Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano – 16 settembre 2021

Registro dei provvedimenti
n. 317 del 16 settembre 2021

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 e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, 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 la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. Introduzione.

Con reclamo del XX, come successivamente integrato in data XX, uno studente dell'Università Commerciale "Luigi Bocconi" di Milano (di seguito, l'"Università" o l'"Ateneo") ha lamentato possibili violazioni della disciplina sulla protezione dei dati personali in relazione all'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 particolare è stato rappresentato che l'Ateneo avrebbe richiesto il consenso degli studenti al trattamento "delle categorie particolari di dati personali (dati biometrici […]), [in mancanza del quale gli studenti] non sarebbero in grado di svolgere esami online" con ciò comportando un "pregiudizio estremo […]".

Con lo stesso reclamo, è stato evidenziato che il responsabile della protezione dei dati dell'Ateneo, in risposta alla richiesta di chiarimenti dell'interessato, ha chiarito che, nel contesto dell'emergenza epidemiologica da SARS-CoV-2, è stata individuata una modalità alternativa di svolgimento degli esami universitari a distanza, che l'obiettivo di assicurare le medesime garanzie previste per gli esami in presenza poteva essere raggiunto attraverso il trattamento di categorie particolari di dati, come i dati biometrici e che, dopo un'attenta analisi, l'Ateneo ha individuato nell'azienda Respondus il migliore fornitore per rispondere alle proprie esigenze, anche tenuto conto della necessità di effettuare circa 60.000/70.000 prove scritte, dovendo assicurare la parità delle condizioni di accesso alle prove per tutti gli studenti.

2. L'attività istruttoria.

Con nota del XX (prot. del Garante n. XX del XX), in risposta alla richiesta d'informazioni del Garante, l'Ateneo ha dichiarato, in particolare, che:

– "l'Università Bocconi è un'università internazionale, non statale, legalmente riconosciuta e autorizzata al rilascio di titoli di studio d'istruzione superiore, aventi valore legale";

– "il recente orientamento del Consiglio di Stato nella controversia tra ANAC/università non statali (per Bocconi sentenza CdS n. 3041/2016; n. 3042/2016; n. 3040/2016) che qualifica quest'ultime come soggetti di diritto privato, […] ritiene che la sola facoltà riconosciuta alle università libere di rilasciare titoli aventi valore legale non è di per sé sufficiente a determinarne l'appartenenza alla categoria degli enti pubblici. […]" e, su tali basi, l'Ateneo avrebbe individuato i presupposti di liceità del trattamento in questione tenuto conto della propria "qualificazione di soggetto di natura privatistica";

– nell'ambito della situazione di emergenza causata dall'epidemia da SARS-CoV-2, "al fine di assicurare il normale svolgimento delle sessioni d'esame, stante l'impossibilità di sostenere le prove come di consueto dal vivo e in presenza, la Bocconi ha deciso di dotarsi di un software ([…] "Respondus") fornito dalla società Respondus Inc. ([…] il "Fornitore") – debitamente nominato responsabile del trattamento ai sensi e per gli effetti dell'art. 28 del [Regolamento] […] che consentisse al docente di poter verificare la genuinità della prova scritta resa dagli Studenti, senza che la stessa potesse esser alterata, attraverso sostituzioni di persona e/o contraffazioni, o altri interventi distorsivi della misura e valutazione dell'apprendimento personale";

– "l'Università ha l'onere di prevedere tutte le misure idonee per poter considerare pienamente validi gli esami sostenuti dai propri studenti […], al fine di garantire il pieno valore legale del titolo di studio dagli stessi conseguito";

– “la Bocconi ha inteso adottare il sistema di proctoring unicamente per i corsi di studi “core”, finalizzati al conseguimento di un titolo con valore legale, quale metodo per garantire terzietà, imparzialità ed eguale trattamento. Per tutti gli altri programmi formativi, invece, l’Università ha preferito sostenere prove a distanza utilizzando sistemi differenti”;

– “l’impossibilità di svolgere le sessioni d’esame secondo la consueta procedura, ha portato l’Università […] a strutturare un processo che, nel rispetto del [Regolamento] e del Codice Privacy, unicamente per le prove d’esame scritte, fosse in grado di identificare gli Studenti attraverso l’utilizzo temporaneo del loro dato biometrico e, dunque, elaborando automaticamente le immagini digitali che raffigurano il volto degli stessi a fini di identificazione, autenticazione e verifica” in particolare la “fotografia del tesserino” e “l’immagine fotografica scattata da Respondus;

– con riguardo alle basi giuridiche del trattamento, l’Università ha dichiarato che “per i dati comuni il fondamento giuridico è stato individuato nell’art. 6 lett. b) del [Regolamento]; per i dati biometrici il fondamento giuridico è stato individuato nell’art. 9 lett. a) del [Regolamento]”;

– nonostante “il provvedimento del Garante del 26 marzo 2020 e il d.p.c.m. del 27.4.2020 art. 1 lett. n)”, l’Ateneo, “ha scelto di considerare per i propri Studenti l’opzione dell’esame scritto online e da remoto tramite sistema di proctoring come strada preferita, per ragioni di coerenza con il modello didattico adottato, basandosi sul consenso. Ciò risulta anche in linea con la natura privatistica dell’Università”;

– il sistema di proctoring è stato impiegato per la prima volta nella sessione estiva “che […] è cominciata dopo la promulgazione del d.p.c.m. del 27.4.2020 ed in particolare, per tutti gli ordinamenti di studio attivi, nel periodo compreso tra il 13.5.2020 e il 21.7.2020”;

– l’Ateneo, “al fine di garantire il diritto allo studio dello Studente, tutelandone la libera autodeterminazione, ha posto in essere immediatamente misure organizzative idonee per consentire agli esaminandi, che avessero eventualmente deciso di non concedere il consenso al trattamento del dato biometrico, di avvalersi di modalità alternative da concordarsi con l’unità Academic Services che gestisce il calendario delle prove d’esame”, senza subire “alcun nocumento né ritardo nella carriera universitaria”;

– è stata resa agli studenti l’informativa “ai sensi e per gli effetti dell’art. 13 del [Regolamento]”;

– “il dato biometrico dello Studente non viene trattato direttamente dall’Università, ma solo dal Fornitore che lo tratta temporaneamente per la durata della sessione d’esame per poi cancellarlo senza conservarlo”;

– “il Trattamento non importa un processo decisionale automatizzato. Infatti, nell’ipotesi in cui Respondus rilevi un evento anomalo potenzialmente idoneo ad invalidare la prova d’esame, il software segnala al docente l’anomalia […] che, nell’esercizio del proprio potere discrezionale di valutazione, deciderà sull’eventuale annullamento”;

– “il Trattamento comporta un trasferimento dei dati extra UE da parte del Fornitore” che ha dichiarato di essere “conforme al Privacy Shield Framework EU -U.S.”;

– “l’Università, ai sensi dell’art 35 par. 11 del [Regolamento], in considerazione della sentenza resa il 16.7.2020 e alla conseguente decisione della Corte di Giustizia Europea di invalidare la Decisione 2016/1250 sull’adeguatezza della tutela approntata per i diritti e le libertà degli interessati dal Privacy Shield, ha ritenuto necessario rivedere l’Accordo di nomina sottoscritto da Respondus”.

Con successiva nota del XX, l’Ateneo ha integrato il proprio riscontro, fornendo, in particolare, copia di un atto aggiuntivo, datato XX, all’accordo sul trattamento dei dati personali stipulato con Respondus, Inc. ai sensi dell’art. 28 del Regolamento, che reca in allegato le clausole contrattuali tipo, di cui alla Decisione della Commissione europea del 5 febbraio 2010, stipulate tra l’Ateneo e Respondus, Inc..

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’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, avente ad oggetto le presunte violazioni:

degli artt. 5, par. 1, lett. a), 6 e 9 del Regolamento, nonché 2-sexies del Codice, per aver trattato i dati biometrici degli studenti, nonché per aver effettuato un trattamento automatizzato finalizzato a consentire l’analisi di determinati aspetti del comportamento degli studenti, danno quindi luogo alla loro “profilazione”, in assenza di un’inidonea base giuridica;

degli artt. 5, par. 1, lett. a), e 13 del Regolamento), per non aver fornito agli interessati una completa informativa sul trattamento;

dell’art. 5, par. 1, lett. c) ed e), e 25 del Regolamento, per aver trattato i dati personali degli studenti in maniera non conforme ai principi di minimizzazione, limitazione della conservazione e protezione dei dati personali fin dalla progettazione e per impostazione predefinita;

degli artt. 44 e 46 del Regolamento, per aver trasferito dati personali verso un Paese terzo, ovvero gli Stati Uniti d’America, senza aver comprovato di aver verificato e assicurato che il trasferimento in questione fosse posto in essere nell’effettivo rispetto delle condizioni di cui al Capo V del Regolamento;

dell’art. 35 del Regolamento, per non aver effettuato un’adeguata valutazione di impatto sulla protezione dei dati con riguardo ai trattamenti di dati personali effettuati mediante “Respondus”.

Con la medesima nota, l’Ateneo 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, dalla l. 24 novembre 1981, n. 689).

Con nota dell'XX (prot. n. XX), l'Ateneo ha presentato la propria memoria difensiva, dichiarando, in particolare, che:

l'Ateneo ha deciso di "dotarsi di sistemi di proctoring", così come altri "atenei che, durante il periodo pandemico correlato all'emergenza causata dal Covid 19, si sono avvalsi del sistema in discussione (o similari) […,] nell'intento di poter garantire complessivamente i diritti degli [studenti che] hanno avuto la possibilità di proseguire – senza danno alcuno – gli studi intrapresi, nonostante l'emergenza in essere";

"il particolare contesto emergenziale […] nonché i tempi strettissimi nei quali occorreva trovare una soluzione efficace ed efficiente […] hanno portato la Bocconi a ritenere che solo un sistema di proctoring avrebbe potuto soddisfare le reali esigenze dei propri studenti – per la maggior parte fuori sede e per il 19% di nazionalità non italiana – e dei circa 2.000 studenti incoming in scambio che ogni anno raggiungono la Bocconi da ogni parte del mondo";

"la stessa Università non ha mai smesso di interrogarsi sulla sostituibilità del software implementato, magari anche attraverso altri sistemi che fossero parimenti in grado di garantire la serietà della prova. […] Inoltre, l'Università ha continuato a intrattenere rapporti con Respondus per valutare in maniera sempre più approfondita il funzionamento del software implementato [, fermo restando che] né la Bocconi né Respondus, infatti, trattano il dato biometrico degli studenti";

"Respondus blocca l'utilizzabilità del browser, inibendo di fatto la possibilità che lo studente durante il periodo della prova d'esame possa avvalersi di strumenti d'ausilio presenti sul proprio dispositivo informatico – per tali intendendo tanto le ricerche effettuabili direttamente sul web quanto le consultazioni di appunti e/o dispense salvati sul dispositivo stesso sotto forma di file di diverso tipo – al fine di sostenere la prova. In altri termini, Respondus Monitor non tiene traccia dell'attività compiuta sulla rete dallo studente, delle applicazioni in uso, dei tasti digitati e dei movimenti del mouse, ma, più semplicemente, blocca lo schermo del computer e impedisce allo studente tutte quelle interazioni con il dispositivo che non siano strettamente correlate allo svolgimento della prova d'esame";

"è […] del tutto improbabile che attraverso il sistema possano essere desunti dati personali o informazioni ulteriori attinenti agli aspetti relativi alla vita privata dello studente";

