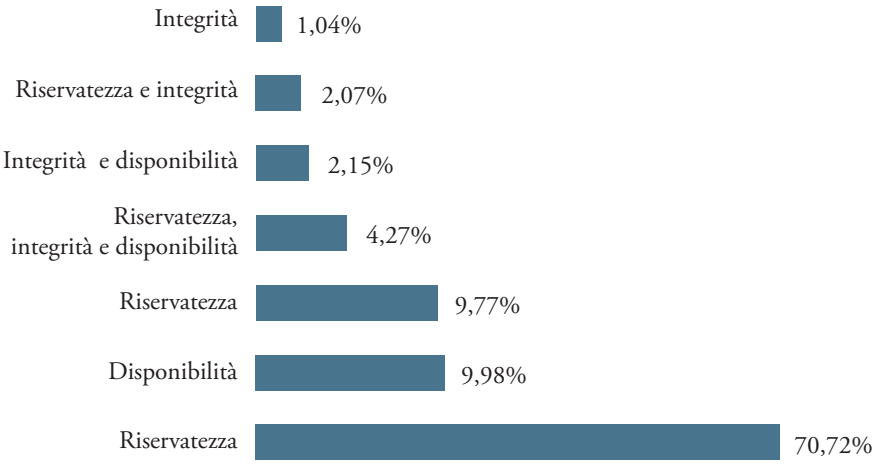


Tabella 12.
Reclami

Reclami			
	Pervenuti nell'anno	Riscontri resi nell'anno (*)	Riscontri resi nell'anno con provvedimento collegiale**
Affari di giustizia e di sicurezza	186	120	4
Affari legali e di giustizia	0	1	0
Attività economiche e lavoro	1723	322	32
Attività ispettive	0	1	
Associazioni, liberi professionisti e videosorveglianza	534	13	4
Intelligenza artificiale	2	1	0
Libertà di manifestazione del pensiero e cyberbullismo	524	381	70
Realtà economiche e produttive	452	757	18
Realtà pubbliche	723	743	66
Reti telematiche e marketing	2.134	1.688	41
Sanità e ricerca	152	132	15
Tecnologie digitali e sicurezza informatica	84	35	0
Altre UU.OO.	90	94	0
Totale	**6.604**	**4.288**	**250**

(*) inerenti anche ad affari pervenuti anteriormente al 2025 e conclusi ai sensi dell'art. 11, reg. Garante 1/2019

(**) inerenti anche ad affari pervenuti anteriormente al 2025

Segnalazioni			
	Pervenuti nell'anno	Riscontri resi nell'anno (*)	Riscontri resi nell'anno con provvedimento collegiale**
Affari di giustizia e di sicurezza	223	100	2
Affari legali e di giustizia	2	3	0
Attività economiche e lavoro	1.946	131	4
Attività ispettive	1	3	0
Associazioni, liberi professionisti e videosorveglianza	988	56	14
Intelligenza artificiale	6	0	0
Libertà di manifestazione del pensiero e cyberbullismo	1.667	1.172***	0
Realtà economiche e produttive	599	1.061	8
Realtà pubbliche	1.158	1.519	22
Reti telematiche e marketing	108.159****	141.189****	40
Sanità e ricerca	336	302	8
Tecnologie digitali e sicurezza informatica	48	182	0
Altre UU.OO.	142	128	0
Totale	**115.275**	**145.846**	**98**

Tabella 13.
Segnalazioni

(*) inerenti anche ad affari pervenuti anteriormente al 2025 e conclusi ai sensi dell'art. 19, reg. Garante 1/2019

(**) inerenti anche ad affari pervenuti anteriormente al 2025

(***) di cui 514 in materia *revenge porn*

(****) di cui 104.433 telemarketing automatizzato

(*****) di cui 138.895 telemarketing automatizzato

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
Affari di giustizia e sicurezza	5	10
Affari legali e giustizia	1	1
Associazioni, liberi professionisti e videosorveglianza	27	0
Attività economiche e lavoro	28	2
Attività ispettive	1	1
Intelligenza artificiale	0	1
Libertà di manifestazione del pensiero e cyberbullismo	2	1
Realtà economiche e produttive	14	49
Realtà pubbliche	71	241
Reti telematiche e marketing	12	5
Sanità e ricerca	17	23
Tecnologie digitali e sicurezza informatica	1	0
Altre UU.OO.	91	89
Totale	**386**	**423**

