Provvedimento del 29 gennaio 2026 [10221611]

VEDI ANCHE Newsletter del 20 febbraio 2026

[doc. web n. 10221611]

Provvedimento del 29 gennaio 2026

Registro dei provvedimenti
n. 35 del 29 gennaio 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 una segnalazione presentata ai sensi dell'art. 144 del Codice, l'Autorità è stata informata della circostanza che l'Università Telematica e-Campus (di seguito, l'"Ateneo"), nell'ambito di un

corso per l'abilitazione all'insegnamento, svoltosi ai sensi dell'art. 13 del d.P.C.M. del 4 agosto 2023, avrebbe utilizzato un sistema di riconoscimento facciale per identificare i partecipanti a detto corso e verificare l'effettiva e continuativa frequenza allo stesso, chiedendo agli interessati di prestare un consenso al trattamento dei dati personali, peraltro prospettato come obbligatorio ai fini della possibilità di seguire il corso e conseguire il titolo.

2. L'attività istruttoria.

In riscontro a una richiesta d'informazioni dell'Autorità (v. nota prot. n. 0067244 del 30 giugno 2024), l'Ateneo, con nota del 24 giugno 2024, ha dichiarato, in particolare, che:

> "l'art. 2-ter, comma 4 […] del D.lgs. 13 aprile 2017 n. 59 […] prevede [le modalità per l'acquisizione dei crediti formativi necessari all'abilitazione all'insegnamento] […] I percorsi […] possono essere svolti anche mediante modalità telematiche […] esclusivamente presso i Centri che organizzano e impartiscono percorsi accreditati […]";
>
> "ai sensi dell'art. 13 DPCM [4 agosto 2023], i centri stabiliscono i contenuti dei corsi per l'ottenimento dei 30 CFU ([…] comma 2 […]) e possono organizzarli anche con modalità telematiche, comunque sincrone ([…] comma 3 […]), come esplicitamente previsto dall'art. 2-ter, comma 4 del D.lgs. 59/2017";
>
> "nel rispetto di quanto previsto dall'art. 4, comma 6 [del predetto] DPCM, l'Agenzia Nazionale di Valutazione del sistema Universitario e della Ricerca ("ANVUR") ha adottato con delibera n. 231 del 26 settembre 2023 le "Linee guida per la valutazione dei requisiti di accreditamento iniziale dei percorsi di formazione per insegnanti per gli anni accademici 2023/24 e 2024/2025" […, che] prevedono la necessità di adottare, in caso di didattica a distanza, una modalità di verifica degli accessi degli studenti in modo che ne sia accertata l'effettiva partecipazione (pag. 5 […])";
>
> "in qualità di "centro" autorizzato all'erogazione dei percorsi di formazione in gestione […], l'Ateneo ha previsto, a partire dal 9 marzo 2024, l'erogazione di corsi tramite webinar svolti in modalità sincrona";
>
> "nella primissima fase del corso, la verifica della presenza degli studenti era effettuata tramite l'invio a questi ultimi di un pop-up tramite il quale confermare la propria presenza; questo sistema, tuttavia, non era in grado di garantire la verifica certificata dell'effettiva partecipazione alle lezioni da parte degli studenti richiesta dalle Linee Guida";
>
> "a partire dal 3 aprile 2024, l'Ateneo ha quindi adottato un sistema di verifica dell'identità degli studenti in grado di verificare con certezza l'effettiva partecipazione degli studenti alle lezioni considerando le seguenti circostanze: il numero dei partecipanti a ogni lezione, in media 400/500 per aula […]; b) la necessita di garantire un controllo certificato dell'identità liberamente accessibile a chiunque […]";
>
> "a fronte dell'impossibilita di procedere alla verifica certificata delle presenze degli studenti […] con modalità alternative, […] eCampus ha deciso di avvalersi del sistema di riconoscimento dell'identità e di verifica biometrica della presenza offerto da [un'azienda fornitrice]; questo sistema è integrato tramite API nel sistema di videoconferenza professionale […] utilizzato dall'Ateneo per lo svolgimento dei webinar in modalità sincrona";
>
> "la base giuridica del trattamento è il consenso degli studenti ai sensi dell'art. 9, par. 2, lett. a) [del Regolamento]";
>
> "[…] il consenso in questione, oltre a stimolare una consapevolezza degli utenti senz'altro superiore rispetto alle basi giuridiche dell'interesse pubblico o della legge, [è] anche libero in

quanto, in caso di rifiuto, gli studenti possono accedere a uno dei molti corsi per l'ottenimento dei 30 CFU tenuto da altri centri in presenza";