"[…] in ogni caso, il descritto sistema opera solo ed esclusivamente per il tempo corrispondente alla durata della prova d'esame […]";

per quanto concerne la presunta "profilazione degli interessati […] l'identificazione e la valutazione della prova sostenuta dallo studente e, dunque, il giudizio e il correlato esito dell'esame, sono rimessi completamente al docente di riferimento, al quale spetta la valutazione del comportamento tenuto dallo studente in concreto: ne consegue che il sistema si limita meramente a segnalare, non potendo certamente essere allo stesso attribuita una funzione decisoria. […] L'unico ausilio fornito dal software in esame è l'estratto di alcuni fotogrammi dalla registrazione audiovisiva, che potrebbero esser indicatori di anomalie durante la prova […]";

in merito ai tempi di conservazione dei dati, “è vero che, in astratto, la registrazione video della prova d’esame potrebbe restare nelle disponibilità dei sistemi informativi del fornitore per […] un anno sul sistema AWS S3 bucket cui si aggiungono quattro anni, di long term storage, sul sistema AWS Glacier. Tuttavia, la DPIA deve essere letta in combinato disposto con tutte le previsioni dell’accordo di nomina a responsabile [, in base alle quali] […] [a] semplice richiesta dell’Università […] il fornitore [procede] tanto alla cancellazione dei dati, quanto alla notifica dell’intervenuta cancellazione. […] La Bocconi, infatti, chiede che venga effettuata le descritta cancellazione non decorsi cinque anni dalla data di espletamento della prova, bensì una volta che si è formalmente chiusa la sessione d’esame e si è perfezionato […] il procedimento di valutazione delle prove sostenute dagli studenti”. […] [in ogni caso,] “la registrazione video non viene archiviata in chiaro sui sistemi informativi dell’Università, tanto che il docente non ha la possibilità di scaricare detto video, senza previa autorizzazione espressa del Titolare. Infatti il video è, fino alla sua cancellazione, conservato in maniera completamente crittografata sui server del fornitore; solo le persone autorizzate all’interno dell’Università, per ciascuna singola prova, detengono la chiave privata per renderlo leggibile. […] Con specifico riferimento alla conservazione delle registrazioni video, la Bocconi ha ritenuto opportuno conservare le stesse, nelle modalità sopra dettagliate, per un tempo corrispondente a 12 mesi decorrenti [dalla data di comunicazione dei risultati della prova agli studenti], salvo che sulla singola prova non siano pendenti dei procedimenti disciplinari o contenziosi di fronte alle Autorità giudiziarie competenti. […] Decorsi, quindi, i richiamati termini, l’Università distrugge l’unica chiave privata di accesso ai dati crittografati e chiede, come descritto, la cancellazione delle registrazioni anche al fornitore.”;

oltre alla possibilità dello svolgimento in presenza in caso di mancato consenso dello studente, “l’Università ha anche concretamente valutato […] di prevedere, per casi particolari, quali gli studenti all’estero, il sostenimento dell’esame orale in modalità online”;

inoltre, “si ritiene non corretto affermare che dare la possibilità di sostenere gli esami presenza avrebbe esposto i docenti e gli studenti a un più elevato rischio per la salute degli stessi [, stante quanto previsto dal] […] d.p.c.m. del 27.4.2020 art. 1 lett. n) […] [, essendo evidente] […] che, con le opportune cautele […] fosse astrattamente già possibile sostenere gli esami in presenza, ovviamente per chi non avesse voluto prestare il consenso”;

l’Ateneo “ha un continuo dialogo con il proprio corpo studentesco che […] non può essere considerato al pari di un contraente debole, la cui posizione sperequata legittimerebbe meccanismi di più forte tutela. Né certo la condizione di presunta ansia in cui versa lo studente chiamato a sostenere le prove d’esame, ovvero il metus nei confronti del docente, possono in alcun modo essere considerati come situazioni idonee a condizionare il consenso eventualmente prestato. […] Specie quando, come nel caso [di specie], l’eventuale rifiuto non sarebbe stato nemmeno manifestato nei riguardi del professore di riferimento, ma unicamente avvalendosi dei canali indicati dall’Università che prevedevano una specifica richiesta all’Academic Services. Ed infine […] nell’ipotesi in cui il docente ponga in essere “ripercussioni negative”, lo stesso non andrà esente da responsabilità disciplinari per propria condotta professionale […]”;

l'Università si è impegnata a "mutare le basi giuridiche indicate all'interno dell'informativa, lasciando impregiudicata quella individuata per il trattamento dei dati comuni e modificando quella per il trattamento dei dati biometrici, individuandola nel perseguimento di un interesse pubblico, ai sensi dell'art. 9 lett g) del GDPR e degli artt. 2 ter e 2 sexies lett. bb del Codice Privacy";

"tuttavia, con riferimento al dato biometrico […] [che] il poco tempo a disposizione per l'implementazione del processo […] ha portato l'Università a fare affidamento su un'affermazione di Respondus successivamente dimostratasi non corrispondente alla realtà dei fatti […] a seguito di ulteriori approfondimenti […] la Bocconi ha appreso [che] l'identificazione dello studente avveniva e avviene a posteriori per il tramite di un operatore umano, senza l'utilizzo del dato biometrico per finalità identificative […] Di conseguenza, a seguito di formale richiesta da parte dell'Università […], Respondus […] ha dichiarato che il proctoring implementato non comporta alcun trattamento di categorie particolari di dati […]";

"[…] il sistema non è in grado di confrontare in maniera univoca il volto dello studente e la fotografia del documento mostrato. In altri termini non si ha in nessun caso, per finalità identificative, la creazione di un modello biometrico del singolo studente dal quale verrà estratto successivamente un campione biometrico da conservare per le successive operazioni di confronto (c.d. match)";"[…] anche in fase di controllo del comportamento dello studente, nessun dato biometrico viene trattato da parte dei sistemi. Il fatto che si utilizzi la locuzione "riconoscimento facciale" non implica necessariamente che i sistemi approntati per il monitoraggio del comportamento dello studente trattino il dato biometrico dello stesso";

con riguardo alla contestazione relativa all'incompletezza dell'informativa resa agli studenti, l'Ateneo evidenzia che "lo stesso documento contestato fa rinvio all'informativa completa […] attraverso specifico link ipertestuale […]";

"la Bocconi riconosce che l'informativa potrebbe potenzialmente difettare di trasparenza, non essendo indicato un periodo di conservazione specifico";

"[…] tenuto conto della previsione dell'art. 13 del GDPR […] gli studenti […hanno] ricevuto, per tempo, diverse istruzioni e chiarimenti ben prima dell'avvio del trattamento, con informazioni multilayer […]";

tenuto della formula ampia della lett. f) dell'art. 13 del Regolamento "l'Università nell'informativa individua l'articolo del Regolamento che consente il trasferimento extra UE dei dati personali degli studenti, facendo specifico riferimento all'art. 46, e lascia in ogni caso la possibilità all'interessato di "richiedere maggiori dettagli al Titolare del Trattamento richiedendo evidenza delle specifiche garanzie adottate";

l'Ateneo ha precisato di aver stipulato "con Respondus, in data XX un primo accordo di nomina a responsabile, ai sensi dell'art. 28 del Regolamento, con il quale, per ciò che attiene al trasferimento dei dati personali extra UE, faceva riferimento, ai sensi dell'art. 46 del Regolamento, al Privacy Shield e, dunque, all'allora vigente Decisione di esecuzione (UE) 2016/1250 della Commissione. A seguito della sentenza della Corte

di Giustizia del 16 luglio 2020, provvedeva a modificare l'accordo di nomina e a sottoscrivere le clausole contrattuali standard già il 10 agosto 2020";

"[…] l'Università [è] ben consapevole delle misure approntate dal fornitore, considerato che proprio le stesse, sebbene soltanto richiamate nell'appendix 2 delle clausole contrattuali tipo sottoscritte, sono state oggetto di opportune valutazioni analitiche […]. L'Università già prima della sentenza Schrems aveva posto in essere "l'adozione di misure supplementari da parte del titolare del trattamento al fine di garantire il rispetto di tale livello di protezione" (par. 133 della sentenza Schrems). Le misure di sicurezza […] sono state allegate alla stessa DPIA […]. Tutta la valutazione d'impatto è stata proprio condotta tenendo in considerazione il documento Respondus Checklist […] da dove risulta evidente che […] dati personali oggetto di trattamento sono tutti crittografati con l'algoritmo Advance Encryption Standard 256 bit29 e la chiave privata è detenuta esclusivamente dalla Bocconi, sì da esser impossibile, anche per il governo americano, accedere agli stessi. A ciò si aggiunga anche che Respondus Monitor tra l'altro i) soddisfa i requisiti di sicurezza di FERPA, GDPR, CCPA, Privacy Shield, SOC 2 ed i suoi ingegneri sono anche AWS Certified30; ii) tutti i dati sono crittografati dall'inizio alla fine del processo che vede coinvolto Respondus. Tale circostanza determina di per sé la conformità con quanto stabilito dalla Corte di Giustizia Europea nonché l'accountability dell'Università. Il fatto che si rinvii alle misure, senza allegarle a quanto sottoscritto, non implica automaticamente che la valutazione condotta dalla Bocconi, quale titolare del trattamento, sia insufficiente […] La stessa clausola tipo […] prevede proprio che l'esportatore si assuma l'obbligo di valutare – dichiarando e garantendo – che l'importatore fornisca sufficienti misure tecniche e organizzative di sicurezza, nulla prevedendo in merito alle modalità con cui tale obbligo debba essere espletato. Detto altrimenti non è normativamente previsto che il contratto indichi le misure di sicurezza per iscritto […] ad substantiam […]";

"[…] le Raccomandazioni 01/2020 del Comitato europeo per la protezione dei dati personali – inidonee peraltro ad assumere la natura di fonte del diritto, trattandosi di soft regulation, e come tali assolutamente non vincolanti – sono successive alle violazioni oggi contestate. […] In ogni caso, [occorre] osservare che, considerate le tipologie di dati personali e le attività di trattamento concretamente poste in essere da Respondus, le misure predisposte sono da considerarsi sufficienti, ed idonee, anche e soprattutto alla luce dell'uso di sistemi di crittografia dei dati personali e alla concreta inaccessibilità degli stessi da parte di soggetti terzi, ivi compreso il responsabile e l'autorità statunitensi";

"al tempo in cui sono state effettuate le scelte d'implementazione dei processi, si è ritenuto che non vi fossero altri sistemi che ragionevolmente potessero essere in grado di garantire, in forma digitale, la serietà di processi che fino a quel momento erano stati costruiti in modalità analogica. È apparso, quindi, che il trattamento secondo le descritte modalità fosse indispensabile, perché sistemi digitali diversi sarebbero stati inevitabilmente insoddisfacenti per almeno due ragioni: a) da un lato, perché sono troppi gli interessati che costituiscono il corpo studentesco dell'Università (oltre 14.000 studenti) […]; dall'altro, il tipo di prova – esame scritto – rende impossibile il raggiungimento delle prescritte finalità senza l'ausilio di sistemi di proctoring […]. Anche il Tribunale di Amsterdam si è recentemente pronunciato sul

sistema di proctoring analogo al presente [, ritenendolo conforme alla normativa in materia di protezione dei dati]";

"la legittimità di ciò è stato recentemente ribadita anche dal Garante spagnolo secondo cui "La situazione generata come conseguenza di Covid-19 e la dichiarazione dello stato di allarme potrebbe avere un'incidenza speciale, in cui la prevalenza del riconoscimento facciale potrebbe essere valutata rispetto ad altre misure […] [, dovendosi limitare tale opzione] a quei corsi e materie specifiche che, a causa della loro importanza, complessità o altre circostanze di particolare incidenza, non rendono consigliabile il ricorso ad altre opzioni […] o renderebbero l'adozione di altri mezzi come il controllo con videocamera o gli esami orali eccessivamente onerosi";

quanto all' "affidabilità della tecnologia impiegata […] l'Università ha effettuato una serie di approfondimenti tecnici in merito alle misure di sicurezza utilizzate dalla società Respondus Inc. – leader di mercato scelto da oltre mille Università – che sono illustrate nella relazione tecnica [prodotta dall'Ateneo]".