Tabella 14.
Quesiti

(*) inerenti anche ad affari pervenuti anteriormente al 2025

Servizio relazioni con il pubblico	
E-mail esaminate	8.432
Contatti telefonici	4.935
Persone in visita al SRP	13
Trattazione pratiche relative a fascicoli	177
Totale	**13.557**

Tabella 15.
Servizio relazioni con il pubblico

Grafico 16.
Oggetto delle e-mail esaminate dal Servizio relazioni con il pubblico

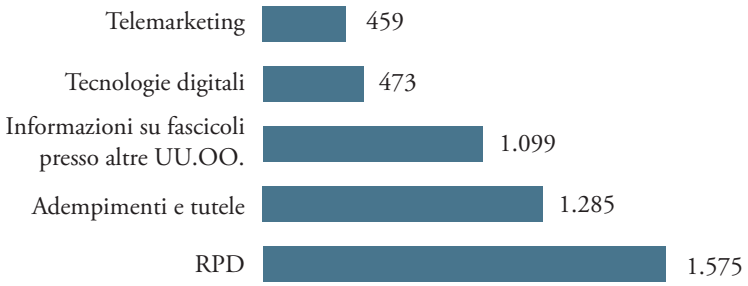


Tabella 17.
Reclami transfrontalieri e procedure di cooperazione ("sportello unico" – ex art. 60 del RGPD)

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	**15**	2	30	**568**	67	22

Tabella 18.
Assistenza reciproca e operazioni congiunte

Assistenza reciproca e operazioni congiunte		
	Richieste inviate	Richieste ricevute
Numero di richieste di assistenza reciproca volontaria (VMN)	54	330
Numero di richieste formali di assistenza reciproca ex art. 61	2	17
Numero di operazioni congiunte ex art. 62	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	0	0	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	59
Newsletter	11
Prodotti editoriali	6
Campagne informative	3
Video spot e *teaser* informativi	55
Infografiche e pagine tematiche	49

Tabella 22.
Attività di comunicazione dell'Autorità

Tabella 23.
Personale in servizio

Personale in servizio (*)					
Area	N. posti nella dotazione organica	Personale di ruolo (a)	Personale di ruolo di altre amministrazioni in servizio presso il Garante (b)	Personale di ruolo del Garante in comando, aspettativa o equiparato presso altre amm.ni (c)	In servizio presso l'Ufficio (a+b-c)
Segretario generale	1	1	0	0	1
Dirigenti	24	19	0	3	16
Funzionari	127	120	4	3	121
Operativi	46	42	1	1	42
Esecutivi	2	2	0	0	2
Totale	**200**	**184**	**5**	**7**	**182**
Personale a contratto					16

(*) Situazione alla data del 31/12/2025

Tabella 24.
Gestione finanziaria

Gestione finanziaria						
Entrate accertate	**Anno 2025**		**Anno 2024**		**Variazione**	
					€	**%**
Entrate correnti		47.421.799		50.444.771	-3.022.972	5.99
Entrate in c/capitale		625.000		0	625.000	100
Totale entrate euro		**48.046.799**		**50.444.771**	**-2.397.972**	**-4,75**
Spese impegnate	**Anno 2025**		**Anno 2024**		**Variazione**	
					€	**%**
Spese di funzionamento (*)		47.657.304		40.916.365	6.740.939	16,47
**di cui trasferimenti ad amministrazioni*	*410.380*		*337.175*			
Spese in c/capitale		246.277		129.464	116.813	90,23
Totale spese euro		**47.903.581**		**41.045.829**	**6.857.752**	**16,71**

Impaginazione, Grafica e Stampa
Solved S.r.l.

Garante per la protezione dei dati personali
Piazza Venezia, 11 - 00187, Roma
Centralino 06.69677.1
protocollo@gpdp.it
www.garanteprivacy.it

Stampa: **Solved** S.r.l.
Via Roberto Paribeni, 29/L - 00173 Roma
Tel. +39 06.64.83.56.67

GPDP
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI