GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento del 3 settembre 2026 [10297167]

[doc. web n. 10297167]

Provvedimento del 3 settembre 2026

Registro dei provvedimenti
n. 620 del 3 settembre 2026

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia, componente, e il dott. Luigi Montuori, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE" (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

Relatore il dott. Agostino Ghiglia;

PREMESSO

1. Introduzione.

Con distinti ma connessi reclami, presentati ai sensi degli artt. 77 del Regolamento nei confronti dell'Istituto Nazionale di Ricerca Metrologica - INRIM (di seguito, l'"Istituto"), due dipendenti dello stesso hanno lamentato una presunta violazione della normativa in materia di protezione dei dati personali.

In particolare, è stato rappresentato che, dopo aver stipulato un accordo con le rappresentanze sindacali, ai sensi dell'art. 4 della l. 20 maggio 1970, n. 300, in relazione all'impiego di un impianto di videosorveglianza presso la sede di Torino dell'Istituito, detto impianto sarebbe stato attivato in fase di test, senza, tuttavia, assicurare la dovuta trasparenza del trattamento nei confronti degli interessati (lavoratori e persone fisiche che a vario titolo visitano la sede), sottoponendo a videosorveglianza aree non contemplate nell'accordo,

nonché ricorrendo a monitor di controllo collocati in aree potenzialmente accessibili anche a soggetti non autorizzati.

2. L'attività istruttoria.

In riscontro a una richiesta d'informazioni (v. XX), formulata ai sensi dell'art. 157 del Codice, l'Istituto, con nota del XX (prot. n. XX), come integrata con successiva nota del XX (prot. n. XX), ha dichiarato, in particolare, che:

- "l'impianto di videosorveglianza oggetto di accordo sindacale stipulato il 16 maggio 2025 ai sensi dell'art. 4 della legge n. 300/1970 […] è stato installato presso la sede INRiM di Torino";

- "le operazioni di installazione fisica delle telecamere, avviate il 19 maggio 2025, sono terminate il giorno 30 ottobre 2025. Risultano installate n. 18 telecamere";

- "il 31 ottobre 2025 l'impianto risulta essere stato attivato in modalità test, attivazione mantenuta anche nelle successive giornate festive e di chiusura dell'Istituto del 1° e del 2 novembre […;] in fase di test risulta attivata la sola funzione di visualizzazione, senza alcuna registrazione delle immagini";

- "nelle giornate lavorative successive, dal 3 al 5 novembre, l'impresa incaricata - per effettuare tarature e regolazioni delle telecamere e dei monitor - ha attivato l'impianto per qualche ora, sempre senza alcuna registrazione delle immagini";

- "dal 6 novembre 2025, al fine di collaudare l'impianto, lo stesso è stato attivato esclusivamente nelle ore di chiusura notturna dell'Ente, dalle 20:30 alle 7:30, e nelle giornate di chiusura: sabati, domeniche e festivi. Nelle fasce orarie di accensione, la registrazione delle immagini avviene solo a seguito di attivazione dell'allarme, cioè a seguito dell'attraversamento della barriera ottica […;] le aree soggette alla videosorveglianza sono tutte interne al perimetro di competenza dell'Istituto, rimanendo esclusa la possibilità di filmare aree ad accesso pubblico";

- "[…] l'impianto non è pertanto mai entrato in esercizio per le prescritte finalità di sorveglianza, sancite dall'[…] Accordo, ma solo per la verifica della funzionalità tecnica e dell'adeguatezza dello stesso, con specifico riguardo alla effettiva e efficace copertura del perimetro di sicurezza e al corretto funzionamento delle telecamere e dei monitor";

- "l'Accordo si basa su[…] finalità […di] tutela del patrimonio aziendale […, consentendo di…] riprendere esclusivamente i muri e le recinzioni perimetrali";

- l'accordo sindacale consentiva "[…] adattamenti dovuti alla presenza di ostacoli visivi (es. vegetazione e strutture esistenti) […]";