"i dati personali trattati attraverso il sistema di riconoscimento dell'identità tramite verifica biometrica […] sono i seguenti: a) dati di identificazione dell'utente: numero di identificazione dello studente; b) dati relativi all'accesso e all'uso dell'applicazione: orari di accesso e uscita dalle lezioni online; c) documento di riconoscimento e immagine facciale dello studente […] raccolti in fase di registrazione e successivamente nella fase di verifica";

"il sistema di riconoscimento dell'identità tramite verifica biometrica [prevede la] registrazione dello studente [, il quale] scatta la foto del proprio volto e del proprio documento di identità [… che vengono] trasmess[i] al server […] per [poi] creare un modello biometrico [anch'esso] memorizzato […] per consentire la successiva verifica […] della presenza dello studente durante la lezione tramite riconoscimento biometrico [; tale verifica] viene avviata dal docente […] durante la lezione [; in tal caso] viene chiesto allo studente di scattarsi una foto tramite la webcam del proprio dispositivo [e] il sistema […] verifica la corrispondenza biometrica […con l'] immagine dello stesso acquisita nella fase di registrazione; […] in caso di esito positivo […] la lezione prosegue [, mentre] in caso di esito negativo […], l'Ateneo [può] effettuare ulteriori verifiche […]";

"l'informativa privacy ai sensi dell'art. 13 [del Regolamento] di eCampus viene fornita agli studenti - che sono tenuti a prenderne visione - prima dell'avvio della fase di registrazione";

"i dati degli studenti utilizzati per il riconoscimento dell'identità e la verifica biometrica della presenza degli studenti sono conservati per il periodo necessario all'assolvimento delle operazioni di elaborazione, identificazione, validazione della presenza e comunque non oltre 12 mesi dal momento dell'acquisizione [tenuto conto che…] il corso dura in media 5/6 mesi […] e [che] i dati vengono conservati per ulteriori 6 mesi per garantire la gestione delle richieste degli studenti e/o di eventuali contestazioni […]";

"dalla mancata corrispondenza tra le due immagini discende un'unica conseguenza, vale a dire il non riconoscimento dell'identità della persona e quindi, in ragione di ciò, della sua presenza";

"in caso, invece, di errori nel processo di autenticazione, questo può essere ripetuto, fermo [restando] che in caso di persistenti errori l'interessato può comunque chiedere che venga effettuata una verifica personale";

"l'Ateneo non ha rinvenuto alcun rischio elevato per i diritti le libertà delle persone e non ha quindi ritenuto necessario riversare le considerazioni sopra illustrate all'interno di un documento ulteriore, ossia di una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 [del Regolamento]".

Con una successiva nota del 29 luglio 2024, l'Ateneo ha integrato e precisato il proprio riscontro, dichiarando, in particolare, che:

"nel corso di ciascuna lezione il docente è tenuto a verificare la presenza degli studenti. Il docente può avviare la verifica in qualsiasi momento della lezione e può farlo anche più volte durante lo svolgimento della stessa […]";

"al termine della verifica, il docente non viene messo a conoscenza di alcuna informazione sull'esito della verifica (positivo o negativo) della presenza dello studente, che viene trasmessa esclusivamente a eCampus";

"eCampus ha deciso di adottare nuove regole per la conservazione dei dati raccolti tramite il

sistema […], prevedendo un regime diverso per la verifica della presenza certificata durante la lezione";

"[…] l'Ateneo sta predisponendo una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 [del Regolamento]".

