Civile Ord. Sez. 1 Num. 12967 Anno 2024
Presidente: GENOVESE FRANCESCO ANTONIO
Relatore: TRICOMI LAURA
Data pubblicazione: 13/05/2024

ORDINANZA

sul ricorso iscritto al n. 801/2023 R.G. proposto da:

GARANTE PROTEZIONE DATI PERSONALI - PRIVACY, in persona del legale rapp. p.t., domiciliato in ROMA VIA DEI PORTOGHESI, presso l'AVVOCATURA GENERALE DELLO STATO che lo rappresenta e difende *ope legis.*

-ricorrente-

contro

UNIVERSITA' COMMERCIALE LUIGI BOCCONI, in persona del legale rapp.p.t., rappresentata e difesa, anche disgiuntamente dagli avvocati Fabio Lepri, Stefano Previti, Enrico Del Guerra e Alessandra Grandoni, ed elettivamente domiciliata presso il secondo in Roma, via Cicerone n. 60, in forza di procura speciale alle liti in atti.

-controricorrente-

avverso la SENTENZA del TRIBUNALE di MILANO n. 8174/2022 depositata il 20/10/2022.

Udita la relazione svolta nella camera di consiglio del 01/02/2024 dal Consigliere LAURA TRICOMI.

RILEVATO CHE:

1.1.- Con la sentenza impugnata, il Tribunale di Milano ha parzialmente accolto il ricorso proposto dalla Università commerciale Luigi Bocconi di Milano avverso il provvedimento n. 317 del 16 settembre 2021, adottato ai sensi degli artt. 78 Reg (UE) 2016/679 (d'ora in avanti anche, "Regolamento"), 152 del d.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali, d'ora in avanti anche, "Codice") e 10 del d.lgs. n. 150/2011, con il quale il Garante per la protezione dei dati personali (di seguito, il Garante), nel rilevare che un trattamento di dati biometrici effettuato dalla ricorrente violava gli artt. 5, par. 1, lett. a), c) ed e), 6, 9, 13, 25, 35, 44 e 46, del Regolamento, nonché 2-*sexies* del Codice, aveva disposto, nei confronti dell'Università, prescrizioni atte a conformare il trattamento al regolamento, ai sensi dell'articolo 58, par. 2, lett. d), del medesimo testo e aveva inflitto allo stesso ente la sanzione amministrativa pecuniaria di euro 200.000,00=, nonché quella accessoria della pubblicazione del provvedimento medesimo sul sito web del Garante (v. artt. 58, par. 2, lett. i, e 83, par. 5, del Regolamento e 166, commi 2 e 7, del Codice).

1.2.- Il provvedimento opposto era stato adottato dal Garante all'esito di una attività di controllo svolta a seguito del reclamo di uno studente concernente l'impiego di un sistema di supervisione "*proctoring*", nell'ambito dello svolgimento delle prove scritte d'esame degli studenti, al fine di identificare questi ultimi e/o di verificarne il corretto comportamento durante lo svolgimento della prova d'esame in video conferenza.

Come si evince dalla sentenza impugnata, l'Università Bocconi, nell'aprile 2020, stante la necessità – a seguito dell'emergenza pandemica - di svolgere gli esami speciali con il sistema della video conferenza, ma in modo da garantirne la serietà, aveva deciso di dotarsi di un *software* (denominato "Respondus") fornito dalla società *Respondus Inc.* (con sede in USA), idoneo a consentire di verificare la genuinità della prova e limitando al massimo i rischi di alterazione della medesima; un *software* del cui utilizzo gli studenti erano stati informati attraverso comunicazioni relative alle nuove modalità di svolgimento delle prove d'esame.