- "la planimetria allegata all'accordo prevedeva l'installazione di n. 10 telecamere. In fase di progettazione definitiva e installazione tecnica è tuttavia emerso che il numero di dispositivi non risultava sufficiente a garantire un'adeguata copertura delle aree da presidiare e, conseguentemente, a perseguire in modo efficace le finalità proprie del sistema di videosorveglianza […] si è reso pertanto necessario integrare il numero originariamente previsto con ulteriori n. 8 telecamere";

- "tale modifica, tuttavia, di per sé non deve ritenersi lesiva dell'accordo. È infatti l'accordo stesso a prevedere forme di verifica della coerenza dell'installazione effettiva rispetto a quanto concordato. All'art. 7 si prevede infatti che: "La coerenza dell'impianto, nella sua installazione finale, rispetto a quanto presentato nel presente accordo, potrà essere soggetta a verifica da parte della RSU e/o delle OO.SS., inoltrando la richiesta alla Direzione Generale";

- "in questo senso deve essere letta la comunicazione e-mail del Direttore Generale del 14 novembre 2025 […] con cui l'Istituto ha rappresentato alla RSU la necessità di convocare un incontro finalizzato a illustrare le integrazioni effettuate, al fine di valutare la rispondenza del sistema alle finalità concordate";

- “i tempi di conservazione dei filmati, in caso di attivazione del sistema, sono quelli indicati all’art. 2.4 [dell’accordo sindacale,] ai sensi del quale: “Il termine massimo previsto per la conservazione delle immagini videoregistrate è di 72 ore dalla rilevazione delle stesse […]”;

- “la fase di collaudo e verifica, con il coinvolgimento della RSU, non risulta terminata e, pertanto, il sistema non è ancora entrato in esercizio”;

- “conseguentemente, l’informativa sul trattamento dei dati personali non è stata ancora resa al personale dell’Istituto [; …] l’informativa verrà fornita ai lavoratori in ogni caso prima dell’entrata in esercizio dell’impianto mediante pubblicazione sulla intranet istituzionale, previa apposita comunicazione interna”;

- “la cartellonistica [contenente l’informativa di primo livello, è stata affissa] il 17 novembre 2025”;

- “l’informativa di secondo livello sarà messa a disposizione degli interessati mediante pubblicazione sul sito web istituzionale dell’Istituto”;

- “l’INRiM ha ritenuto di posticipare [la] valutazione [di impatto sulla protezione dei dati] all’effettiva definizione dell’assetto tecnico e organizzativo dell’impianto, in ogni caso propedeuticamente alla sua entrata in esercizio”;

- “i monitor di sorveglianza sono posizionati nella portineria, locale dove opera - in orario diurno - il personale della società affidataria del relativo servizio e, in orario notturno, il personale della società cui è affidata la vigilanza armata”;

- “a seguito delle attività di test è stata rilevata la necessità di oscuramento di alcune vetrate della portineria, da realizzarsi prima dell’entrata in esercizio dell’impianto”;

- “[…] l’accesso ai filmati sarà limitato al personale dell’Istituto all’uopo autorizzato”.

Con nota del XX (prot. n. XX), l’Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell’attività istruttoria, ha notificato all’Istituto, ai sensi dell’art. 166, comma 5, del Codice, l’avvio del procedimento per l’adozione dei provvedimenti di cui all’art. 58, par. 2, del Regolamento, per aver lo stesso posto in essere un trattamento, mediante telecamere di videosorveglianza, dei dati personali dei lavoratori in servizio e di altri soggetti a vario titolo presenti presso la sede di Torino, in maniera non conforme al principio di “liceità, correttezza e trasparenza” e in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) e parr. 2 e 3, e 88, par. 1, del Regolamento, nonché 2-ter e 114 del Codice (in riferimento all’art. 4 della l. n. 300/1970); per non aver assicurato la necessaria trasparenza del trattamento nei confronti degli interessati, in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento; per non aver svolto una valutazione di impatto sulla protezione dei dati prima di dare avvio al trattamento, in violazione dell’art. 35 del Regolamento. Con la medesima nota, il predetto titolare è stato invitato a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall’Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, della l. 24 novembre 1981, n. 689).