In occasione dell'audizione, richiesta ai sensi dell'art. 166, comma 6, del Codice e tenutasi in data XX (verbale prot. n. XX del XX), l'Ateneo, discostandosi con riguardo a taluni profili dalle dichiarazioni rese nelle precedenti comunicazioni, ha dichiarato, in particolare, che:

"prima dell'emergenza pandemica le prove si svolgevano in aule con un rapporto 1 a 3, ovvero convocando uno studente ogni tre posti in aula, per garantire l'efficacia dei controlli effettuati dai "proctor" fisici, i quali verificavano l'identità dello studente chiedendo di esibire il tesserino, nonché vigilavano sulla correttezza della prova. […] In tale contesto, con un solo docente si riusciva a seguire l'esame effettuato da 50 persone. L'Università si è pertanto trovata, nello stato emergenziale, nella condizione di dover effettuare le medesime prove ma a distanza […] L'alternativa di utilizzare un sistema di mera videoconferenza con supervisione di un proctor fisico avrebbe, probabilmente, richiesto un proctor ogni cinque studenti da verificare. Tale alternativa non sarebbe stata percorribile, richiedendo l'impiego di personale dieci volte superiore a quello disponibile";

"solo una decina, tra tutti gli studenti a cui è stata sottoposta la liberatoria, hanno scritto all'Università e solo un paio tra questi si sono detti contrari a questa modalità di svolgimento della prova; tuttavia, questi studenti non hanno poi dato seguito alle comunicazioni dell'Università, la quale si era resa disponibile a trovare delle alternative, e quindi non c'è stata l'esigenza di organizzare delle prove per questi due studenti con modalità diverse che non prevedessero il proctoring";

"a partire da marzo 2020 l'Università ha cominciato a raccogliere documentazione dal fornitore e tale documentazione è risultata essere stata redatta in maniera esaustiva e conforme agli standard internazionali. Il fornitore in tale documentazione e sul suo sito citava l'utilizzo di tecnologie biometriche. Tuttavia, nel contesto dell'emergenza, l'Università non ha potuto tempestivamente verificare in cosa consistesse l'asserito trattamento di dati biometrici. L'Università ha, quindi, cautelativamente assunto che per dati biometrici si intendesse la tipologia di dati di cui alla definizione fornita nel Regolamento UE 2016/679. In realtà, è poi successivamente emerso che Respondus

acquisisce l'immagine dello studente e verifica che questo volto rimanga lo stesso durante la prova, ma non mette il volto in relazione con l'identificativo della persona. Questa identificazione è effettuata dal docente solo successivamente: il docente, quando riceve il report con il filmato della prova, confronta una fotografia scattata dal sistema all'inizio della prova con la fotografia, presente negli archivi dell'Università, dello studente che avrebbe dovuto sostenere la stessa. Quindi, solo a posteriori, si è potuto concludere che non vi era l'utilizzo di un dato biometrico a norma del Regolamento UE 2016/679. Si precisa che, per quanto sopra, non si effettua alcuna estrazione del campione biometrico relativo al volto dello studente";

"il software Respondus ha due componenti: Respondus lockdown browser e Respondus monitor. Lockdown browser si comporta come un browser web perché visualizza le pagine che vengono caricate e proibisce di aprire altre pagine o finestre; impedisce, ad esempio, che si possa fare l'operazione di copia e incolla. Inoltre, impedisce l'esecuzione della prova se prima non vengono chiuse tutte le altre applicazioni. Pertanto, quando inizia la prova d'esame è garantito che sia in esecuzione solo lockdown browser e che lo studente visualizzi solo la pagina relativa alla prova d'esame. A questo punto la prova parte: durante la prova lo studente non può fare null'altro che non sia consentito dal sistema. Le altre funzioni del PC sono precluse e non viene tenuta traccia dei tentativi di effettuare attività precluse. In nessun caso viene tenuta traccia dei siti web eventualmente visitati. È possibile, peraltro, impostare il sistema in maniera tale da consentire di visitare determinati siti o usare determinate applicazioni utili ai soli fini del sostenimento della prova d'esame";

"Respondus monitor si attiva solo dopo che Lockdown browser ha garantito le condizioni necessarie per l'avvio della prova e rileva e analizza, ai fini della definizione dell'indice di correttezza della prova, dati come, ad esempio, il filmato, le modifiche del volto oggetto di ripresa o l'assenza dello stesso, il tempo di compilazione della prova e di risposta a ciascun quesito, i tasti digitati sulla tastiera, i movimenti del mouse, le applicazioni in esecuzione (al fine di eventualmente consentire talune applicazioni necessarie ai fini dell'esecuzione della prova, fermo restando che nell'esperienza dell'Ateneo non è mai stato dato accesso a siti esterni; pertanto, questa funzionalità non è stata utilizzata). Quanto all'attività della rete internet, viene misurato il traffico di rete e se questo traffico ha un quantitativo di byte anomalo, tale da far presumere un calo della banda di rete dello studente. Poiché non ci possono essere altre applicazioni in esecuzione, il sistema acquisisce solo i dati che sono necessari per determinare la correttezza della prova. Al termine della prova l'applicazione si chiude e non viene raccolta più nessuna informazione. Dopo l'elaborazione dei dati raccolti, il docente riceve un report che riporta l'immagine dello studente ai fini dell'identificazione e gli indici di eventuali anomalie, con il dettaglio della specifica motivazione dell'anomalia. La decisione sulla correttezza della prova d'esame è sempre responsabilità del docente. Il video che viene registrato non si può scaricare; il docente accede con le proprie credenziali e non può vedere i filmati di studenti che non sono propri. I dati sono cifrati in transito. Inoltre, terminata l'elaborazione da parte del fornitore, i dati vengono cifrati dal fornitore, fermo restando che la chiave di cifratura privata è nella disponibilità della sola Università".

Con successiva nota del XX, l'Ateneo ha fatto pervenire una nota inviata dalla società "Respondus" all'Ateneo, nella quale si afferma, in particolare, che (testo tradotto dal Garante dall'originale in inglese): non vengono generate segnalazioni basate sui dati relativi alla tempistica di svolgimento della prova nonché sui dati relativi alla pressione dei tasti sulla tastiera, al movimento del mouse e del trackpad (salvo che non siano utilizzati per passare da un'applicazione all'altra (per esempio, trascinamento con tre dita) o per uscire dal sistema, questo può comportare la generazione di un'allerta); il numero delle interruzioni e la durata di ciascuna interruzione della connessione internet hanno impatto sulla c.d. Priorità della Review.

3. Esito dell'attività istruttoria.

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

In via preliminare, si osserva 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, comma 1, della legge n. 240 del 2010, riferito sia alle università statali sia alle università non statali). Inoltre, analogamente alle università pubbliche, anche quelle private:

a) sono assoggettate alle medesime modalità di istituzione e di soppressione (disposte con decreto del Ministro dell'istruzione, dell'università e della ricerca, nell'ambito della programmazione triennale del sistema universitario ai sensi dell'art. 2, comma 5, del decreto del Presidente della Repubblica 27 gennaio 1998, n. 25);

b) sono soggette alle medesime disposizioni, in ordine alle modalità di accreditamento delle sedi e dei corsi di studio universitari (disciplinate con decreto del Ministro dell'istruzione, dell'università e della ricerca, su conforme parere dell'ANVUR, ai sensi dell'art. 7 del d.lgs. 27 gennaio 2012, n. 19);

c) hanno il potere di attribuire il medesimo valore legale ai titoli di studio rilasciati (art. 167 del r.d. 31 agosto 1933, n. 1592; art. 4, comma 3, del d.m. 22 ottobre 2004, n. 270 e art. 7, comma 1, del d.P.R. 5 giugno 2001, n. 328);

d) utilizzano le medesime modalità di reclutamento del personale docente e ricercatore, come da ultimo normate dagli artt. 18 e 24 della l. 30 dicembre 2010, n. 240 (v. anche art. 3 del d.lgs. 165/2001);

e) riconoscono al personale docente, in servizio presso le Università statali e non statali, il medesimo status giuridico, ai sensi dell'art. 6, comma 10, della l. 30 dicembre 2010, n. 240;

f) rientrano nell'ambito di applicazione del decreto del d.P.R. 27 gennaio 1998, n. 25, il quale prevede che "nel caso di soppressione di ateneo è garantito […] al personale docente e ricercatore il mantenimento del posto, anche in altra sede universitaria";

g) sono sottoposte ai poteri di indirizzo e coordinamento da parte del Ministero dell'Università e della Ricerca, ai sensi della l. 9 maggio 1989, n. 168, poteri tra cui rientra, fra l'altro, il controllo di legittimità e di merito dello statuto e dei regolamenti di ateneo (tra cui quello generale, quello didattico e quello di amministrazione e contabilità), ai sensi dell'art. 6, commi 9 e 10, della medesima l. n. 168 del 1989;

h) applicano la medesima normativa in materia di diritto allo studio, di cui al d.lgs. n. 68 del 2012.

In merito a tali profili si è di recente espresso il Consiglio di Stato, riconoscendo "il rilevantissimo interesse generale naturalmente rivestito da siffatte attività e finalità", indipendentemente dalla natura e dalla forma giuridica del soggetto che le persegue (Sezione Consultiva per gli Atti Normativi, Adunanza di Sezione del 9 maggio 2019, n. 1433/2019, che fa seguito a Sezione Consultiva per gli Atti Normativi, Adunanza di Sezione del 31 gennaio 2019, n. 370/2019).

Tanto premesso, considerato che il quadro normativo in materia di protezione dei dati previsto dal Regolamento, che non prevede un diverso regime applicabile ai soggetti pubblici e a quelli privati, 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 si ritiene che, contrariamente a quanto sostenuto originariamente dall'Ateneo, i trattamenti dei dati degli studenti finalizzati al rilascio di titoli di studio aventi valore legale o quelli connessi allo svolgimento di attività soggette alla vigilanza del Ministero dell'Università e della Ricerca non possano trovare fondamento in altre basi giuridiche quali, il consenso e/o il contratto.

In tale quadro, il titolare del trattamento è comunque tenuto a rispettare i principi in materia di protezione dei dati (art. 5 del Regolamento) e, nell'ambito della necessaria individuazione delle misure tecniche e organizzative per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento, tenuto altresì conto degli specifici rischi derivanti dal trattamento e in conformità ai principi della "protezione dei dati fin dalla progettazione" e della "protezione per impostazione predefinita"(artt. 24 e 25 del Regolamento), può ricorrere a un responsabile per lo svolgimento di alcune attività di trattamento cui impartisce specifiche istruzioni (cons. 81, artt. 4, punto 8), e 28 del Regolamento).

3.2 I trattamenti dei dati degli studenti effettuati mediante "Respondus" per la regolarità delle prove d'esame a distanza. Considerazioni generali.

Nel corso dell'istruttoria è emerso che l'Università si avvale di un sistema di supervisione a distanza delle prove d'esame scritte, denominato "Respondus" e fornito dalla società Respondus Inc. (stabilita negli Stati Uniti d'America), strutturato nelle componenti "LockDown Browser" e "Respondus Monitor" per consentire, nel contesto dell'emergenza epidemiologica da SARS-CoV-2, lo svolgimento degli esami universitari a distanza con l'obiettivo di assicurare garanzie il più possibile equivalenti a quelle previste per gli esami in presenza.

Il software Respondus Monitor 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 quali: sguardo non rivolto verso il monitor, volto parzialmente assente dalla foto, volto mancante.

Al termine della prova, il sistema elabora il video, inserendo segnali di allerta in merito a possibili indici di comportamenti scorretti (c.d. "flag") e attribuendo, fra l'altro, una c.d. "Review Priority", affinché il docente (utente supervisore) possa poi valutare se effettivamente sia stata commessa un'azione non consentita nel corso della prova.