A seguito dell'attività di controllo, svolta in contraddittorio con l'Ateneo, il Garante, tra l'altro, aveva riscontrato e contestato diverse violazioni del Regolamento: articoli 5, par. 1, lett. a), c) ed e) (principi di liceità, correttezza e trasparenza, principio di minimizzazione del trattamento e principio di limitazione della conservazione); 13 (informativa); 25 (*privacy by design e by default*); 35 (valutazione di impatto sulla protezione dei dati); 44 (principio generale per il trasferimento); 46 (trasferimento soggetto a garanzie adeguate). Nonché dell'art. 2-*sexies* (trattamento di categorie particolari di dati personali, necessario per motivi di interesse pubblico rilevante) del Codice.

1.3.- Con la decisione in epigrafe indicata, il Tribunale ha affermato che non costituiva oggetto di discussione tra le parti il meccanismo di funzionamento del *software* "Respondus", descritto in sentenza come un *software* che: «cattura le immagini video e lo schermo dello studente identificando e contrassegnando con un flag i momenti in cui sono rilevati comportamenti insoliti e/o sospetti mediante registrazione video e istantanee scattate a intervalli casuali per tenere traccia di comportamenti anomali… Al termine della prova, il sistema elabora il video, inserendo segnali di allerta in merito a possibili indici di comportamenti scorretti …

affinché il docente … possa poi valutare se effettivamente sia stata commessa un'azione non consentita nel corso della prova» (fol.12).

Ha, quindi, escluso che, nella fattispecie in esame, potesse trovare applicazione l'art.9 del regolamento 679/2016, come invece ritenuto dal Garante, osservando che il regime ivi delineato è applicabile unicamente al trattamento di dati biometrici «intesi a identificare in modo univoco una persona fisica»; che il trattamento di dati biometrici per finalità identificative si riferisce al riconoscimento automatico di persone fisiche basato su una rappresentazione analogica o digitale di una caratteristica biometrica ottenuta al termine di un processo di acquisizione; che non ricorreva un trattamento di dati biometrici secondo il ciclo di vita dei dati biometrici, costituito dalla sequenza in quattro fasi — secondo la Descrizione accreditata dal Garante per la protezione dei dati personali, Linee Guida in materia di riconoscimento biometrico e firma grafometrica, 12 novembre 2014 — seguenti: Prima fase o rilevamento tramite sensori specializzati (ad es. scanner per il rilevamento dell'impronta digitale) o dispositivi di uso generale (ad es. videocamera) di caratteristiche biometriche (ad es. viso dell'individuo); Seconda fase, secondo cui, a seguito del rilevamento si acquisisce un campione biometrico (ad es. immagine del viso); Terza fase, quella per cui dal campione biometrico vengono estratti tratti biometrici (ad es. specifici punti del viso) idonei a costituire il modello biometrico che sarà conservato in una banca dati; Quarta fase, cd. del confronto (o di *match*), ove il modello biometrico viene confrontato con le effettive caratteristiche dell'individuo e il confronto in parola consente la identificazione univoca della persona fisica.

In particolare, il Tribunale ha affermato che la mera acquisizione di una foto (o di una registrazione video) non configura un trattamento di dati biometrici, bensì di dati comuni; di contro, il trattamento in parola implica ricavare - da una foto o da

un video - caratteristiche biologiche per derivarne un modello matematico del volto del soggetto ritratto, a fini di riconoscimento dello stesso e che, nel caso in esame, non era configurabile il trattamento di dati biometrici perché tale finalità non era contemplata nel meccanismo attuato dal *software Respondus*, giacché ogni eventuale valutazione era lasciata al docente e non vi era alcuna dimostrazione che la quarta fase, precedentemente indicata (cd. del confronto o del *match*), fosse stata concretamente attuata.

Ha, quindi, ritenuto applicabile la disciplina prevista per i dati personali comuni, *ex* art. 6 del reg. 679/2016, e proceduto alla disamina della fattispecie in relazione ad esso.