Con nota del XX (prot. n. XX), l’Istituto ha presentato una memoria difensiva, dichiarando, in particolare, che:

- “l'attivazione in [fase di] test del sistema è avvenuta […] con modalità significativamente circoscritte sia sotto il profilo operativo che temporale”;

- “il sistema operava esclusivamente in modalità di visualizzazione, senza alcuna registrazione delle immagini e l'attivazione dell'impianto in presenza del personale si è limitata a un numero estremamente circoscritto di giornate lavorative (quattro giornate lavorative complessive) e precisamente: alla giornata di venerdì 31 ottobre 2025 e, successivamente, al periodo compreso tra il 3 e il 5 novembre 2025, per il tempo strettamente necessario (quantificabile in qualche ora giornaliera) all'esecuzione delle attività di verifica, taratura e regolazione delle apparecchiature da parte dell'impresa incaricata […]”;

- “[…] il sistema non è mai stato utilizzato per il controllo dell'attività lavorativa dei dipendenti o per finalità disciplinari […]”;

- “le attività […] sono state poste in essere nel contesto di una fase di installazione, verifica tecnica e collaudo dell'impianto che l'Istituto riteneva non ancora corrispondente alla sua effettiva entrata in esercizio per le finalità di videosorveglianza previste dall'Accordo sindacale”;

- vi è stata, pertanto, “un'erronea valutazione interpretativa del quadro normativo applicabile alla fase di test e collaudo del sistema”;

- sussistevano “circostanze tecniche che hanno reso necessaria, in fase di installazione, l’integrazione del numero dei moduli di ripresa ottica (da 10 a 18) [… per] garantire la continuità della copertura perimetrale dell'Istituto […]”;

- “l'Istituto ha […] avviato la predisposizione della documentazione privacy correlata all'impianto”;

- “in data 12 giugno 2026 si è tenuto l'incontro convocato dalla Direzione Generale con le rappresentanze sindacali […e] le parti hanno convenuto sull'opportunità di acquisire ulteriori elementi tecnici dalla ditta installatrice e di procedere, all'esito dei necessari approfondimenti, a un ulteriore momento di verifica congiunta”.

3. Esito dell’attività istruttoria.

3.1 La liceità del trattamento.

Il trattamento di dati personali relativi a lavoratori, posto in essere mediante telecamere di videosorveglianza, idonee a riprendere anche il personale che transita o sosta nei luoghi di lavoro, può essere effettuato dal datore di lavoro se esso è necessario per la gestione del rapporto di lavoro, nel rispetto del quadro giuridico applicabile, definito dalla normativa nazionale ed eurounitaria, da regolamenti o da contratti collettivi (artt. 6, par. 1, lett. c), e 88 del Regolamento).

In tale quadro, il datore di lavoro deve rispettare le norme nazionali che “includono misure appropriate e specifiche a salvaguardia della dignità umana […] degli interessati in particolare per quanto riguarda la trasparenza del trattamento […] e i sistemi di monitoraggio sul posto di lavoro” (88, par. 2, del Regolamento, a cui fa rinvio l’art. 6, par. 2, del Regolamento).

Come costantemente ribadito nei provvedimenti del Garante, i trattamenti conseguenti all’impiego di strumenti tecnologici nei luoghi ove si svolge anche l’attività lavorativa trovano la propria base giuridica nella disciplina di settore di cui all’art. 4 della l. 20 maggio 1970, n. 300 (Statuto dei Lavoratori), il cui comma 1 prevede che “gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali […]. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, […] della sede centrale dell'Ispettorato nazionale del lavoro”.