A tal riguardo, si osserva, in via preliminare, che l'esigenza di verificare il corretto svolgimento delle prove d'esame ha assunto una maggiore rilevanza nel contesto dell'emergenza epidemiologica da SARS-CoV-2, in quanto, al fine di assicurare la continuità dell'attività didattica con modalità compatibili con le esigenze di salute pubblica, sono state privilegiate modalità "a distanza" per lo svolgimento di attività formativa e prove d'esame.

Con riguardo ai rischi per gli interessati derivanti, sotto il profilo della protezione dei dati, dall'impiego di sistemi di supervisione del comportamento degli studenti durante le prove d'esame a distanza, il Garante ha di recente evidenziato che tali sistemi "non devono essere indebitamente invasivi e comportare un monitoraggio dello studente eccedente le effettive necessità", in quanto, sebbene il necessario rispetto delle regole di svolgimento delle prove vada garantito anche online, non possono considerarsi accettabili sistemi che comportano "una sorveglianza elettronica priva dei necessari limiti e garanzie" (cfr., Memoria del Presidente del Garante del 27 aprile 2021 presso le Commissioni riunite 7a e 12a del Senato in tema di "Impatto della didattica digitale integrata (DDI) sui processi di apprendimento e sul benessere psicofisico degli studenti", doc. web n. 9581498, spec. par. 2).

In tale quadro, pertanto, le università, nello svolgimento dei propri compiti istituzionali, che implicano anche la verifica sul corretto svolgimento delle prove d'esame, anche quando siano svolte a distanza, devono rispettare i principi di protezione dei dati, verificando, in primo luogo, la sussistenza dei presupposti di liceità con riguardo agli specifici trattamenti derivanti dall'impiego dai sistemi di supervisione e assolvendo, prima dell'inizio del trattamento agli obblighi di correttezza e trasparenza nei confronti degli interessati. Ciò anche in considerazione della particolare invasività che l'impiego di tali soluzioni tecnologiche può, in taluni casi, comportare (trattamento di categorie particolari di dati; profilazione; trasferimenti internazionali dei dati).

3.3 La correttezza e la trasparenza del trattamento: l'informativa.

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

Dall'esame della documentazione in atti risulta che l'informativa sul trattamento dei dati personali fornita agli studenti (cfr. all. 5 alla nota del XX), non riporta tutte le informazioni richieste dal Regolamento per assicurare un trattamento corretto e trasparente. Il documento, che fa riferimento al trattamento dei dati biometrici e di alcuni altri dati degli studenti (nome, cognome e data di nascita), solo "a titolo esemplificativo e non esaustivo", non menziona invece gli ulteriori specifici trattamenti posti in essere mediante il sistema "Respondus", quali il tracciamento del comportamento dello studente durante la prova (posizione del viso; disconnessioni dalla rete Internet; tentativi di utilizzare il mouse o il trackpad per passare da un'applicazione all'altra o per uscire dal sistema; applicazioni in uso), le successive elaborazioni mediante profilazione, la registrazione audio-video della prova. Né vi è menzione della fotografia scattata dal sistema all'inizio della prova allo studente, cui viene chiesto di esibire un documento di identità e di effettuare una ripresa panoramica dell'ambiente circostante (cfr. all. n. 16 alla memoria difensiva, riportante la relazione tecnica del sistema).

Sul punto l'Ateneo ha dichiarato che l'informativa originariamente resa agli studenti conteneva un rinvio "attraverso specifico link ipertestuale" al testo della "informativa completa sul trattamento dei dati degli studenti" (cfr., memoria difensiva), non fornendone tuttavia evidenza nel corso dell'istruttoria.

Da verifiche puntuali (cfr. relazione di servizio dell'XX, in atti) è emerso tuttavia che il predetto collegamento ipertestuale rinvia a pagine web (https://www.unibocconi.it/privacy, che a sua volta reca un collegamento alla pagina "Informativa Studenti, Partecipanti, Alumni e Donor") che in realtà recano informazioni generiche ai trattamenti dell'Università legati alla "esperienza scolastica, accademica o professionale, al titolo della tesi, al titolo del progetto finale, alla durata degli studi e ai risultati degli esami [, nonché alla] documentazione sulla valutazione del vostro lavoro, […]", senza alcuno specifico riferimento ai trattamenti effettuati mediante il sistema "Respondus". Peraltro, anche l'informativa aggiornata in data 7 ottobre 2020, a seguito delle interlocuzioni con l'Ufficio (cfr. all. 10 alla memoria difensiva), non contiene comunque tutti gli elementi necessari per rappresentare compiutamente il trattamento.

Il testo dell'informativa originariamente resa agli interessati non indica, inoltre, gli specifici tempi di conservazione dei dati personali, limitandosi a prevedere, in modo generico, che "i dati verranno conservati per il periodo strettamente necessario al perseguimento delle finalità indicate […e] per un periodo ulteriore in caso emergano necessità di gestire eventuali contestazioni o contenziosi" (v. informativa del XX sub all. 5 alla nota del XX). Analoga generica formulazione è contenuta anche nella versione dell'informativa del XX, sebbene contenga qualche precisazione in merito al fatto che "i […] dati personali biometrici, che non sono trattati e conservati

dall'università, saranno cancellati immediatamente da Respondus Inc al termine di ogni prova di esame" (v. all. 10 alla memoria difensiva).

A tal riguardo, si evidenzia che "non è sufficiente che il titolare del trattamento affermi in maniera generica che i dati personali saranno conservati finché sarà necessario per le finalità legittime del trattamento", dovendosi fissare "periodi di conservazione diversi per le diverse categorie di dati personali e/o finalità del trattamento, inclusi, se del caso, i periodi di archiviazione" ("Linee guida sulla trasparenza ai sensi del regolamento 2016/679" dell'11 aprile 2018, WP260 rev.01, fatte successivamente proprie dal Comitato europeo per la protezione dei dati). Sul punto il titolare del trattamento ha, infatti, dichiarato che "per ciò che attiene al periodo di conservazione, in effetti, la Bocconi riconosce che l'informativa potrebbe potenzialmente difettare di trasparenza, non essendo indicato un periodo di conservazione specifico" (cfr. memoria difensiva in atti).

Sempre sotto il profilo della correttezza e trasparenza del trattamento, l'informativa non menziona che i dati personali sono oggetto di trasferimento negli Stati Uniti d'America, limitandosi genericamente a prevedere che "i […] dati personali saranno trattati dal Titolare all'interno e all'esterno del territorio dell'Unione Europea", né è specificato il presupposto del trasferimento, ovvero – al tempo – la Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy (Privacy Shield), non essendo gli studenti edotti né dello specifico Paese terzo di destinazione dei dati né delle particolari garanzie adottate per tale trasferimento, essendo tali garanzie elencate solo a tiolo esemplificativo. Peraltro anche nella successiva versione dell'informativa del XX (cfr. all. 10 alla memoria difensiva), non viene indicato lo specifico Paese terzo di destinazione dei dati (gli Stati Uniti d'America). A tal riguardo, le Linee guida sopra citate chiariscono che "dovrebbe essere specificato l'articolo del regolamento che consente il trasferimento e il meccanismo corrispondente […] [, anche fornendo] informazioni su dove e come accedere al documento pertinente od ottenerlo, ad es. fornendo un collegamento al meccanismo utilizzato. Conformemente al principio di correttezza, le informazioni fornite sui trasferimenti a paesi terzi dovrebbero essere il più pregnanti possibile per gli interessati. In genere, ciò significa indicare il nome dei paesi terzi".

Si rileva, inoltre, che, sebbene il trattamento in questione non si risolva in un processo decisionale interamente automatizzato (cfr. art. 22 del Regolamento), l'informativa resa agli interessati non esplicita la logica su cui si basa il funzionamento del sistema di supervisione (cfr. art. 5, par. 1, lett. a), del Regolamento). non essendo chiarite le diverse funzionalità del sistema e i meccanismi che comportano la generazione dei segnali di allarme/anomalia, né sono rese note l'importanza e le conseguenze per l'interessato nel caso in cui vengano posti in essere determinati comportamenti nel corso dello svolgimento della prova.

La necessità di assicurare la correttezza e la trasparenza del trattamento impone che l'interessato sia "informato della esistenza di una profilazione e delle conseguenze della stessa" (cons. 60 del Regolamento) e che, indipendentemente dagli specifici obblighi di trasparenza applicabili al processo decisionale automatizzato (artt. 13, par. 2, lett. f), e 14, par. 2, lett. g) del Regolamento), "l'importanza d'informare gli

interessati delle conseguenze del trattamento […] e il principio generale secondo cui questo trattamento non dovrebbe cogliere di sorpresa l'interessato si applicano parimenti alla profilazione in generale, non solo a quella descritta all'articolo 22" (v., "Linee guida sulla trasparenza ai sensi del regolamento 2016/679" dell'11 aprile 2018, WP260 rev.01; in generale, sulla necessità che gli interessati vengano debitamente informati in merito allo "schema esecutivo dell'algoritmo e gli elementi di cui si compone", v. Cass. civ. Sez. I, Ord., 25 maggio 2021, n. 14381, che ha confermato un precedente provvedimento del Garante).

Né può ritenersi sufficiente che "i rappresentati degli Studenti […], già prima dell'implementazione di Respondus, [fossero stati] informati del nuovo processo e delle funzionalità dello stesso" (par. 3.3 della memoria difensiva), atteso che le informazioni sul trattamento dei dati personali devono essere "fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici" individualmente a ciascun interessato. L'aver illustrato le funzionalità del sistema ai soli rappresentati degli studenti non risulta, invece, idoneo a rendere edotti individualmente gli interessati con riguardo a tutte le operazioni di trattamento effettuate. Peraltro, l'informativa può essere resa oralmente solo se richiesto dall'interessato (cfr. art. 12 del Regolamento). Anche la "procedura interna per lo svolgimento delle prove d'esame online, diffusa tra gli Studenti e il corpo docente" (par. 3.3 della memoria difensiva e all. 13 denominato "Linee guida esami online scritti" che, peraltro, nella versione in atti, riporta la data del XX), comunque non idonea ad assolvere l'obbligo di informare gli interessati ai sensi dell'art. 13 del Regolamento, si limita a illustrare aspetti tecnici e procedurali relativi allo svolgimento delle prove ad esame a distanza, senza illustrare la logica su cui si basa il sistema di supervisione "Respondus".

In ogni caso, in relazione all'affermazione che gli studenti avrebbero "ricevuto, per tempo, diverse istruzioni e chiarimenti ben prima dell'avvio del trattamento, con informazioni multilayer", si osserva che l'approccio di fornire agli interessati informative stratificate è utile ai fini del rispetto del principio di trasparenza solo se le informazioni di primo e di secondo livello sono presentate tra loro in maniera coerente e strutturata, consentendo agli interessati di conoscere gli elementi essenziali del trattamento nella prima informativa di primo livello, potendo poi scegliere di approfondire determinati aspetti nelle informative di dettaglio (sul punto, "Linee guida sulla trasparenza ai sensi del regolamento 2016/67" adottate l'11 aprile 2018, WP260 rev.01, par. 35, successivamente fatte proprie dal Comitato europeo per la protezione dei dati con "Endorsement 1/2018" del 25 maggio 2018: "le dichiarazioni/informative sulla privacy non sono mere pagine annidiate in altre che richiedono diversi clic per arrivare all'informazione voluta: il design e il layout del primo strato della dichiarazione/informativa sulla privacy dovrebbe essere tale da offrire all'interessato una panoramica chiara delle informazioni a sua disposizione sul trattamento dei dati personali e del luogo e del modo in cui può trovarle fra i diversi strati"). Nel caso di specie, invece, le diverse informazioni agli studenti – che sono in ogni caso carenti con riguardo alla logica sottostante allo strumento utilizzato – sono state presentate in maniera frammentaria e disorganica (e talvolta, come nel caso delle indicazioni impartite oralmente, non documentabile), senza coerenti rimandi tra i diversi documenti (ad esempio, l'informativa sul trattamento dei dati personali non menziona affatto la procedura "Linee guida esami online scritti").