1.4.- Sotto altro profilo, in punto di trasferimento internazionale dei dati personali, il Tribunale ha affermato che l'Accordo di modifica sottoscritto tra l'Università e la società fornitrice *Respondus*, in data 18 agosto 2020, fosse tale da impedire il trasferimento internazionale di dati personali. Ciò in quanto, all'accordo di modifica, erano state allegate le clausole tipo (di cui alla Decisione della Commissione europea del 5 febbraio 2010 n. 87/UE). Tale allegato si compone di due appendici: la prima, descrive il tipo di trattamento; la seconda, indica le misure tecniche e organizzative implementate dalla società *Respondus* e da *Amazon*. Il Tribunale ha ritenuto corrette le clausole allegate – seppure mediante semplice rinvio – sia sul piano formale che su quello sostanziale, ritenendo che il rispetto delle stesse fosse idoneo a garantire agli interessati una tutela adeguata rispetto agli standard europei. Ha ritenuto che la "pseudonomizzazione" (ossia l'utilizzazione di pseudonimi per denominare i dati acquisiti in relazione a ciascuna persona) costituisse una misura di protezione adeguata.

1.5.- Conclusivamente, il Tribunale, in parziale accoglimento del ricorso, ha confermato il provvedimento n. 317 del 2021 del

Garante per la Protezione dei Dati Personali, limitatamente alla contestazione di cui agli artt. 5 par. 1 lett. a), 13 Reg. 679/2016, riducendo la sanzione irrogata a euro 10.000,00=; ha confermato il provvedimento n. 317 del 2021, pronunciato dal Garante per la protezione dei dati personali, relativamente all'applicazione dell'art. 58 Reg. 679/2016, limitatamente al divieto di trasferimento dei dati personali degli interessati negli Stati Uniti d'America, in assenza di adeguate garanzie informative e all'obbligo di comunicare all'Autorità le iniziative intraprese al fine di dare attuazione a tale aspetto; ha condannato il Garante alla restituzione in favore dell'Università Commerciale Luigi Bocconi della somma di € 190.000,00, oltre agli interessi legali dal 26.10.2021 al saldo.

1.6.- Il Garante per la protezione dei dati personali ha proposto ricorso con tre mezzi, per la cassazione della sentenza del Tribunale di Milano pubblicata il 20 ottobre 2022.

L'Università Commerciale Luigi Bocconi ha replicato con controricorso, assistito da memoria.

È stata disposta la trattazione camerale.

CONSIDERATO CHE:

2.1.- Con il primo motivo si denuncia la violazione e falsa applicazione degli artt. 6 e 9 par. 2, lett. g) regolamento (UE) 2016/679 e dell'art. 2 sexies, comma 2, lett. bb) del d.lgs. n. 196/2003 (art. 360, primo comma, n. 3 c.p.c.).

Il giudice di primo grado ha ritenuto di escludere la configurabilità, nella fattispecie, di un trattamento di dati biometrici, sulla base della considerazione che la finalità di identificazione univoca della persona richiesta dall'art. 9, par. 1, del regolamento UE n. 679/2016 non sarebbe contemplata dal sistema informatico Respondus utilizzato dall'Università ricorrente, in quanto ogni eventuale valutazione sul punto sarebbe lasciata al docente e non vi sarebbe pertanto alcuna dimostrazione che la fase

quattro (del confronto o del *match*), enucleata dalle Linee Guida in materia di riconoscimento biometrico e firma grafometrica adottate dal Garante il 12 novembre 2014, sia stata concretamente attuata.

Secondo il ricorrente, la tesi è errata ed è il frutto di una non corretta interpretazione dell'art. 9 par. 2, lett. g), del Regolamento e dell'art. 2 sexies, comma 2, lett. bb) del Codice, che sono, invece, del tutto applicabili nella specie.

2.2.- Il motivo è fondato e va accolto.

2.3.- Nel diritto dell'Unione Europea, i dati biometrici sono dati personali se sono usati per identificare in modo univoco una persona. Il trattamento di tali dati è regolato da tre diversi atti dell'Unione: 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; la Direttiva 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati; e il Regolamento 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati. Tutti questi atti definiscono allo stesso modo i dati biometrici come *«i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»* (art. 4 n. 14 del Regolamento 2016/679; art. 3 n. 13 della Direttiva 2016/680; art. 3 n. 18 del Regolamento 2018/1725), mentre la

disciplina sul trattamento è diversa in base alla finalità specificamene perseguita.