Tale disposizione perimetra in modo uniforme a livello nazionale l’ambito del trattamento consentito in ogni contesto lavorativo (pubblico e privato) e costituisce nell’ordinamento interno una disposizione più specifica e di maggiore garanzia di cui all’art. 88 del Regolamento, la cui osservanza - per effetto del rinvio contenuto nel Codice alle preesistenti disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro, con particolare riferimento ai possibili controlli da parte del datore di lavoro (art. 114 “Garanzie in materia di controllo a distanza”) - è condizione di liceità del trattamento (v. art. 5, par.1, lett. a) e 6, par. 1, lett. c) del Regolamento; cfr., a livello europeo, le indicazioni contenute nelle “Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video”, adottate dal Comitato europeo per la protezione dei dati il 29 gennaio 2020, par. 11, nonché le precedenti indicazioni del Gruppo di Lavoro Articolo 29 nel “Parere 2/2017 sul trattamento dei dati sul posto di lavoro”, WP 249; cfr. par. 4.1 del “Provvedimento in materia di videosorveglianza” dell’8 aprile 2010, doc. web n. 1712680, e, da ultimo, la FAQ n. 9 del Garante in materia di videosorveglianza, del dicembre 2020, doc. web 9496574, e le numerose decisioni del Garante

riferite a casi concreti, tra cui, con specifico riguardo al ricorso alla videosorveglianza sui luoghi di lavoro, provv.ti 12 febbraio 2026, n. 70, doc. web n. 10226611; 29 gennaio 2026, n. 43, doc. web n. 10226639; 23 ottobre 2025, n. 628, doc. web n. 10196164; 10 luglio 2025, n. 410, doc. web n. 10162731; 10 aprile 2025, n. 201, doc. web n. 10139433; 11 aprile 2024, n. 234, doc. web n. 10013356; 16 novembre 2023, n. 578, doc. web n. 9963486; 11 marzo 2021, n. 90, doc. web n. 9582791; 5 marzo 2020, n. 53, doc. web n. 9433080; cfr. provv. 19 settembre 2019, n. 167, doc. web n. 9147290).

Ciò in conformità alla giurisprudenza della Corte europea dei diritti dell'uomo, nel caso Antovic e Mirković v. Montenegro (Application n. 70838/13 del 28.11.2017), che ha stabilito che il rispetto della vita privata deve essere esteso anche ai luoghi di lavoro pubblici, evidenziando che l'impiego di dispositivi video sul posto di lavoro può essere giustificato solo nel rispetto delle garanzie previste dalla legge nazionale applicabile, in mancanza delle quali costituisce un'interferenza illecita nella vita privata del dipendente, ai sensi dell'art. 8, par. 2, della CEDU.

Nel caso oggetto di istruttoria, l'Istituto, in data 16 maggio 2025, ha stipulato con le organizzazioni sindacali, ai sensi dell'art. 4 della l. n. 300/1970, un accordo relativo all'impiego di un "impianto di videosorveglianza perimetrale" (premesse) presso la propria sede di Torino per "garantire la tutela del patrimonio aziendale" (art. 1.1). In detto accordo si precisa che "le TVCC saranno installate in modo da riprendere esclusivamente i muri e le recinzioni perimetrali, compatibilmente con i necessari adattamenti dovuti alla presenza di ostacoli visivi (es. vegetazioni e strutture esistenti) […] secondo la planimetria di dettaglio fornita in visione alle Parti sindacali" (art. 2.1); "il sistema provvede a registrare le immagini rilevate dalla TVCC su tutto l'arco delle 24 ore anche nelle giornate di sabato, domenica, festivi e nei giorni di chiusura" (art. 2.3).