In riscontro a una seconda richiesta d'informazioni dell'Autorità (v. nota prot. n. 0139142 del 26 novembre 2024), l'Ateneo, con nota del 16 dicembre 2024, nel ribadire quanto già rappresentato con la predetta nota del 29 luglio 2024, ha precisato che "l'Ateneo non conserva dati biometrici, che vengono invece eliminati subito dopo la loro generazione e il confronto tra i Modelli Biometrici 1 e 2 durante la fase di verifica certificata della presenza dello studente nel corso della lezione tramite riconoscimento biometrico. Al contrario, l'Ateneo conserva solo il Dataset Grezzo 1, rappresentato dalla fotografia del volto dello studente e l'immagine del documento di identità dello stesso".

L'Ateneo ha, inoltre, prodotto in atti "la [valutazione di impatto sulla protezione dei dati] relativa al trattamento dei dati degli studenti effettuato dall'Ateneo tramite il sistema […] per la verifica certificata della partecipazione degli stessi alle lezioni online effettuate in modalità sincrona".

A fronte di un'ultima richiesta d'informazioni formulata dall'Autorità (v. nota prot. n. 0049433 del 10 aprile 2024), l'Ateneo, con nota del 20 maggio 2025 inviata dal proprio avvocato, ha dichiarato, in particolare, che:

"il sistema di riconoscimento [oggetto di istruttoria] è stato utilizzato nelle prime due edizioni e nella terza solo parzialmente. Al momento della richiesta di maggiori informazioni [formulata dall'Autorità] in data 26/11/2024, infatti, il sistema di riconoscimento era stato sospeso per tornare alla modalità di identificazione c.d. pop-up";

successivamente, il procedimento è stato modificato prevedendo una "fase di registrazione dello studente, […] nei giorni precedenti all'inizio del corso, [in cui] viene raccolto il Dataset Grezzo 1 [, ossia "la fotografia […] scattata dallo [studente]; [e] l'immagine del documento di riconoscimento […senza] alcun modello […]. Il Dataset Grezzo 1 viene […] cancellato al termine delle lezioni […; dopodiché si effettua la] verifica […] della presenza dello studente nel corso della lezione tramite riconoscimento biometrico [; il docente avvia la verifica […] della presenza [… e il] sistema […] raccoglie un nuovo dato grezzo [, ovvero la] fotografia scattata dallo studente durante la verifica ("Dataset Grezzo 2") [per il] confronto con il Dataset Grezzo 1. La sequenza delle operazioni […] è la seguente: i) viene creato il Modello Biometrico 1 basato sul Dataset Grezzo 1; ii) viene creato il Modello Biometrico 2 basato sull'immagine della webcam (Dataset Grezzo 2) […;] il software compara il Modello […] 2 con il Modello […] 1 per certificare la presenza dello studente e: in caso di esito positivo […], il Dataset Grezzo 2 e Modelli […] 1 e 2 vengono cancellati[;] in caso di esito negativo […], i Modelli […] 1 e 2 vengono cancellati, mentre il Dataset Grezzo 2, […] modificato […] con l'apposizione di una filigrana in modo da non poter riottenere un nuovo modello biometrico, sarà conservato fino alla convocazione alla prova orale […, allorquando] il Dataset Grezzo 2 viene cancellato […]";

"[…] le immagini del c.d. Dataset Grezzo 1 sono conservate con modalità tali da non rientrare entro la nozione di dato biometrico, poiché durante il periodo di conservazione successivo all'enrolment-registrazione e sino al momento della verifica della presenza dello studente nel corso delle lezioni, tali dati personali non vengono trattati "attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica" (considerando n. 51 del [Regolamento])".