2.4.- Nel caso in esame, trovano applicazione il Reg (UE) 2016/679 (Regolamento) ed il d.lgs. n. 196/2003 (Codice).

Il Considerando 51 del Regolamento recita: *« Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. (…) Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. (…)»*.

Ferma la definizione di "trattamento" contenuta all'art.4, par.1, n.2 del Regolamento, come *«qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la*

distruzione», l'art. 9, par. 1, par. 2 lett. g) del Regolamento prevede che: *«1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; (…) g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».*

Quindi, l'art. 2-*sexies* del Codice (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante) stabilisce che *«1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. (…) 2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti*

effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: (…) bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;».

2.5.- E' opportuno, inoltre ricordare che nell'art.5, par. 1, del Regolamento, così vengono sinteticamente enucleati i principi a cui si deve complessivamente conformare il trattamento dei dati personali: a) "liceità, correttezza e trasparenza"; b) "limitazione della finalità"; c) "minimizzazione dei dati"; d) "esattezza"; e) "limitazione della conservazione"; f) "integrità e riservatezza" e che, sempre, nell'art.5, par. 2, del regolamento 2016/679, è stato introdotto espressamente il principio di responsabilizzazione ("*accountability*", nella versione in lingua inglese) con la precisazione che *«Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")»*.

Il principio di "responsabilizzazione" connota, in termini del tutto innovativi, l'intero impianto del Regolamento 2016/679 (v., oltre l'art.5 e tra gli altri, gli artt.23-25, l'art.28 e i Considerando nn. 74 e 78).

Invero, il sistema di tutela dei dati personali non è più definito soltanto con prescrizioni dirette e precise alla cui mancata applicazione consegue una sanzione, ma anche come un obiettivo da realizzare che obbliga il titolare a dimostrare il rispetto e la conformità, del trattamento dei dati messo in atto, al regolamento, mediante l'adozione di preventive politiche interne e di meccanismi idonei a garantire tale osservanza; esse devono sostanziarsi in una serie di attività specifiche e dimostrabili, volte a assicurare la gestione del rischio connesso al trattamento dei dati personali, tanto è vero che viene resa esplicita la richiesta di documentare le scelte in merito al raggiungimento dell'obiettivo prefissato di protezione dei dati.

È utile rammentare che la Corte di Giustizia dell'Unione Europea (v., in tal senso, la sentenza del 16 gennaio 2019, *Deutsche Post*, C-496/17, EU-C/2019/26, punto 57 e giurisprudenza ivi citata) ha affermato che ogni trattamento di dati personali deve, da un lato, essere conforme ai principi relativi al trattamento di quelli elencati all'articolo 5 del Regolamento e, dall'altro, rispondere a uno dei principi relativi alla liceità del trattamento dati elencati all'articolo 6 di detto regolamento.

3.1. - In sintesi, per quanto interessa nel presente caso, il trattamento dei dati biometrici intesi a identificare in modo univoco una persona fisica in mancanza del consenso dell'interessato è vietato ai sensi del Regolamento 2016/6790; il divieto viene meno e il trattamento è ammesso quando è necessario per motivi di interesse pubblico rilevante, in specifiche materie, tra cui rientra l'istruzione e la formazione in ambito scolastico, professionale, superiore o universitario, secondo quanto previsto dal d.lgs. n. 196/2003, con la precisazione che il trattamento *«deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato »*, in linea anche con il principio di "responsabilizzazione" dettato dall'art.5, par. 2 del Regolamento 2016/679.

3.2.- Il Tribunale ha affermato che *Respondus*, descritto come un *software* che «cattura le immagini video e lo schermo dello studente identificando e contrassegnando con un flag i momenti in cui sono rilevati comportamenti insoliti e/o sospetti mediante registrazione video e istantanee scattate a intervalli casuali per tenere traccia di comportamenti anomali… Al termine della prova, il sistema elabora il video, inserendo segnali di allerta in merito a possibili indici di comportamenti scorretti … affinché il docente … possa poi valutare se effettivamente sia stata commessa un'azione non consentita nel corso della prova» (fol.12), realizza la mera

acquisizione di una foto (o una registrazione video) e non configura un trattamento di dati biometrici.