Dopo aver stipulato tale accordo con le organizzazioni sindacali, l'Istituto ha, tuttavia, installato l'impianto in maniera non conforme alla planimetria condivisa con le organizzazioni sindacali, aumentando di otto unità il numero di telecamere previsto e modificando la loro collocazione e la relativa area di ripresa. Ciò nonostante lo stesso accordo sindacale prevedesse che "l'impianto di videosorveglianza perimetrale potrà essere oggetto di interventi di manutenzione straordinaria, inclusi miglioramenti o aggiornamento tecnologici non sostanziali, senza necessità di modifica del presente accordo, a condizione che non vengano alterate […] le zone di ripresa definite" (art. 2.5).

L'Istituto ha messo in funzione tale impianto, in maniera non conforme alla planimetria condivisa con le organizzazioni sindacali, anche in giornate lavorative (in data 31 ottobre 2025 e poi dal 3 al 5 novembre, ancorché per qualche ora in ciascuna giornata).

Sebbene l'attivazione dell'impianto sia stata effettuata a fini di test del sistema e senza procedere alle registrazioni delle immagini, con la sola visualizzazione delle stesse in tempo reale, essa ha comunque comportato un trattamento di dati personali dei lavoratori in servizio e di altri soggetti a vario titolo presenti presso la sede di Torino, secondo modalità difformi da quelle concordate con le organizzazioni sindacali e, pertanto, in maniera non conforme al principio di "liceità, correttezza e trasparenza" e in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) e parr. 2 e 3, e 88, par. 1, del Regolamento, nonché 2-ter e 114 del Codice (in riferimento all'art. 4 della l. n. 300/1970).

Non si ritiene, invece, di poter accogliere il motivo di reclamo che attiene alla collocazione dei monitor di controllo in aree potenzialmente accessibili anche a soggetti non autorizzati, tenuto conto che, come dichiarato dall'Istituto nel corso dell'istruttoria, con assunzione di responsabilità anche ai sensi dell'art. 168 del Codice, tali monitor sono posizionati nella portineria, locale in cui opera unicamente il personale addetto al servizio di portineria o alla vigilanza, e che, conclusa la fase di test e una volta avviato l'impianto in regime ordinario, saranno comunque oscurate alcune vetrate della portineria per evitare che i monitor possano essere visionati da soggetti non autorizzati.

3.2. La trasparenza del trattamento.

3.2.1. Nei confronti dei lavoratori.

Nel rispetto del principio di "liceità, correttezza e trasparenza" (art. 5, par. 1, lett. a), del Regolamento), il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 del Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (cfr. art. 12, par. 1, del Regolamento).

L'Istituto ha, a tal riguardo, dichiarato di non aver fornito ai propri lavoratori una specifica informativa relativa al sistema di videosorveglianza in questione nelle more "della definizione, da verificare con la RSU, degli aspetti tecnico-funzionali".

Come sopra illustrato, l'Istituto ha, tuttavia, messo in funzione l'impianto di videosorveglianza in alcune giornate di apertura degli uffici, peraltro con modalità difformi da quelle concordate con le organizzazioni sindacali, senza che i lavoratori avessero contezza di tale circostanza e delle caratteristiche essenziali del conseguente trattamento dei propri dati personali.

L'Istituto avrebbe, invece, dovuto fornire ai propri lavoratori una specifica informativa sul trattamento dei dati personali prima di mettere in funzione l'impianto e dunque prima di dare corso a qualunque trattamento di dati mediante detto impianto, essendo irrilevante che l'attivazione dello stesso sia avvenuta a soli fini di test e di verifica tecnica.

Deve, pertanto, concludersi che l'Istituto ha agito in maniera non conforme al principio di "liceità, correttezza e trasparenza", in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento.

3.2.2. Nei confronti delle altre categorie di interessati.

Allorquando siano impiegati dispositivi video, il titolare del trattamento, oltre a rendere l'informativa di primo livello mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, deve fornire agli interessati anche delle "informazioni di secondo livello", che devono "contenere tutti gli elementi obbligatori a norma dell'articolo 13 del [Regolamento]" ed "essere facilmente accessibili per l'interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale […] o affissa in un luogo di facile accesso" ("Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", cit., in particolare par. 7; ma si veda già il "Provvedimento in materia di videosorveglianza" del Garante dell'8 aprile 2010, cit., in particolare par. 3.1; da ultimo, v. la FAQ n. 4 del Garante in materia di videosorveglianza, cit.).