Con nota del 15 settembre 2025 (prot. n. 0120479), l'Ufficio, sulla base degli elementi acquisiti,

dalle verifiche compiute e dei fatti emersi a seguito dell'attività istruttoria, ha notificato all'Ateneo, 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 posto in essere un trattamento di dati personali biometrici in violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 9, par. 1, lett. g), 25 e 35 del Regolamento, nonché 2-ter e 2-sexies del Codice. 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 15 ottobre 2025 (prot. del Garante n. 0136542/25 della medesima data), l'Ateneo, per il tramite del proprio avvocato, ha presentato una memoria difensiva, con la quale, riprendendo argomenti già in precedenza esposti, ha dichiarato, in particolare, che:

> "[preso] atto che il trattamento posto in essere dall'Ateneo rientri a ragione nell'ambito dello svolgimento di un compito di interesse pubblico [, …] l'Ateneo si impegna - nell'ipotesi di reimpiego di rinnovati sistemi di identificazione simili a quelli oggetto di istruttoria e il cui impiego è da tempo stato interrotto - a mutare [coerentemente] le basi giuridiche per il trattamento dei dati biometrici […]";
>
> "in considerazione della tipologia di corso oggetto di disamina […] e della possibilità per i partecipanti di assentarsi volontariamente dalle lezioni tenute a distanza, la conservazione dei dati relativi all'esito negativo della verifica sino alla prova finale nel periodo di utilizzo di tale sistema [è] da ritenersi proporzionata in relazione al numero potenziale di partecipanti alle predette attività formative in rapporto al numero dei docenti […] e, ancora, conforme ai principi di minimizzazione, poiché idonea a fornire tempestivamente la prova legale, su richiesta del partecipante, del numero di assenze maturate ai fini dell'ammissione all'esame orale finale";
>
> "la durata media di tali corsi (e dunque anche il periodo di conservazione dei dati) è stato [comunque] sempre inferiore ai cinque mesi";
>
> "dopo la data dell'11 novembre 2024 non è stata posta in essere alcuna ulteriore attività di trattamento identica o ancora simile a quelle oggetto di istruttoria".

3. Esito dell'attività istruttoria.

3.1 I presupposti di liceità dei trattamenti di dati personali in ambito universitario.

In via preliminare, deve osservarsi che la libertà di insegnamento (cfr. artt. 33 Cost. e 1 della l. 30 dicembre 2010, n. 240), anche a livello universitario, può essere esercitata da soggetti pubblici o privati, indipendentemente dalla forma giuridica degli stessi (enti pubblici, fondazioni, società di capitali). La normativa vigente, infatti, non prevede espressamente quale sia la natura giuridica delle università non statali (o anche "università libere" o "università private"), limitandosi a disciplinarne singoli aspetti di analogia o differenza rispetto a quanto disposto per le università statali. Tra i profili di analogia rispetto alla disciplina delle università statali (pubbliche), ricorre, anzitutto, il perseguimento di finalità di interesse pubblico (cfr. art. 1, co. 1, della l. 30 dicembre 2010, n. 240, riferito sia alle università statali sia alle università non statali).

Considerato che il quadro normativo in materia di protezione dei dati personali non prevede un diverso regime applicabile ai soggetti pubblici e a quelli privati e tiene conto del solo profilo funzionale nel trattamento dei dati, si ritiene che, stante il perseguimento di un medesimo interesse pubblico, da parte delle università pubbliche e private, i relativi trattamenti di dati personali siano leciti se necessari "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" o "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di

pubblici poteri" (art. 6, par. 1, lett. c) ed e), e, con riguardo alle categorie particolari di dati, art. 9, lett. g), del Regolamento).

Per tali ragioni, contrariamente a quanto sostenuto dall'Ateneo, i trattamenti dei dati biometrici dei partecipanti ai corsi per l'ottenimento dei crediti formativi necessari all'abilitazione all'insegnamento non possano trovare fondamento in altre basi giuridiche e, in particolare, nel consenso degli interessati (art. 6, par. 1, lett. a), del Regolamento e, con riguardo alle categorie particolari di dati, art. 9, lett. a), del Regolamento; cfr. provv. 16 settembre 2021, n. 317, doc. web n. 9703988, spec. par. 3.1, confermato da Cass. civ., Sez. I, n. 12967 del 13 maggio 2024 e, da ultimo, Tribunale di Milano, n. 8872 del 19 novembre 2025).