In questa sequenza, secondo il Tribunale, non vi sarebbe trattamento dei dati biometrici tesi a identificare in modo univoco una persona fisica, posto che lo studente esaminato dal *software* non sarebbe identificato attraverso i suoi dati biometrici raccolti e trattati dal sistema *Respondus*, ma dal docente chiamato a vagliare il video finale.

3.3.- La conclusione è in contrasto con le norme in materia di trattamento dei dati personali e l'errore che segna la ricostruzione del Tribunale riguarda la sussunzione della fattispecie concreta nella fattispecie astratta di trattamento di dati personali, *genus* nel quale rientrano i dati biometrici.

3.4.- Come si evince dalla descrizione del funzionamento del *software Respondus* (prima ricordata e desunta dalla sentenza impugnata), questo non si limita a registrare a video la prova di esame, ma nel corso della ripresa cattura immagini della persona fisica che svolge la prova di esame e seleziona, mediante la realizzazione di video, lo scatto di istantanee ad intervalli casuali e i momenti in cui rileva comportamenti insoliti. Proprio in ragione della contestuale selezione del materiale raccolto in merito a comportamenti anomali, al termine della prova, lo stesso *software* realizza un video in cui confluiscono gli elementi anomali (contrassegnati da flag) che possono attenere alla conferma o meno della corrispondenza fisica della persona esaminata con lo studente (già identificato dall'Università come da sottoporre alla prova) e a ulteriori anomalie registrate; video che viene sottoposto al docente, per la sua valutazione finale in ordine alla regolarità della prova sostenuta dalla persona.

Risulta da ciò palese che le riprese video e foto realizzate da *Respondus* non hanno solo la funzione di documentare la prova di esame, ma si connotano per la contestuale elaborazione e

selezione del materiale, di momento in momento raccolto, selezione che converge nella individuazione ed alla segnalazione di comportamenti anomali, attraverso la produzione del video finale.

Il Tribunale ha mancato di considerare che questa complessiva attività integra un autonomo e articolato trattamento dei dati biometrici acquisiti ed elaborati dallo stesso *software*, e attiene anche alla conferma dell'identità della persona fisica esaminata, come previsto dall'art.4, n.14 del Regolamento, giacché l'esito di detta elaborazione risulta sottoposto solo *ex post* al docente per la sua valutazione in ordine alla regolarità della prova.

Come ricordato dallo stesso Tribunale, il ciclo di vita dei dati biometrici è costituito dalla sequenza in quattro fasi — secondo la Descrizione accreditata dal Garante per la protezione dei dati personali, Linee Guida in materia di riconoscimento biometrico e firma grafometrica, 12 novembre 2014 — che vede:

a) Una prima fase, con un rilevamento tramite sensori specializzati (ad es. scanner per il rilevamento dell'impronta digitale) o dispositivi di uso generale (ad es. videocamera) di caratteristiche biometriche (ad es. viso dell'individuo);
b) Una seconda fase: a seguito del rilevamento si acquisisce un campione biometrico (ad es. immagine del viso);
c) Una terza fase: dal campione biometrico vengono estratti tratti (ad es. specifici punti del viso) idonei a costituire il modello biometrico che sarà conservato in una banca dati;
d) Una quarta fase, cd. del confronto (o di *match*): il modello biometrico viene confrontato con le effettive caratteristiche dell'individuo ed il confronto in parola consente la identificazione univoca della persona fisica.