Per tutte le ragioni sopra rappresentate, il trattamento posto in essere dall'Ateneo non può ritenersi conforme al principio di liceità, trasparenza e correttezza non essendo stati forniti tutti gli elementi informativi previsti dal Regolamento (art. 5, par. 1, lett. a), e 13 del Regolamento).

3.4 L'assenza di base giuridica per il trattamento di dati biometrici degli studenti.

In risposta all'iniziale richiesta d'informazioni del Garante, l'Ateneo ha dichiarato di aver strutturato "un processo che […] unicamente per le prove d'esame scritte, fosse in grado di identificare gli Studenti attraverso l'utilizzo temporaneo del loro dato biometrico e, dunque, elaborando automaticamente le immagini digitali che raffigurano il volto degli stessi a fini di identificazione, autenticazione e verifica", con ciò, pertanto, confermando che l'utilizzo del sistema implicasse il trattamento di "dati biometrici" (art. 4, par. 1, n. 14), del Regolamento).

In seguito, l'Ateneo ha rettificato le proprie dichiarazioni, affermando, nella memoria difensiva, nonché in sede di audizione, che a seguito di approfondimenti con il fornitore il sistema non comporta il trattamento di dati biometrici degli interessati. Nella relazione tecnica allegata alla memoria difensiva (all. 16), inoltre, si afferma che "il video della webcam viene analizzato utilizzando la tecnologia di Respondus, senza estrazione di campione biometrico" e che "diversi eventi segnalati dipendono in larga misura dalla tecnologia di rilevamento facciale, che non comporta in alcun caso l'estrazione di un campione biometrico".

Si rileva, anzitutto, che, contrariamente a quanto sostenuto dall'Ateneo, Respondus, Inc. ha affermato che un template biometrico viene comunque generato, avendo precisato che "non c'è corrispondenza del template biometrico temporaneo con nessuna persona identificata in nessun database interno o esterno" (cfr. nota di Respondus all'Ateneo del XX, sub all. 12 alla memoria difensiva).

Da quanto emerge dagli atti, in merito al funzionamento dell'applicativo, è possibile affermare che il software Respondus Monitor effettua un trattamento tecnico specifico di una caratteristica fisica degli interessati per confermare la presenza e la coincidenza dell'interessato per tutta la durata della prova. Seppur il sistema non comporta l'identificazione del candidato – nonostante fra le azioni preliminari di LockDown Browser sia previsto che lo studente scatti una propria foto con le funzionalità interne a LockDown Browser ed esibisca un documento identificativo (cfr. relazione tecnica sub all. 16 alla memoria difensiva) – e non confronti l'immagine del volto con altre immagini presenti in propri database e in database esterni, ovvero non effettui una identificazione (1 a molti) o verifica biometrica (uno a uno), il sistema effettua comunque un trattamento di dati biometrici che consiste nella raccolta, elaborazione e analisi del video prodotto dal software tramite un algoritmo di intelligenza artificiale al fine di produrre i "flag".

Per tale motivo, tenuto anche conto di quanto già affermato dall'Autorità in casi analoghi, "nel caso del riconoscimento facciale, il presupposto perché il trattamento delle immagini possa essere qualificato come trattamento biometrico è che i confronti finalizzati al riconoscimento dell'individuo (verifica dell'identità, nel caso in esame) siano automatizzati mediante l'ausilio di appositi strumenti software o hardware"

(provv. 26 luglio 2017, n. 345, doc. web n. 6826368). Per tali ragioni, stante la definizione di dati biometrici (art. 4, par. 1, n. 14, del Regolamento: "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"), si ritiene che l'utilizzo effettuato dall'Università Bocconi tramite il software Respondus comporti il trattamento di dati biometrici relativi all'immagine del volto degli studenti. Tale circostanza trova conferma dell'informativa sul trattamento dei dati personali, nella versione del XX (v. all. 10 alla memoria difensiva "i […] dati personali biometrici, che non sono trattati e conservati dall'università, saranno cancellati immediatamente da Respondus Inc al termine di ogni prova di esame").

Ciò chiarito, 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. provv. n. 16 del 14 gennaio 2021, 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 aveva identificato nel consenso dello studente la base giuridica del trattamento dei dati biometrici trattati mediante il sistema "Respondus". Tuttavia, come già precisato al precedente par. 3.1, considerato che il trattamento è stato effettuato dall'Ateneo ai fini del rilascio di titoli di studio aventi valore legale, contrariamente a quanto sostenuto dall'Ateneo (cfr. parere del RPD e punto 2.4., 3.1 e 5.1 della valutazione d'impatto sulla protezione dei dati, in atti), il consenso non costituisce la base giuridica del trattamento né può ritenersi una "manifestazione di volontà libera" (art. 4, par. 1, n. 11) del Regolamento), in ragione dello squilibrio della posizione degli studenti rispetto al titolare del trattamento (cfr. considerando n. 43 del Regolamento).

Sebbene, infatti, solo in sede di audizione, l'Ateneo abbia dichiarato che"la direzione Academic Services, consultato il docente, ha […] trovato delle soluzioni alternative [allo svolgimento della prova mediante il sistema in questione] pur in costanza dello stato di emergenza (orale o scritto con videoconferenza e proctoring individuale)", con il comunicato del XX, allegato al reclamo, gli studenti sono stati avvertiti che "in assenza del rilascio del […] consenso, non sarà possibile sostenere le prove d'esame online", prospettando come unica alternativa l'effettuazione dell'esame in presenza con modalità da concordare con il docente (v anche par. 5 dell'informativa del 24 aprile 2020: "l'eventuale rifiuto di prestare il consenso per il trattamento dei dai biometrici […] comporterà l'impossibilità di sostenere l'esame in modalità online e a distanza. Potrai, pertanto, sostenere la prova d'esame unicamente dal vivo, alla presenza reale e non virtuale del docente di riferimento, presso le sedi dell'Università"). Ciò, tenuto conto del contesto emergenziale derivante dalla diffusione del virus SARS-CoV-2 può, da un lato, esporre docenti e studenti a un più elevato rischio per la salute nel contesto epidemiologico e, dell'altro, può ingenerare

nello studente il timore di subire ripercussioni negative, anche indirette, da parte dei docenti come conseguenza del rifiuto (cfr. punto 3.1 delle "Linee guida 5/2020 sul consenso ai sensi del regolamento(UE) 2016/679" adottate dal Comitato europeo per la protezione dei dati il 4 maggio 2020).

Stante l'impossibilità di far ricorso al consenso, il trattamento dei dati biometrici effettuati dall'Ateneo, riconducibili allo svolgimento di compiti di interesse pubblico, è consentito solo nella misura in cui sia "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" (art. 9, par. 2, lett. g), del Regolamento; art. 2-sexies, comma 2, lett. bb) del Codice ha definito "rilevante" l'interesse pubblico per il trattamento effettuato per finalità di "istruzione e formazione in ambito scolastico, professionale, superiore o universitario"). Nel margine di flessibilità concesso al legislatore nazionale, l'art. 2-sexies del Codice ha specificato le condizioni, richieste dall'art. 9, par. 1, lett. g), del Regolamento, delimitando i presupposti di legittimità del trattamento, quando sono necessari per motivi di interesse pubblico rilevante, alla sussistenza di una previsione normativa che deve specificare, oltre al motivo di interesse pubblico rilevante, tra l'altro, i tipi di dati, le operazioni eseguibili, le misure appropriate per tutelare i diritti degli interessati.

In tale quadro, quindi, affinché uno specifico trattamento avente a oggetto dati biometrici possa essere lecitamente iniziato è necessario che lo stesso trovi il proprio fondamento in una disposizione normativa che abbia le caratteristiche richieste dalla disciplina di protezione dei dati in termini di qualità della fonte, contenuti necessari e rispetto del principio di proporzionalità (art. 6, par. 3, del Regolamento; sul punto, ancorché con riguardo a un diverso contesto di trattamento cfr. provv. n. 16 del 14 gennaio 2021, doc. web n. 9542071). Tali elementi, allo stato, non sono stati individuati da alcuna legge o regolamento di settore né dalle diposizioni dell'emergenza.

Per tali ragioni, atteso che nell'ordinamento vigente non si rinviene – né l'Ateneo ha, invero, individuato – una disposizione normativa che espressamente autorizzi il trattamento dei dati biometrici per le finalità di verifica della regolarità delle prove d'esame, il trattamento dei dati biometrici in questione risulta avvenuto in assenza di idonea base giuridica, in violazione degli artt. 5, 6 e 9 del Regolamento e dell'art. 2-sexies, comma 1, del Codice.

3.5 L'analisi del comportamento degli studenti nel corso della prova d'esame.

Come risulta dall'esame della documentazione in atti, il sistema di supervisione "Respondus", nella componente denominata "Respondus Monitor", è dotato di funzionalità e meccanismi che comportano la generazione di segnali di allarme (c.d. "flag") al fine di rilevare anomalie del comportamento dello studente durante la prova per verificarne la correttezza e la conseguente regolarità. In particolare, il documento denominato "RespondusFeedback" (cfr. all. alla nota del XX, cit.) illustra taluni esempi di reportistica restituita dal software sulla base dell'analisi del comportamento dello studente durante della prova (es. posizione dello studente rispetto alla web cam,

disconnessioni dalla rete Internet, applicazioni in uso, e movimenti del mouse per passare da un'applicazione all'altra o per uscire dal sistema), consentendo al docente di visualizzare i fotogrammi rispetto ai quali il sistema abbia evidenziato una presunta anomalia (v. documento "Additional Privacy Information – Respondus Monitor", pubblicato sul sito web di Respondus, all. 11 alla memoria difensiva, nella versione dell'XX, ove si legge, in particolare, che "Respondus Monitor traccia continuamente le applicazioni e i processi che sono in esecuzione sul dispositivo informatico durante una sessione di esame"; relazione tecnica sub. all. 16 alla memoria difensiva; nota di Respondus del XX, allegata alla nota dell'Ateneo del XX, con la quale sono stati precisate le tipologie di eventi anomali rilevati dal sistema).

Nel riepilogo mostrato al docente figura l'indice "Review Priority", "che indica se la sessione d'esame di uno studente richiede attenzione maggiore da parte del docente. I risultati vengono rappresentati nelle categorie Basso (LOW), Medio (MEDIUM) e Alto (HIGH) con un grafico a barre da verde a rosso che indica il livello di rischio"; il valore "Review Priority deriva da tre fonti di dati: il video della webcam dello studente; il dispositivo informatico e la rete utilizzati per la prova; l'interazione dello studente con la prova […]" tenendo conto di vari indici di anomalia quali, ad esempio, le interruzioni del video, il riavvio automatico di una sessione della webcam, i tentativi di cambiare applicazione; diverse anomalie, inoltre, "dipendono in larga misura dalla tecnologia di rilevamento facciale" che è in grado di segnalare l'assenza del candidato o la sostituzione di persona (v. relazione tecnica cit.).

Alla luce del complesso degli elementi emersi nel corso dell'istruttoria e pur tenendo conto delle rettifiche e delle precisazioni dell'Ateneo, si ritiene che le funzionalità della componente "Respondus Monitor", che determinano un trattamento parzialmente automatizzato per l'analisi del comportamento degli interessati, in funzione della successiva valutazione del docente, diano comunque luogo a una "profilazione" degli studenti (art. 4, par. 1, n. 4, del Regolamento), intesa come l'operazione di trattamento automatizzato di dati personali "per valutare aspetti personali relativi a una persona fisica" e, in particolare, come nel caso in esame, per analizzare aspetti riguardanti il comportamento o l'affidabilità dell'interessato (art. 4, n. 4, del Regolamento).