3.2. Il trattamento dei dati personali biometrici dei partecipanti al corso.

Sulla base di quanto è emerso a seguito dell'istruttoria, risulta accertato che l'Ateneo ha posto in essere un trattamento di dati personali, relativi alle caratteristiche biometriche del volto dei partecipanti a un corso per l'abilitazione all'insegnamento, svoltosi ai sensi dell'art. 13 del d.P.C.M. 4 agosto 2023.

Tale trattamento è stato posto in essere da marzo a luglio 2024, prima con le modalità illustrate nella citata nota del 24 giugno 2024 e poi con quelle di cui alla nota del 29 luglio 2024. Dal 23 settembre 2024, il sistema di riconoscimento biometrico è rimasto "parzialmente in uso" e il suo impiego è definitivamente cessato in data 11 novembre 2024 (v. la tabella riportata nella nota dell'Ateneo del 20 maggio 2025).

In via generale, deve rammentarsi che il rafforzamento delle tutele dei dati biometrici previste dal Regolamento e dal Codice, come modificato dal d.lgs. n. 101/2018 - in ragione della loro delicatezza, derivante dalla stretta e stabile relazione con l'individuo e la sua identità - mediante l'inclusione degli stessi nelle categorie di dati particolari e, al pari dei dati sulla salute e genetici, tra quelle assistite da un più elevato livello di garanzie (art. 9, par. 1, 2 e 4, del Regolamento; l'art. 2-septies del Codice), ha riguardato anzitutto i presupposti giuridici che rendono leciti i trattamenti di tali categorie di dati (cfr. il citato provv. 16 settembre 2021, n. 317, par. 3.4; v. anche, tra i numerosi provvedimenti in materia, provv. 14 gennaio 2021, n. 16, doc. web n. 9542071). In tale quadro il trattamento dei dati biometrici è di regola vietato, salvo che sussista una delle condizioni di cui all'art. 9 del Regolamento "ed in conformità alle misure di garanzia disposte dal Garante".

Nel caso di specie, l'Ateneo non ha indicato alcuna idonea disposizione normativa che espressamente prevedesse e disciplinasse il trattamento di dati biometrici in questione (cfr. artt. 6, par. 1, lett. c) e d), e parr. 2 e 3, 9, par. 1, lett. g), del Regolamento, nonché 2-ter e 2-sexies del Codice).

L'Ateneo ha, infatti, invocato esclusivamente talune linee guida predisposte dall'ANVUR in materia di accreditamento dei percorsi di formazione per gli insegnanti, che non possono considerarsi idonee, né per rango né per qualità, a costituire la base giuridica di un trattamento di dati personali biometrici come quello in esame, limitandosi, peraltro, le stesse genericamente a prevedere, "relativamente alla didattica a distanza […, la necessità che sia] indicata la modalità di verifica degli accessi degli studenti, in modo che ne sia accertata l'effettiva partecipazione alle lezioni", nonché che siano indicate "le modalità che l'istituzione intende adottare per la gestione della partecipazione degli studenti alle prove d'esame e il controllo del loro svolgimento", senza alcun riferimento a modalità di accertamento dell'identità dei partecipanti ai corsi basate su strumenti di riconoscimento biometrico.

Né, per le ragioni illustrate al precedente par. 3.1, detto trattamento poteva fondarsi sul consenso reso dagli interessati. Peraltro, detto consenso non equivale comunque a una "manifestazione di volontà libera […] dell'interessato" (art. 4, par. 1, n. 11), del Regolamento), atteso che, in caso di