La decisione impugnata non risulta avere tenuto conto, rettamente, di tali indicazioni, perché ha trascurato di considerare che, nel procedimento attuato mediante l'utilizzo del *software Respondus*, per come descritto dalla stesso Tribunale, la quarta

fase di confronto appare svolgersi nel corso di tutta la ripresa, sulla scorta della elaborazione informatica dei dati di volta in volta acquisiti ed elaborati mediante la creazione di flag relativi ai comportamenti anomali, che possono riguardare anche la conferma della corrispondenza identitaria della persona ripresa in video con quella dello studente da esaminare, proprio perché già identificato dall'Università, e che il controllo conclusivo della prova di esame, affidato al docente persona fisica non esclude (ne è incompatibile con) il trattamento automatizzato dei dati biometrici, ove già attuato mediante l'impiego del *software,* e non lo sottrae alla disciplina dettata dall'art.9 del Regolamento 2016/679.

3.5.- Il motivo, che è dunque fondato, va accolto e il Tribunale, in sede di rinvio, dovrà procedere al riesame, attenendosi al seguente principio di diritto:

«In tema di trattamento dei dati personali, ai sensi dell'art.9 del Reg (UE) 2016/679, ricorre un trattamento di dati biometrici, come definiti dall'art. 4, n.14 del Regolamento 2016/679, quando i dati personali sono ottenuti mediante un trattamento tecnico automatizzato specifico, realizzato con un *software* che, sulla base di riprese e analisi delle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, le elabora, evidenziando comportamenti o elementi anomali, e che perviene a un esito conclusivo, costituito da una elaborato video/foto che consente (o che conferma) l'identificazione univoca della persona fisica, restando irrilevante la circostanza che l'esito finale del trattamento sia successivamente sottoposto alla verifica finale di una persona fisica».

4.1.- Con il secondo motivo si denuncia la violazione e falsa applicazione degli artt. 44, 45 e 46 Regolamento (UE) 2016/679; degli artt. 3, 4 e 5 delle clausole contrattuali allegate alla Decisione n. 2010/87/UE Commissione Europea; art. 1321 c.c. (art. 360 primo comma, n. 3 c.p.c.).

A parere del ricorrente, la sentenza va parimenti cassata con riferimento a quanto erroneamente ritenuto dal Tribunale in punto di trasferimento internazionale dei dati personali, sull'osservazione che l'Accordo di modifica sottoscritto dall'Università e dalla società *Respondus*, in data 18 agosto 2020, fosse tale da impedire il trasferimento internazionale di dati personali.

Ancora la decisione impugnata sarebbe erronea, laddove ha ritenuto che la "pseudonomizzazione" dei dati trattati fosse misura "adeguata", senza considerare che il dato trattato, coincidendo con il volto di una persona poteva sempre condurre alla identificazione della stessa, indipendentemente dai dati aggiuntivi di cui disponeva il titolare.

4.2.- Il motivo è fondato e va accolto.

4.3.- Con la sentenza del 16 luglio 2020 relativa alla causa C-311/18, la Corte di Giustizia europea ha dichiarata invalida la decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime del Privacy Shield, lo scudo UE-USA per la protezione dei dati personali oggetto di trasferimento verso gli Stati Uniti. Essa ha giudicato, invece, valida la decisione 2010/87 relativa alle Clausole Contrattuali Tipo (SCC) per il trasferimento di dati personali a destinatari stabiliti in Paesi terzi.

A seguito di questa decisione è intervenuto tra l'Università Bocconi e la società Respondus un accordo di modifica sottoscritto in data 18 agosto 2020, con il quale sono state recepite le clausole contrattuali tipo dettate nella Decisione della Commissione europea del 5 febbraio 2010 n. 87/UE.

Il Tribunale ha ritenuto che l'accordo così riformulato fosse tale da impedire il trasferimento internazionale di dati personali, proprio perché all'accordo di modifica erano allegate le clausole tipo di cui alla Decisione 2010/87/UE.

Segnatamente, il Tribunale, sul rilievo che l'allegato si compone di due appendici, di cui la prima descrive il tipo di trattamento e la seconda indica le misure tecniche- organizzative implementate da Responsus e da Amazon Web Service, sub-responsabile di Respondus, ha ritenuto corrette le clausole allegate mediante semplice rinvio *per relationem*, sia sul piano formale che sul piano sostanziale, osservando che il rispetto delle stesse era idoneo a garantire agli interessati una tutela adeguata rispetto agli standard europei.