Specialmente nel contesto dell'esercizio di compiti di interesse pubblico, come nel caso in esame, occorre tenere conto degli specifici rischi derivanti dalla profilazione, che, generando informazioni nuove e ulteriori da quelle fornite dall'interessato o altrove acquisite, può talvolta comportare conseguenze pregiudizievoli per l'interessato, quali, in generale, l'esclusione da benefici, il mancato accesso a beni e servizi o, come in questo caso, l'annullamento di una prova d'esame, in violazione del principio di non discriminazione. Pertanto, il trattamento in questione, per essere lecito, oltre a dover essere chiaramente rappresentato agli interessati, deve essere, in questo contesto, necessario per l'esecuzione di un compito di interesse pubblico e deve quindi essere previsto da una norma di legge o di regolamento (art. 6, par. 1, lett. e), e par. 3, e cons. 72 del Regolamento, art. 2-ter del Codice) che, nel caso di specie però non sussiste.

Per tali ragioni, si ritiene che i descritti trattamenti consistenti nell'analisi del comportamento degli studenti nel corso della prova d'esame il trattamento dei dati

personali degli studenti è stato effettuato in violazione degli artt. 5, par. 1, lett. a) e 6 del Regolamento.

3.6 Protezione dei dati fin dalla progettazione e per impostazione predefinita, minimizzazione e limitazione della conservazione.

In disparte dal rilevo dell'assenza della base giuridica del trattamento, dalla documentazione in atti si evince che il sistema di supervisione "Respondus" non si limita a inibire specifiche funzionalità dei dispositivi in uso agli studenti nel corso dello svolgimento dell'esame (mediante l'utilizzo della sola funzione c.d. "LockDown Browser"). Attraverso l'estensione "Respondus Monitor", il sistema tiene traccia del comportamento dello studente durante la prova (disconnessioni dalla rete Internet; tentativi di utilizzare il mouse o il trackpad per passare da un'applicazione all'altra o per uscire dal sistema; applicazioni in uso; posizione del viso dello studente), generando una pluralità di informazioni e dati personali relativi allo studente e alla sua condotta, il cui trattamento non risulta strettamente necessario per assicurare il regolare svolgimento e la validità della prova. Peraltro, talune di tali informazioni, come nel caso delle applicazioni in uso sul terminale dello studente, sono potenzialmente idonee a rivelare aspetti relativi alla sua vita privata.

Anche in considerazione del rischio che incombe sui diritti e le libertà degli interessati, il titolare del trattamento, anche avvalendosi del supporto del responsabile della protezione dei dati, deve "fin dalla progettazione" e "per impostazione predefinita" (art. 25 del Regolamento) adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del Regolamento), quali i principi di minimizzazione e di limitazione della conservazione di cui agli artt. 5, par. 1, lett. c) e e), del Regolamento) e integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati (cfr. "Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate il 20 ottobre 2020 dal Comitato europeo per la protezione dei dati, spec. punti 42, 44 e 49). Ciò anche quando il titolare del trattamento utilizza prodotti o servizi realizzati da terzi, impartendo se del caso le necessarie istruzioni al fornitore del servizio e assicurandosi che siano, ad esempio, disattivate le funzioni che non abbiano una base giuridica ovvero non siano compatibili con le finalità del trattamento (cfr., in particolare, con riguardo al trattamento di dati di utenti e dipendenti mediante un sistema di prenotazione di servizi allo sportello, provv. 17 dicembre 2020, n. 282, doc. web n. 9525337, ma già provv. 7 marzo 2019, n. 81, doc. web n. 9121890).

Considerato inoltre che i dati personali devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati" (art. 5, par. 1, lett. e), del Regolamento), si osserva che, con riguardo ai tempi di conservazione delle registrazioni audio-video delle prove d'esame (ovvero cinque anni dalla data della prova – cfr. par. 3.5 della valutazione d'impatto sub all. 3 alla nota del XX –, poi riformulati dall'Ateneo in dodici mesi successivamente alla contestazione amministrativa – cfr. memoria difensiva), il titolare non ha fornito le specifiche motivazioni sulla cui base si renderebbe necessaria la conservazione dei dati per un così esteso lasso temporale. Sul punto si fa presente, in ogni caso, che tale periodo di

conservazione non risulta proporzionato rispetto alla finalità di assicurare la regolarità delle prove d'esame. Né tale ampio arco temporale può essere giustificato per l'ulteriore finalità legata all'utilizzo dei medesimi dati in caso di eventuali contestazioni da parte degli interessati, considerati i termini previsti dalla legge per impugnare l'esito della prova (reclamo alla commissione esaminatrice ovvero ricorso al TAR).

Come tradizionalmente affermato dal Garante, il trattamento di dati effettuato per finalità di tutela dei propri diritti, anche in giudizio, come si afferma nell'informativa resa agli studenti, deve, infatti, riferirsi a contenziosi in atto o a situazioni precontenziose, e non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti (tale principio generale è stato, da ultimo, ribadito dal Garante, sebbene in un contesto diverso, nel "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101", all. 1, par. 1.3, lett. d), doc. web n. 9124510; v. anche provv. 8 marzo 2018, n. 139, doc. web n. 8163433, par. 4.1). Anche sul piano europeo, sebbene in materia di trasferimenti internazionali di dati personali, il Comitato europeo per la protezione dei dati ha affermato che "non è ammesso il ricorso alla deroga [al generale divieto di trasferimento] per giustificare il trasferimento di dati personali sulla base della mera possibilità di eventuali procedimenti giudiziari o procedure formali in futuro" ("Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679" adottate il 25 maggio 2018), così confermando che il trattamento dei dati per finalità di tutela dei propri diritti in giudizio non può dipendere dalla possibilità di un contenzioso meramente eventuale.

Quanto alla circostanza che, come dichiarato dall'Ateneo, la valutazione d'impatto sulla protezione dei dati personali, ove è indicato il periodo di conservazione di cinque anni, debba essere letta congiuntamente con le previsioni dell'accordo sul trattamento dei dati stipulato con il fornitore, ai sensi del quale il titolare del trattamento può chiedere in qualsiasi momento al fornitore di cancellare i dati, e che, sulla base di dette previsioni, "la Bocconi, infatti, chiede che venga effettuata le descritta cancellazione non decorsi cinque anni dalla data di espletamento della prova, bensì una volta che si è formalmente chiusa la sessione d'esame e si è perfezionato […] il procedimento di valutazione delle prove sostenute dagli studenti" (cfr. memoria difensiva), si osserva che, nel rispetto del principio di responsabilizzazione, i tempi di conservazione dei dati devono essere fissati ex ante dal titolare del trattamento in maniera certa e documentabile (cfr. art. 5, par. 2, 24 e 25 del Regolamento). Diversamente, il titolare del trattamento non potrebbe informare gli interessati in merito ai tempi di conservazione dei dati prima di dar luogo al trattamento (cfr. artt. 13, par. 2, lett. a) e 14, par. 2, lett. a) del Regolamento) e, nell'ambito della valutazione d'impatto sulla protezione dei dati, come nel caso di specie, non potrebbe effettuare una compiuta "valutazione delle necessità e proporzionalità dei trattamenti in relazione alle finalità" (art. 35, par. 7, lett. b) del Regolamento), anche con riguardo alla "limitazione della conservazione (articolo 5, paragrafo 1, lettera e))" ("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" del Gruppo di lavoro art. 29, adottate il 4 ottobre 2017, WP 248 rev.01, fatte proprie dal Comitato europeo per la protezione dei dati con "Endorsement 1/2018" del 25 maggio 2018).

Con riguardo all'affermazione dell'Ateneo per cui "la registrazione video non viene archiviata in chiaro sui sistemi informativi dell'Università […] [, essendo il] video […], fino alla sua cancellazione, conservato in maniera completamente crittografata sui server del fornitore" (cfr. memoria difensiva), si rileva che, seppure i dati in questione risiedano sui sistemi informatici del fornitore, che quindi tratta i dati per conto e nell'interesse del titolare (cfr. cons. 81, artt. 4, punto 8), e 28 del Regolamento), è comunque su quest'ultimo che grava la "responsabilità generale" (cons. 74 del Regolamento) connessa al trattamento (cfr. artt. 5, par. 2, e 24 del Regolamento), anche per quanto concerne la definizione certa dei tempi di conservazione dei dati (cfr. art. 5, par. 2, del Regolamento, ai sensi del quale "il titolare del trattamento è competete per il rispetto del paragrafo 1", ovvero dei principi applicabili al trattamento di dati personali, tra i quali il principio di limitazione della conservazione).

Per le ragioni rappresentate, il trattamento dei dati personali degli studenti risulta effettuato in maniera non conforme ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, minimizzazione e limitazione della conservazione, in violazione degli artt. 5, par. 1, lett. c) ed e) e 25 del Regolamento.

3.7 Trasferimenti internazionali di dati personali

Come emerso dall'istruttoria, il sistema di supervisione utilizzato dall'Ateneo è fornito da Respondus, Inc., società stabilita negli Stati Uniti d'America, che tratta i dati personali in qualità di responsabile del trattamento, sulla base di un accordo sul trattamento dei dati personali ("Appointment of an External Data Processor under Regulation (EU) 2016/679"), stipulato tra le parti in data XX ai sensi dell'art. 28 del Regolamento.

A tal proposito, in generale, si osserva che i trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo sono consentiti a condizione che l'adeguatezza del Paese terzo sia stata riconosciuta da una decisione della Commissione europea (cfr. artt. 44 e 45 del Regolamento). In assenza di una tale decisione, il trasferimento è consentito a condizione che il titolare del trattamento fornisca garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 del Regolamento). Al riguardo, possono costituire garanzie adeguate, tra le altre, le clausole tipo di protezione dei dati adottate dalla Commissione europea (art. 46, par. 2, lett. c), del Regolamento).

In assenza di ogni altro presupposto, è possibile trasferire i dati personali in base ad alcune deroghe che si verificano in talune specifiche ipotesi (art. 49 del Regolamento), che devono essere interpretate restrittivamente e che possono applicarsi solo in caso di trasferimenti occasionali e non ripetitivi (cfr. le "Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679", adottate il 25 maggio 2018 dal Comitato europeo per la protezione dei dati).

Con riferimento al trasferimento dei dati personali negli Stati Uniti d'America, la Corte di Giustizia dell'Unione Europea, con sentenza del 16 luglio 2020 (Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems, Causa C-311/18), ha dichiarato invalida la decisione relativa al c.d. scudo per la privacy (Privacy Shield) (Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12

luglio 2016 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy), in considerazione del fatto che il diritto interno degli Stati Uniti d'America (in particolare l'art. 702 del Foreign Intelligence Surveillance Act – FISA e l'Executive Order 12333) – consentendo alle autorità pubbliche, nel quadro di determinati programmi di sicurezza nazionale, di accedere senza adeguate limitazioni ai dati personali oggetto di trasferimento ai fini della sicurezza nazionale – non garantisce un livello di tutela sostanzialmente equivalente a quello riconosciuto dal diritto europeo e non accorda, ai soggetti interessati, diritti azionabili in sede giudiziaria nei confronti delle autorità statunitensi.

La Corte ha, altresì, esaminato la validità della Decisione della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi, e ne ha ritenuto la validità, sul presupposto che tali clausole mirano unicamente a fornire garanzie contrattuali che si applicano in modo uniforme in tutti i paesi terzi, indipendentemente dal livello di protezione garantito in ciascuno di essi. Tuttavia, poiché tali clausole, tenuto conto della loro natura, non forniscono garanzie che vadano al di là di un obbligo contrattuale di rispettare il livello di protezione richiesto dal diritto dell'Unione europea, "esse possono richiedere, in funzione della situazione esistente nell'uno o nell'altro paese terzo, l'adozione di misure supplementari da parte del titolare del trattamento al fine di garantire il rispetto di tale livello di protezione" (par. 133 della sentenza). Incombe pertanto sul titolare del trattamento l'obbligo di verificare, caso per caso, ed eventualmente in collaborazione con il destinatario del trasferimento, se il diritto del Paese terzo di destinazione garantisce una protezione adeguata, alla luce del diritto dell'Unione europea, dei dati personali che sono oggetto di trasferimento fornendo, se necessario, garanzie supplementari rispetto a quelle offerte dalle clausole tipo. Qualora non sia possibile adottare tali misure supplementari, è necessario "sospendere o mettere fine al trasferimento di dati personali verso il paese terzo interessato" (par. 135 della sentenza). Tale ipotesi ricorre, in particolare, "nel caso in cui il diritto di tale paese terzo imponga al destinatario di un trasferimento di dati personali proveniente dall'Unione obblighi in contrasto con dette clausole e, pertanto, atti a rimettere in discussione la garanzia contrattuale di un livello di protezione adeguato contro l'accesso delle autorità pubbliche di detto paese terzo a tali dati" (ibidem).