mancato consenso, agli interessati sarebbe stata del tutto negata la possibilità di partecipare al corso di abilitazione e conseguire il relativo titolo, dovendosi, a tal riguardo, evidenziare che, come previsto dall'art. 7, par. 4, del Regolamento, "nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto" (cfr. l'informativa sul trattamento dei dati personali resa dall'Ateneo ai partecipanti al corso, sub all. 3 alla nota del 24 giugno 2024, ove si legge che "il mancato consenso al trattamento non permetterà la partecipazione alle lezioni dei percorsi formativi abilitanti 30 CFU ex art. 13"). Non rileva, a tal riguardo, che, come sostenuto dall'Ateneo, "il consenso [… è] libero in quanto, in caso di rifiuto, gli studenti possono accedere a uno dei molti corsi per l'ottenimento dei 30 CFU tenuto da altri centri in presenza" (nota del 24 giugno 2024). Come, infatti, chiarito anche dal Comitato europeo per la protezione dei dati "il consenso non [può] considerarsi prestato liberamente se il titolare del trattamento sostiene che esiste la possibilità di scegliere tra il suo servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente offerto da un altro titolare del trattamento", poiché "in tal caso la libertà di scelta dipenderebbe dagli altri operatori del mercato e dal fatto che l'interessato ritenga che i servizi offerti dall'altro titolare del trattamento siano effettivamente equivalenti" ("Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679", adottate il 4 maggio 2020, par. 38).

La libertà del consenso chiesto ai partecipanti è poi ulteriormente viziata dalla circostanza che, allorquando, come nel caso di specie, il titolare del trattamento è chiamato a perseguire una finalità d'interesse pubblico, connessa ad attività formative - che, come detto, già trovano la propria legittimazione nella pertinente cornice giuridica di settore - sussiste un evidente squilibrio tra l'interessato e il titolare del trattamento, che rende improbabile che il consenso sia espresso liberamente (v. cons. 43 del Regolamento; cfr. le citate, par. 16, ove si evidenzia come, in tali circostanze, "esistano altre basi legittime, in linea di principio più appropriate, per il trattamento da parte delle autorità pubbliche").

Pertanto, come già precisato al precedente par. 3.1, considerato che il trattamento è stato effettuato dall'Ateneo ai fini dello svolgimento di un corso abilitante riconosciuto dalla legge, e dunque nello svolgimento di un compito di interesse pubblico, il consenso non poteva costituire, nel contesto in questione, la base giuridica del trattamento, sussistendo nella relazione con i frequentanti i corsi anche una situazione di evidente squilibrio (cfr. il citato provv. 16 settembre 2021, n. 317, par. 3.4).

Alla luce delle considerazioni che precedono, deve concludersi che l'Ateneo ha posto in essere un trattamento di dati personali biometrici in maniera non conforme al principio di "liceità, correttezza e trasparenza" e in assenza di base giuridica, in violazione degli artt. 6, par. 1, lett. c) ed e), e parr. 2 e 3, 9, par. 1, lett. g), del Regolamento, nonché 2-ter e 2-sexies del Codice.

3.3 La violazione dei principi di minimizzazione, limitazione della conservazione e protezione dei dati fin dalla progettazione e per impostazione predefinita.

Sotto il profilo del rispetto dei principi di minimizzazione, limitazione della conservazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita (v. artt. 5, par. 1, lett. c) ed e) e 25 del Regolamento), si osserva che nel caso di specie, l'Ateneo, da marzo a luglio 2024, ha conservato i dati personali degli studenti, utilizzati per ai fini del riconoscimento biometrico, per un periodo di dodici mesi dalla loro acquisizione.

Impregiudicate le valutazioni già svolte in relazione alla carenza di un presupposto legittimante il trattamento di tali dati, occorre osservare che, alla luce delle finalità di trattamento effettivamente perseguite e del contesto in cui ha avuto luogo il trattamento, tale esteso periodo di conservazione dei dati non può comunque considerarsi proporzionato e giustificato.

In generale, il riconoscimento biometrico poteva, infatti, avere esito positivo o negativo. Nel primo caso (vale a dire ove il sistema di riconoscimento biometrico avesse confermato l'identità del partecipante), non vi sarebbe stata alcuna ragione per conservare i dati personali dell'interessato dopo la cessazione del corso o dell'esame in questione; nel secondo caso (vale a dire allorquando il sistema di riconoscimento biometrico non avesse confermato l'identità del partecipante), l'accertamento dell'identità dello studente, come dichiarato dall'Ateneo, sarebbe stato comunque effettuata con modalità tradizionali (riconoscimento de visu) e, pertanto, non sarebbe stato comunque necessario continuare a conservare i dati personali raccolti e utilizzati ai fini del riconoscimento biometrico per un così esteso arco temporale.