Sul piano formale, il Tribunale ha argomento richiamando la giurisprudenza di legittimità che ha ammesso che il contenuto di una clausola contrattuale possa essere determinato tramite rinvio ad un documento esterno al contratto stesso; sul piano sostanziale, concernente l'adeguatezza delle clausole contrattuali standard e delle garanzie supplementari, il Tribunale ha ravvisato un "difetto probatorio" dell'argomentazione spesa dal Garante.

4.4.- Tali conclusioni sono errate.

4.5.- E' opportuno ricordare che la Decisione della Commissione del 5 febbraio 2010 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, rimarca, tra l'altro, la posizione centrale che assume l'interessato (e cioè la persona fisica i cui dati personali sono trattati) affermando, ai Considerando 19 e 20, che *«(19) È opportuno che le clausole contrattuali tipo possano essere fatte valere non solo dalle organizzazioni che stipulano il contratto ma anche dalle persone cui si riferiscono i dati, in particolare laddove l'eventuale violazione del contratto rechi ad esse pregiudizio.»* e che l'interessato deve poter agire in giudizio, anche ai fini del risarcimento dei danni, nei confronti dell'esportatore che è il responsabile del trattamento dei dati personali trasferiti e, a

determinate condizioni, nei confronti dell'importatore o di un suo sub incaricato per violazione degli obblighi stabiliti dalla clausola 3 dell'Allegato.

Inoltre, all'art.1, è puntualizzato che *«Le clausole contrattuali tipo riportate in allegato costituiscono garanzie sufficienti per la tutela della vita privata e dei diritti e della libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE.»*

Ed invero, il relativo Allegato "Clausole Contrattuali Tipo («Incaricati Del Trattamento»)" espressamente introduce con la clausola 3 (clausola del terzo beneficiario) i diritti che l'interessato può far valere – a seconda dei casi – sia con riferimento alla medesima clausola 3, sia in relazione alla clausola 4, lettere da b) a i), alla clausola 5, lettere da a) ad e) e da g) a j), alla clausola 6, paragrafi 1 e 2, alla clausola 7, alla clausola 8, paragrafo 2, e alle clausole da 9 a 12 in qualità di terzo beneficiario, nei confronti dell'esportatore, dell'importatore o del sub incaricato, anche mediante la rappresentanza da parte di un'associazione o di altra organizzazione, ove siffatta rappresentanza corrisponda alla esplicita volontà dell'interessato e sia ammessa dalla legislazione nazionale.

Va, quindi, evidenziato che la clausola 4, par. 1, lett. c) e la clausola 5, lett. c) delle clausole standard, prevedono espressamente che le misure di sicurezza debbano essere appunto "indicate nell'appendice 2" e che nella stessa appendice 2 si specifica che essa "costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti", contemplando una specifica sezione, denominata «Descrizione delle misure tecniche e organizzative di sicurezza attuate dall'importatore in conformità della clausola 4, lettera d), e della clausola 5, lettera c) (o del documento/atto legislativo allegato)» e

che tali disposizioni hanno efficacia anche con riferimento all' "interessato", che non è parte contraente, ma terzo beneficiario.

Alla luce di tali disposizioni, risulta errata al tesi del Tribunale secondo la quale il contenuto delle clausole contrattuali recanti le misure di sicurezza può essere determinato tramite rinvio ad un documento esterno al contratto stesso, considerato che tale principio nella specie non può trovare applicazione, in quanto la volontà contrattuale delle parti, *lex specialis* del rapporto sinallagmatico, si è espressa in senso ben diverso, proprio mediante l'integrale recepimento di quanto previsto dalla Decisione della Commissione del 5 febbraio 2010 e dai suoi allegati, in special modo dall'allegato due e dalle prescrizioni ivi contenute, tanto più che – come già ricordato – il contratto in esame assistito dalle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi non obbliga solo i contraenti tra loro, ma regola anche i diritti del terzo beneficiario che potrebbero essere elusi e frustrati, ove gli obblighi in materia di sicurezza non fossero oggettivamente individuati o individuabili, a maggior ragione ove le misure di sicurezza fossero consultabili solo mediante ripetuti accessi a sito web del fornitore e potessero mutare senza una espressa rinegoziazione tra i contraenti adeguatamente accessibile al terzo beneficiario.