L'art. 8.2 dell'accordo sulla protezione dei dati stipulato tra l'Ateneo e Respondus, Inc. prevede che "il Titolare del Trattamento autorizza il Responsabile del Trattamento a trattare o trasferire i dati fuori dall'Unione europea, a condizione che il Responsabile del Trattamento garantisca che sussistano dei meccanismi che possano assicurare un adeguato livello di protezione e che gli interessati dispongano di diritti azionabili ed effettivi mezzi di impugnazione".

Il trasferimento dei dati personali, relativi agli studenti e al personale dell'Ateneo, a Respondus, Inc. è stato effettuato sul presupposto che, come affermato nella nota dell'Ateneo del XX, Respondus, Inc. "dichiara e garantisce, per mezzo della propria privacy policy pubblicata al seguente indirizzo telematico https://web.respondus.com/gdpr-privacy-shield/, di aderire al Privacy Shield", secondo quanto previsto dalla Decisione di esecuzione (UE) 2016/1250 della Commissione

europea, del 12 luglio 2016 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy.

In conseguenza della citata sentenza della Corte di Giustizia dell'Unione Europea del 16 luglio 2020 (Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems, Causa C-311/18), con la quale è stata invalidata la predetta Decisione di esecuzione (UE) 2016/1250, l'Ateneo ha stipulato con Respondus, Inc., in data 18 agosto 2020, un atto aggiuntivo all'accordo sulla protezione dei dati, denominato "Amendment to Appointment of an External Data Processor under Regulation (EU) 2016/679". Tale atto riporta, in allegato, le clausole tipo di protezione dei dati di cui alla Decisione della Commissione del 5 febbraio 2010 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi, recanti la data del 20 agosto 2020.

L'Appendice n. 2 alle clausole contrattuali tipo (Appendix 2) prevede che "l'importatore dei dati dovrà mettere in atto misure amministrative, fisiche e tecniche per la protezione della sicurezza, la confidenzialità e l'integrità dei Dati Personali caricati per l'utilizzo dei prodotti concessi in licenza" e che "i dettagli relativi a tali misure sono disponibili sul modulo Monitor Hecvat di Respondus, che è consultabile su richiesta al seguente indirizzo: https://web.respondus.com/hecvat/" ("details regarding these safeguards are available on the Respondus Monitor HECVAT form, which is available upon request via URL: https://web.respondus.com/hecvat").

Al riguardo, si osserva che la descrizione delle misure tecniche e organizzative di sicurezza, effettuata con tali modalità, non risulta tuttavia idonea a soddisfare quanto previsto dall'art. 4, par. 1, lett. c) delle clausole contrattuali tipo, ai sensi del quale, "l'esportatore dichiara e garantisce […] che l'importatore fornirà sufficienti garanzie per quanto riguarda le misure tecniche e organizzative di sicurezza indicate nell'appendice 2", specificandosi, alla successiva lett. d), che "alla luce della normativa sulla protezione dei dati, le misure di sicurezza sono atte a garantire la protezione dei dati personali […]" (specularmente, l'art. 5, lett. c), delle clausole standard prevede che "l'importatore dichiara e garantisce quanto segue: […] c) di aver applicato le misure tecniche e organizzative di sicurezza indicate nell'appendice 2 prima di procedere al trattamento dei dati personali trasferiti"). Ciò in particolare tenuto conto che tali misure tecniche e organizzative non risultano allegate al contratto sottoscritto, essendo rese disponibili, solo su richiesta attraverso un modulo di richiesta online, e non essendovi alcuna certezza in merito a quali misure siano effettivamente adottate dall'importatore, con riguardo allo specifico trasferimento, potendo le stesse variare nel tempo (peraltro senza che l'esportatore ne abbia necessariamente contezza), e non essendo chiaramente individuato l'obbligo contrattualmente assunto dall'importatore in materia di sicurezza.

Non può, peraltro, accogliersi la tesi difensiva dell'Ateneo, secondo la quale l'Università era comunque "ben consapevole delle misure approntate dal fornitore" e che tali misure erano "allegate alla stessa DPIA [ovvero alla valutazione d'impatto sulla protezione dei dati]", sussistendo una "relatio solo formale […] perché la determinazione delle misure fa riferimento ad un elemento che, seppur esterno all'accordo, è noto ad entrambe le parti". Deve, infatti, considerarsi che gli artt. 4, par. 1, lett. c) e 5, lett. c) delle clausole standard, sopra richiamati, prevedono

espressamente che le misure di sicurezza debbano essere “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 all.)”.

Nella documentazione fornita, invece, le misure tecniche e organizzative non stato state specificamente descritte, essendo soltanto indicato che esse possono essere ottenute dal titolare su richiesta. Occorre, altresì, considerare che, ai sensi dell’art. 3, par. 1, delle clausole contrattuali tipo allegate alla decisione della Commissione Europea 2010/87/UE, “l’interessato può far valere, nei confronti dell’esportatore, […] la clausola 4, lettere da b) a i), la clausola 5, lettere da a) ad e) […] in qualità di terzo beneficiario”, inclusi, dunque, gli artt. art. 4, par. 1, lett. c) e 5, lett. c) sopra richiamati.

È pertanto evidente che, non avendo le parti indicato con certezza, nell’appendice 2 alle clausole standard, le specifiche misure di sicurezza da adottare, gli interessati, in quanto terzi beneficiari, non possono far valere gli impegni assunti contrattualmente in materia di sicurezza nei confronti dell’esportatore, in violazione di quanto previsto dall’art. 3, par. 1, sopra richiamato, essendo a tal fine irrilevante che le misure di sicurezza da adottare fossero comunque note alle parti stipulanti le clausole standard.

Sotto altro profilo, con riferimento a quanto considerato dalla Corte di giustizia nella citata sentenza del 16 luglio 2020, non risulta dalla documentazione in atti che l’esportatore abbia effettuato una valutazione circa l’effettiva capacità delle misure adottate a garantire il rispetto degli obblighi assunti dall’importatore con la sottoscrizione delle predette clausole, alla luce della legislazione del paese terzo in cui i dati devono essere trasferiti.

In particolare, considerato che i dati personali sono oggetto di trasferimento verso gli Stati Uniti d’America, un Paese terzo il cui diritto interno, come stabilito nella predetta sentenza della Corte di Giustizia, non garantisce un livello di tutela sostanzialmente equivalente a quello riconosciuto dal diritto europeo e non accorda ai soggetti interessati diritti azionabili, in sede giudiziaria nei confronti delle autorità statunitensi, l’Ateneo, nell’ambito della stipula delle clausole contrattuali tipo, avrebbe dovuto espressamente valutare e prevedere, se del caso, “l’adozione di misure supplementari da parte del titolare del trattamento al fine di garantire il rispetto di tale livello di protezione” (par. 133 della sentenza), valutazione di cui non vi è alcuna evidenza nella documentazione contrattuale stipulata con Respondus, Inc. e fornita al Garante.

Al riguardo si rappresenta che, come chiarito nelle “Raccomandazioni 01/2020 sulle misure che integrano gli strumenti di trasferimento per assicurare il rispetto con il livello di protezione dei dati personali dell’Unione europea”, adottate dal Comitato europeo per la protezione dei dati personali in data 10 novembre 2020, nel caso in cui il diritto interno del Paese in cui è stabilito l’importatore (nel caso di specie gli Stati Uniti d’America) imponga a quest’ultimo degli obblighi che sono in contrasto con quelli previsti a suo carico dalle clausole contrattuali tipo(e non sia possibile porre in essere misure supplementari capaci di assicurare il rispetto di tali obblighi), il titolare è tenuto a sospendere il trasferimento dei dati personali in questione verso il Paese

terzo in questione e/o risolvere le clausole contrattuali tipo stipulate con l'importatore, così come previsto dall'art. 5, lett. a) e b), delle clausole contrattuali stesse.

Le medesime considerazioni valgono anche per quanto concerne il trasferimento dei dati personali in questione al sub-responsabile del trattamento, indicato nell'Appendice n. 2 alle clausole contrattuali tipo, ovvero Amazon Web Services Inc., anch'essa stabilita negli Stati Uniti d'America.

Non trova, infatti, riscontro nella documentazione quanto dichiarato dall'Ateneo nelle proprie memorie, in relazione alla circostanza che "le misure predisposte sono da considerarsi sufficienti, ed idonee, anche e soprattutto alla luce dell'uso di sistemi di crittografia dei dati personali e alla concreta inaccessibilità degli stessi da parte di soggetti terzi, ivi compreso il responsabile e l'autorità statunitensi". Come precisato dall'Ateneo in sede di audizione, infatti, i dati personali "sono cifrati in transito" e poi, "terminata l'elaborazione da parte del fornitore", essi "vengono cifrati dal fornitore, fermo restando che la chiave di cifratura privata è nella disponibilità della sola Università". Ne consegue che la cifratura dei dati con la chiave dell'Università avviene soltanto dopo l'elaborazione degli stessi da parte del fornitore, il quale, al fine di poter esaminare i video relativi agli esami e determinarne l'indice di rischio (anche mediante il trattamento di dati biometrici degli interessati), deve quindi necessariamente accedere ai dati in chiaro, essendo gli stessi cifrati solo al termine di detto processo. Ciò trova conferma anche nella a relazione tecnica prodotta dall'Ateneo in allegato alla memoria difensiva ("il sistema sotteso al funzionamento di Respondus Monitor impiega circa 8/12 ore per predisporre il video alla visione del docente, perché l'algoritmo che elabora il video è molto accurato. Terminata l'elaborazione dei video relativi all'esame sostenuto dagli studenti, nella dashboard di Respondus Monitor verrà abilitata la funzione "Class Results", dove i docenti potranno accedere alle informazioni sulle sessioni d'esame").

Né può essere ritenuta sufficiente la mera pseudonimizzazione dei dati oggetto di trasferimento all'estero (cfr. la relazione tecnica allegata: "i file video, relativi alla prova di ciascuno studente, vengono veicolati dalle API connesse all'LMS al sistema in SaaS che Respondus detiene su AWS" e che "vengono quindi generati degli identificativi di sessione contenenti dati pseudonimizzati e che non contengono dati personali"), in quanto, anche ipotizzando che la pseudonimizzazione potesse essere efficacemente realizzata nel caso di specie, tenuto conto degli specifici dati trattati (es. registrazione delle prove d'esame), essa è, in ogni caso, da considerarsi "un trattamento dei dati personali" (art. 4, n. 5, del Regolamento) volto ad assicurare la sicurezza del trattamento (cfr. art. 32, par. 1, lett. a) del Codice, ove si cita la "pseudonimizzazione" tra le possibili misure tecniche adeguate a garantire un livello di sicurezza adeguato al rischio). La pseudonimizzazione non equivale all'anonimizzazione dei dati.

In considerazione di quanto sopra, l'Ateneo ha dunque trasferito dati personali verso un Paese terzo, ovvero gli Stati Uniti d'America, senza aver comprovato di aver verificato e assicurato che il trasferimento in questione fosse posto in essere nell'effettivo rispetto delle condizioni di cui al Capo V del Regolamento, in violazione degli artt. 44 e 46 del Regolamento. Tale circostanza assume particolare rilevanza

tenuto conto che, tra i dati oggetto di trasferimento internazionale, figurano anche dati relativi a categorie particolari, quali i dati biometrici.