Le medesime considerazioni valgono, altresì, in relazione alla diversa modalità di riconoscimento biometrico impiegata dall'Ateneo a partire dalla fine di luglio 2024, nell'ambito della quale è stato comunque conservato il c.d. "Dataset Grezzo 2" (vale a dire la fotografia scattata dal sistema allo studente quando il docente decideva di avviare la verifica della presenza durante la lezione) fino alla data della prova orale, essendo stato tale Dataset "cancellato subito dopo la prova orale o la mancata ammissione alla stessa". Ciò come "evidenza della non partecipazione alla lezione o della presenza di una persona diversa dallo studente previamente registrato", fermo restando che "sul Dataset Grezzo 2 [è stata] apposta una filigrana digitale volta a impedire la possibilità di tentare di creare un nuovo modello biometrico su quel dato grezzo". Anche in tale caso, infatti, l'Ateneo, a fronte del mancato riconoscimento biometrico, avrebbe potuto ricorrere tempestivamente al riconoscimento de visu dell'interessato, senza attendere la data della prova orale.

Alla luce delle considerazioni che precedono, il trattamento posto in essere risulta, anche con riguardo ai predetti profili, in contrasto con la disciplina di protezione dei dati, in quanto non conforme ai principi di "minimizzazione", "limitazione della conservazione" e "protezione dei dati per impostazione predefinita", in violazione degli artt. 5, par. 1, lett. c) ed e), e 25 del Regolamento.

3.4 La valutazione di impatto sulla protezione dei dati.

In relazione allo svolgimento di una valutazione di impatto ai sensi dell'art. 35 del Regolamento, si osserva che le "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" (WP 248) adottate dal Gruppo di lavoro art. 29 il 4 aprile 2017, fatte proprie dal Comitato europeo per la protezione dei dati con "Endorsement 1/2018" del 25 maggio 2018, individuano, tra i criteri in presenza dei quali il titolare del trattamento è tenuto ad effettuare una valutazione di impatto, rilevanti nel caso di specie, il trattamento di "dati sensibili", tra i quali sono compresi i dati biometrici (v. cap. III, B, n. 4), nonché i trattamenti che realizzano un "uso innovativo o [l']applicazione di nuove soluzioni tecnologiche od organizzative" (v. cap. III, B, n. 8) (cfr. il "Parere 11/2024 sull'uso del riconoscimento facciale per snellire il flusso dei passeggeri negli aeroporti", del 23 maggio 2024, con il quale il Comitato europeo per la protezione dei dati ha "ricorda[to] che l'uso dei dati biometrici e in particolare della tecnologia di riconoscimento facciale comporta maggiori rischi per i diritti e le libertà degli interessati", con la conseguenza che "prima di utilizzare tali tecnologie, anche se dovessero essere ritenute particolarmente efficaci, i titolari del trattamento dovrebbero valutare l'impatto sui diritti e sulle libertà fondamentali degli interessati e considerare se mezzi meno invasivi possano raggiungere la finalità legittima del rispettivo trattamento" - par. 26).

La valutazione di impatto è, in ogni caso, necessaria in caso di "[…] trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 […]" (art. 35, par. 1, par. 3, lett. b), del Regolamento), dovendosi, a tal riguardo, considerare che, nel caso di specie, il trattamento dei dati biometrici ha riguardato un elevato numero di interessati (si vedano le dichiarazioni rese nel corso dell'istruttoria in relazione al "numero dei partecipanti a ogni lezione, in

media 400/500 per aula"), sussistendo, pertanto, nel contesto in questione, l'obbligo di svolgere una valutazione di impatto sulla protezione dei dati, ai sensi dell'art. 35 del Regolamento, prima di dare avvio al trattamento.