È opportuno rammentare che con la sentenza del 16 luglio 2020 relativa alla causa C-311/18, la Corte di Giustizia europea non solo ha dichiarato invalida la decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime del Privacy Shield, lo scudo UE-USA per la protezione dei dati personali oggetto di trasferimento verso gli Stati Uniti ed ha giudicato, invece, valida la decisione 2010/87 relativa alle Clausole Contrattuali Tipo (SCC) per il trasferimento di dati personali a destinatari stabiliti in Paesi terzi, ma altresì precisato (in sintesi, in dispositivo) che *«L'articolo 46, paragrafo 1, e*

l'articolo 46, paragrafo 2, lettera c), del regolamento 2016/679 devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta dei diritti fondamentali dell'Unione europea. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo, in particolare quelli enunciati all'articolo 45, paragrafo 2, di detto regolamento.» e che *«L'articolo 58, paragrafo 2, lettere f) e j), del regolamento 2016/679 deve essere interpretato nel senso che, a meno che esista una decisione di adeguatezza validamente adottata dalla Commissione europea, l'autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora detta autorità di controllo ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, segnatamente dagli articoli 45 e 46 di tale regolamento e dalla Carta dei diritti fondamentali, non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del*

trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo.». Si deve, in proposito osservare che, nel caso in esame, la mancata esplicitazione delle misure di sicurezza nell'allegato 2, in difformità da quanto da questo previsto, la complessità, non contestata, della modalità di accesso informatico alle misure di sicurezza e l'incertezza sul contenuto delle stesse, come evidenziate dall'Autorità di controllo, sono circostanze che avrebbero dovuto essere espressamente valutate dal Tribunale in ordine all'applicabilità dell'art.58, par. 2, lett. f) e j), del regolamento 2016/679.

4.6.- Resta assorbita all'esito del riesame, la questione sostanziale dell'adeguatezza o meno delle clausole contrattuali standard e delle garanzie supplementari, risolta dal Tribunale ravvisando impropriamente un "difetto probatorio" dell'argomentazione spesa dal Garante.

4.7.- Anche la questione introdotta in merito alla ravvista pseudonomizzazione dei dati resta assorbita all'esito del riesame, atteso che la decisione sul punto risulta inficiata dalla erronea qualificazione dei dati trattati come dati personali comuni piuttosto che come dati biometrici , cioè dati personali ottenuti da un trattamento tecnico automatizzato specifico, relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quale, nel presente caso, l'immagine facciale.

5.- Il terzo motivo, con cui in via subordinata, si denuncia l'omesso esame circa un fatto decisivo per il giudizio che è stato oggetto di discussione tra le parti (art. 360, primo comma, n. 5 c.p.c.) con riferimento alla parte della sentenza in cui il Tribunale ha rideterminato la sanzione applicabile alla controparte, è assorbito.

6.- In conclusione, vanno accolti i primi due motivi di ricorso e dichiarato assorbito il terzo; la sentenza impugnata è cassata con

rinvio della causa al Tribunale di Milano in persona di diverso magistrato, per il riesame della controversia alla luce dei principi enunciati e la liquidazione delle spese anche del presente giudizio.

P.Q.M.

- Accoglie i motivi primo e secondo; dichiara assorbito il terzo;

- Cassa la sentenza impugnata in relazione ai motivi accolti e rinvia la causa al Tribunale di Milano in persona di diverso magistrato, cui demanda di provvedere anche sulle spese del giudizio di legittimità;

Così deciso in Roma, nella camera di consiglio della Prima