Le informazioni di primo livello (cartello di avvertimento) "dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento" ("Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", cit., par. 114). Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l'interessato. Potrebbe trattarsi, ad esempio, della trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'UE, e del periodo di conservazione dei dati. Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale, senza alcuna registrazione di dati o trasmissione a soggetti terzi (ibidem, cit., par. 115). La segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento al secondo livello di informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa.

Nel caso si specie, l'Istituto, pur avendo attivato l'impianto di videosorveglianza in data 31 ottobre 2025 e poi dal 3 al 5 novembre (per qualche ora in ciascuna giornata), ha dichiarato di aver apposto "la cartellonistica [, contenente l'informativa di primo livello sul trattamento dei dati, [soltanto] il 17 novembre 2025", mentre nessuna informativa di secondo livello è stata messa a disposizione degli interessati.

Deve, peraltro, osservarsi che tale cartello, affisso successivamente alle date in cui il sistema di videosorveglianza è stato attivato a fini di test, non risulta comunque conforme alla disciplina in materia di protezione dei dati, atteso che esso non indica chiaramente gli estremi del titolare del trattamento (si legge soltanto l'acronimo "INRIM", senza alcun dato di recapito/contatto); fa riferimento a una finalità di trattamento generica e che può essere fuorviante ("sicurezza") in luogo di quella effettivamente perseguita (tutela del patrimonio aziendale); non menziona l'esistenza dei diritti degli interessati, non indica i tempi di conservazione dei dati e non chiarisce che il c.d. "QR Code" consente di consultare un'informativa completa di secondo livello (cfr. il modello esemplificativo di cartello informativo sub par. 115 delle "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", cit.).

L'Istituto ha, pertanto, agito in maniera non conforme al principio di "liceità, correttezza e trasparenza" e in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento.

3.3 La valutazione di impatto sulla protezione dei dati.

Quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche e, in ogni caso, al ricorrere delle ipotesi tassativamente previste, il titolare del trattamento, prima di porre in essere lo stesso, deve svolgere una valutazione di impatto sulla protezione dei dati, al fine di adottare, in particolare, le misure adeguate ad affrontare tali rischi, consultando preventivamente il Garante, ove ne ricorrano i presupposti (v. artt. 35 e 36, par. 1, del Regolamento).

Tenuto conto delle indicazioni fornite anche a livello europeo sul punto, si ritiene che, nel caso specie, l'Istituto avrebbe dovuto svolgere una valutazione di impatto sulla protezione dei dati prima di avviare il trattamento, atteso che lo stesso comportava rischi specifici per i diritti e le libertà dei lavoratori. Ciò, tanto in considerazione della particolare "vulnerabilità" degli interessati nel contesto lavorativo (cfr. cons. 75 e art. 88 del Regolamento e le "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679", WP 248 del 4 aprile 2017, che, tra le categorie di interessati vulnerabili, menzionano espressamente "i dipendenti") quanto del fatto che sono impiegati sistemi che comportano il "monitoraggio sistematico" in ambito lavorativo, inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti" (cfr. criterio n. 3 indicato nelle Linee guida, cit., ma vedi anche criteri 4 e 7; v. artt. 35 e 88, par. 2, del Regolamento; v. anche provv. 11 ottobre 2018, n. 467, doc. web n. 9058979, all. n. 1, che espressamente menziona i "trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici […] dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti"). La mancata esecuzione di una valutazione di impatto sulla protezione dei dati in relazione a sistemi di videosorveglianza impiegati nel contesto lavorativo è stata, per tali motivi, oggetto di recenti provvedimenti anche correttivi e sanzionatori del Garante (v. in particolare, provv.ti 12 febbraio 2026, n. 70, doc. web n. 10226611; 29 gennaio 2026, n. 43, doc. web n. 10226639; 23 ottobre 2025, n. 628, cit.; 10 luglio 2025, n. 410, doc. web n. 10162731; 10 aprile 2025, doc. web n. 10139433; 13 marzo 2025, n.135, doc. web n. 10128005; 16 novembre 2023, n. 578, doc. web n. 9963486).