Dall'istruttoria è, invece, emerso che l'Ateneo "non ha rinvenuto alcun rischio elevato per i diritti le libertà delle persone e non ha quindi ritenuto necessario riversare le considerazioni sopra illustrate all'interno di un documento ulteriore, ossia di una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 [del Regolamento]" (nota del 24 giugno 2024).

Soltanto nel corso dell'istruttoria, con la nota del 16 dicembre 2024, l'Ateneo ha prodotto in atti copia di una valutazione di impatto sulla protezione dei dati. Si tratta, tuttavia, di un foglio di calcolo elettronico, privo sia di data certa sia di sottoscrizione da parte del legale rappresentante del titolare del trattamento o di altro soggetto da questo autorizzato, non essendo, pertanto, tale documento idoneo a comprovare l'assolvimento dell'obbligo previsto dall'art. 35 del Regolamento in data anteriore a quella in cui il trattamento è definitivamente cessato, vale a dire in data 11 novembre 2024 (cfr. provv.ti 10 aprile 2025, n. 232, doc. web n. 10127930; 10 aprile 2025, n. 202, doc. web n. 10140338; 12 dicembre 2024, n. 766, doc. web n. 10102334; 11 gennaio 2024, n. 5, doc. web n. 9977020).

Deve, pertanto, concludersi che l'Ateneo ha agito 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'Ateneo, per aver posto in essere un trattamento di dati personali biometrici in violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 9, par. 1, lett. g), 25 e 35 del Regolamento, nonché 2-ter e 2-sexies del Codice.

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), c) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 9, par. 1, lett. g), del Regolamento, nonché 2-ter e 2-sexies 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 l'Ateneo ha dichiarato di aver cessato di impiegare il sistema di riconoscimento biometrico in questione e che è oramai decorso il periodo massimo di conservazione dei dati (quantificato dal titolare in cinque mesi) - 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 la violazione abbia carattere colposo, essendo l'Ateneo incorso in un errore in diritto in merito alla base giuridica applicabile al trattamento (cfr. art. 83, par. 2, lett. b), del Regolamento), e lo stesso non abbia interessato l'intera popolazione studentesca, bensì soltanto i partecipanti al predetto corso per l'abilitazione all'insegnamento (cfr. art. 83, par. 2, lett. a), del Regolamento) - il trattamento ha riguardato dati particolari appartenenti alle categorie particolari di cui all'art. 9 del Regolamento, rispetto ai quali il quadro normativo in materia di protezione dei dati personali prevede un livello più alto di tutela (cfr. art. 83, par. 2, lett. g), del Regolamento), nonché considerato che il trattamento si è protratto per un discreto arco temporale, ovvero da marzo a novembre 2024 (cfr. art. 83, par. 2, lett. a), del Regolamento), si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia alto (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'università telematica di notevoli dimensioni (49.856 studenti iscritti nell'a.a. 2024/2025, secondo i dati pubblicati dal Ministero dell'Università e della Ricerca), si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

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

- l'Ateneo ha offerto una buona cooperazione con l'Autorità, avendo, peraltro, spontaneamente, nel corso dell'istruttoria, prima modificato le modalità del trattamento dei dati e poi posto fine allo stesso (cfr. art. 83, par. 2, lett. f), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 50.000 (cinquantamila) per la violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 9, par. 1, lett. g), 25 e 35 del Regolamento, nonché 2-ter e 2-sexies 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 della particolare delicatezza dei dati trattati.

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'Università Telematica e-Campus per la violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 9, par. 1, lett. g), 25 e 35 del Regolamento, nonché 2-ter e 2-sexies del Codice, nei termini di cui in motivazione;

ORDINA

all'Università Telematica e-Campus, in persona del legale rappresentante pro-tempore, con sede legale in Via Isimbardi, 10 - 22060 Novedrate (CO), C.F. 90027520130, di pagare la somma di euro 50.000 (cinquantamila) 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 Ateneo, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 50.000 (cinquantamila) 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, 29 gennaio 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Montuori