Alla luce di tutte le considerazioni che precedono, deve concludersi che l'Istituto ha posto in essere un trattamento di dati personali dei lavoratori, mediante il sistema di videosorveglianza in questione, in assenza di una preliminare valutazione di impatto sulla protezione dei dati e, pertanto, in violazione dell'art. 35 del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria - della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice -, seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dall'Istituto, per aver posto in essere un trattamento di dati personali, mediante telecamere di videosorveglianza, in violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) e parr. 2 e 3, 12, par. 1, 13, 35 e 88, par. 1, del Regolamento, nonché 2-ter e 114 del Codice (in riferimento all'art. 4 della l. n. 300/1970).

Tenuto conto che la violazione delle predette disposizioni ha avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, le violazioni più gravi, relative agli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) e parr. 2 e 3, 12, par. 1, 13 e 88, par. 1, del Regolamento, nonché 2-ter del Codice, sono soggette alla sanzione prevista dall'art. 83, par. 5, del Regolamento, come richiamato anche dall'art. 166, comma 2, del Codice, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti, atteso che, come dichiarato dall'Istituto, le telecamere di videosorveglianza in questione sono state attivate in orario di

apertura degli uffici soltanto per quattro giornate lavorative, non ricorrono i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2, del Regolamento.

5. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

Tenuto conto che:

- ancorché il trattamento sia avvenuto in maniera non pienamente conforme a quanto previsto dall'accordo sindacale, esso è stato posto in essere a fini di test e nel corso di alcune ore in sole quattro giornate lavorative (cfr. art. 83, par. 2, lett. a), del Regolamento);

- la violazione ha carattere colposo (cfr. art. 83, par. 2, lett. b), del Regolamento);

- il trattamento non ha riguardato dati particolari appartenenti alle categorie particolari di cui all'art. 9 del Regolamento (cfr. art. 83, par. 2, lett. g), del Regolamento),

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia basso (cfr. Comitato europeo per la protezione dei dati, "Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR" del 24 maggio 2023, punto 60).

Ciò premesso, nel considerare che il titolare del trattamento è un ente pubblico di ricerca a rilevanza nazionale, ma operante su base locale e senza fornire servizi direttamente all'utenza, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

- l'Istituto ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria (cfr. art. 83, par. 2, lett. f), del Regolamento);

- non risultano precedenti violazioni pertinenti commesse dall'Istituto (cfr. art. 83, par. 2, lett. e), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 10.000 (diecimila) per la violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) e parr. 2 e 3, 12, par. 1, 13, 35 e 88, par. 1, del Regolamento, nonché 2-ter e 114 del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione del fatto che il trattamento ha riguardo i dati personali di dipendenti, soggetti vulnerabili nel contesto lavorativo, peraltro non informati in merito alle caratteristiche del trattamento.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dall'Istituto per la violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) e parr. 2 e 3, 12, par. 1, 13, 35 e 88, par. 1, del Regolamento, nonché 2-ter e 114 del Codice, nei termini di cui in motivazione;

ORDINA

all'Istituto Nazionale di Ricerca Metrologica (INRIM), in persona del legale rappresentante pro-tempore, con sede legale in Strada Delle Cacce, 91 - 10135 Torino (TO), C.F. 09261710017, di pagare la somma di euro 10.000 (diecimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al predetto Istituto, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 10.000 (diecimila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

- ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell'Autorità;

- ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento.

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 3 settembre 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Montuori