3.8 La valutazione di impatto sulla protezione dei dati

In attuazione del principio di responsabilizzazione (cfr. art. 5, par. 2, e 24 del Regolamento), spetta al titolare valutare se i trattamenti che si intendono realizzare possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche – in ragione delle tecnologie impiegate e considerata la natura, l'oggetto, il contesto e le finalità perseguite – che renda necessaria una preventiva valutazione di impatto sulla protezione dei dati personali (cfr. cons. 90 e art. 35 del Regolamento).

Dall'esame della documentazione in atti è risultato che la valutazione di impatto sulla protezione dei dati, sebbene effettuata dall'Ateneo, non è stata condotta in maniera del tutto adeguata, limitandosi a illustrare le caratteristiche del sistema di supervisione utilizzato, rappresentandolo come conforme al quadro normativo in materia di protezione dei dati, senza però una puntuale valutazione "della necessità e proporzionalità dei trattamenti in relazione alla finalità" e "dei rischi per i diritti e le libertà degli interessati" (art. 35, par. 7, lett. b) e c)), anche in termini di possibile condizionamento o pressioni indirette nei confronti degli studenti, riportando giudizi di adeguatezza estremamente sintetici, privi di idonea motivazione (cfr., in particolare, parr. 3 e 4 della valutazione di impatto in atti), non essendo state, pertanto, individuate, in relazione a taluni profili, appropriate misure "per affrontare i rischi" e per attenuare gli stessi (art. 35, par. 7, lett. d) del Regolamento). In particolare, nella valutazione d'impatto sulla protezione dei dati redatta dall'Ateneo:

al par. 3.3, relativo al rispetto del principio di minimizzazione, si dà conto genericamente che "l'Università ritiene che i dati trattati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità perseguite, non raccogliendo dati ultronei a quelli necessari per lo svolgimento della prova d'esame scritta. valutazione di conformità: positiva", non riportando una puntuale valutazione in merito all'adeguatezza, alla pertinenza e alla proporzionalità di ciascuna categoria di dati oggetto di trattamento mediante il sistema di supervisione, con particolare riguardo ai dati relativi all'analisi del comportamento dello studente durante la prova, e, dunque, senza fornire idonea giustificazione in merito al giudizio di positività;

al par. 3.4, relativo al rispetto del principio di esattezza, si afferma genericamente che "i dati personali – comuni e biometrici – dello Studente devono essere esatti altrimenti non potrebbero essere perseguite le finalità indicate. valutazione di conformità: positiva", non dettagliando un'adeguata valutazione in merito all'effettiva affidabilità dello strumento di supervisione, con riguardo sia alle funzioni di riconoscimento facciale (ad esempio per appurare che non si verifichino malfunzionamenti in ragione del colore della pelle o di tratti somatici legati all'origine etnica degli interessati), sia ai meccanismi con i quali vengono definiti gli indici di rischio, non essendo state, pertanto, valutate le possibili ripercussioni per gli interessati in caso di errori o falsi positivi/negativi. Peraltro, al par. 7 della valutazione d'impatto, il rischio relativo alla discriminazione è stato valutato come "poco probabile", con potenziale danno "medio", in quanto "non si potrebbe determinare discriminazione alcuna", senza, tuttavia, una previa valutazione sull'affidabilità degli algoritmi utilizzati dal sistema di

supervisione. Vengono, peraltro, indicate misure inconferenti per la mitigazione del rischio di discriminazione ("il sistema è costruito in modo da non permettere la conservazione del dato biometrico. Protezione da intrusioni tramite firewall, assenza di esposizione sulla rete e crittografia sul traffico di transito").

Per quanto riguarda l'"affidabilità in tema di protezione dei dati personali", l'Ateneo ha dichiarato, nella propria memoria difensiva, che "l'Università ha effettuato una serie di approfondimenti tecnici in merito alle misure di sicurezza utilizzate dalla società Respondus Inc. – leader di mercato scelto da oltre mille Università – che sono illustrate nella relazione tecnica [allegata alle memorie]"; tale relazione tecnica, che è priva di data, è stata, in ogni caso, fornita dall'Ateneo successivamente alla data di notifica della violazione, in ciò trovando implicita conferma il fatto che la valutazione d'impatto sulla protezione dei dati non avesse affrontato adeguatamente tale aspetto.

Sebbene nella relazione tecnica sia previsto che "anche se la sessione d'esame di uno studente riceve una "High Review Priority", non significa che si sia realizzata un'azione illecita. Molti dati contribuiscono ad una classificazione di priorità e alcuni, come un'interruzione del servizio Internet o video di bassa qualità, non sono necessariamente indicatori di un comportamento vietato. A causa dell'elevato traffico sulla rete, specialmente in questo periodo storico, è probabile che gli studenti possano subire questo tipo di interruzioni", con ciò confermando che è previsto l'intervento umano per assumere decisioni nei confronti dell'interessato, non risulta, tuttavia, che l'Ateneo abbia individuato i criteri in base ai quali i docenti, rivedendo il video della prova d'esame, possano valutare e decidere in concreto se l'interruzione o la degradazione del video sia dipesa da un problema tecnico o da un comportamento scorretto dello studente. Né risulta che siano state fornite specifiche istruzioni sul punto ai docenti, al fine di assicurare la parità di trattamento degli studenti, nonché l'esattezza e l'omogeneità delle valutazioni degli eventi segnalati, con possibili ricadute sulla validità della prova.

In relazione al rispetto del principio di limitazione della conservazione, l'Ateneo si è limitato a riportare i tempi di conservazione dei dati dichiarati dal fornitore nel "nella scheda presente nel Privacy Shield Framework" e nella "Checklist Respondus", senza alcuna puntuale valutazione, dalla prospettiva del titolare, in merito alla congruità di tali tempi di conservazione rispetto alle finalità del trattamento perseguite;

al par. 4, relativo alla "necessità e proporzionalità del trattamento", si riporta genericamente che "il trattamento è necessario per il perseguimento delle finalità enucleate. I dati raccolti sono, infatti, adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati", senza illustrare le valutazioni effettuate dal titolare in merito alle ragioni per le quali si è reso necessario adottare uno strumento di supervisione degli esami a distanza dotato di funzioni di riconoscimento facciale e in grado di profilare il comportamento degli studenti durante la prova, nonché i motivi per i quali non fosse possibile fare ricorso a strumenti di supervisione alternativi, ma meno invasivi per i diritti e le libertà degli stessi;

al par. 7, con riguardo ai potenziali "danni fisici o psichici", l'analisi dell'Ateneo si è concentrata unicamente sui possibili danni psichici derivanti dalla "divulgazione delle

registrazioni degli esami", valutando il rischio come "improbabile" e il potenziale danno come "medio", senza, tuttavia, considerare che, indipendentemente da un'eventuale divulgazione delle registrazioni, l'impatto sulla sfera emotiva e psicologica degli interessati può derivare anche dalle specifiche funzionalità del sistema di supervisione, quali, nel caso di specie, il riconoscimento facciale e la profilazione del comportamento, con possibili ripercussioni sull'esattezza delle anomalie rilevate dall'algoritmo e quindi, indirettamente, anche sul complessivo esito della prova.

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, in violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 9, 13, 25, 35, 44 e 46 del Regolamento, nonché 2-sexies del Codice.

La violazione delle predette disposizioni comporta, ai sensi dell'art. 2-decies del Codice e "salvo quanto previsto dall'articolo 160-bis", l'inutilizzabilità dei dati personali trattati.
La violazione delle predette disposizioni rende, altresì, applicabile la sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo e art. 166, comma 2, del Codice.

5. Misure correttive (art. 58, par. 2, lett. d), del Regolamento).

L'art. 58, par. 2, lett. f), del Regolamento prevede che il Garante ha i poteri correttivi di "imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento".

Prendendo atto di quanto emerso in fase di istruttoria e tenendo conto della circostanza che il sistema "Respondus" non risulta dismesso dall'Ateneo, si rende necessario, ai sensi dell'art. 58, par. 2, lett. f), del Regolamento, disporre la limitazione del trattamento, vietando all'Università ogni ulteriore operazione di trattamento, con riguardo ai dati biometrici degli studenti e ai dati sulla cui base viene effettuata la profilazione degli interessati mediante il sistema "Respondus", e vietare il trasferimento dei dati personali degli interessati negli Stati Uniti d'America, in assenza di adeguate garanzie per gli stessi.

Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, l'Ateneo dovrà, inoltre, provvedere a comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente

provvedimento, le iniziative intraprese al fine di dare attuazione a quanto sopra ordinato ai sensi del citato art. 58, par. 2, lett. f), nonché le eventuali misure poste in essere per assicurare la conformità del trattamento alla normativa in materia di protezione dei dati personali.

6. 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 – considerando anche il richiamo contenuto nell'art. 166, comma 2, del Codice – la violazione delle disposizioni citate è soggetta all'applicazione della stessa 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

In relazione ai predetti elementi è stato considerato che il trattamento ha avuto ad oggetto anche dati appartenenti a categorie particolari, rispetto ai quali il quadro normativo in materia di protezione dei dati personali prevede un livello più alto di tutela, e ha riguardato un numero elevato di interessati, in considerazione del fatto che l'Ateneo conta, stando a quanto dichiarato, "oltre 14.000 studenti"

Di contro, è stato considerato che l'Ateneo, nel fronteggiare inedite problematiche derivanti dal contesto emergenziale determinato dalla pandemia da Sar-Cov-2, ha dovuto operare scelte e adottare misure tecniche e organizzative in tempi rapidi al fine di assicurare la continuità dell'attività didattica e lo svolgimento delle sessioni d'esame. Inoltre, con riguardo alla violazione degli artt. 44 e 46 del Regolamento, si è considerato che la sentenza del 16 luglio 2020 della Corte di Giustizia Europea (Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems, Causa C-311/18) è stata emessa quando i trattamenti in questione erano già in essere, che le conseguenze dei principi di diritto in essa formalizzati possono, in taluni casi, essere di complessa attuazione, nonché, più in generale, che il quadro giuridico in materia di trasferimenti internazionali è ancora in evoluzione (v. le "Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE" del Comitato europeo per la protezione dei dati del 10 novembre 2020, che al tempo in cui è stato posta in essere la condotta non erano state definitivamente adottate; v. anche la

recente decisione di esecuzione (UE) 2021/914 della Commissione europea del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, efficace a partire dal 27 giugno 2021). Infine, si è preso favorevolmente atto che, nonostante la contraddittorietà delle dichiarazioni rese su taluni profili, l'Ateneo si è sostanzialmente dimostrato collaborativo e ben disposto a recepire i rilievi dell'Autorità.

Non risultano, inoltre, precedenti violazioni commesse dal titolare del trattamento o precedenti provvedimenti di cui all'art. 58 del Regolamento.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 200.000,00 (duecentomila) per la violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 9, 13, 25, 35, 44 e 46 del Regolamento, nonché 2-sexies del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, paragrafo 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Tenuto conto della particolare delicatezza dei dati trattati, si ritiene altresì che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019.

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

TUTTO CIÒ PREMESSO IL GARANTE

rileva l'illiceità del trattamento effettuato dall'Università Commerciale "Luigi Bocconi" di Milano per violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 9, 13, 25, 35, 44 e 46 del Regolamento, nonché 2-sexies del Codice, nei termini di cui in motivazione, e dichiara, ai sensi dell'art. 2-decies del Codice, l'inutilizzabilità dei dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali, salvo quanto previsto dall'art. 160-bis del Codice;

ORDINA

all'Università Commerciale "Luigi Bocconi" di Milano, in persona del legale rappresentante pro-tempore, con sede legale in Via Sarfatti, 25 – 20136 Milano (MI), C.F. 80024610158, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento, di pagare la somma di euro 200.000,00 (duecentomila) 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 trenta giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

alla predetta Università:

a) di pagare la somma di euro 200.000,00 (duecentomila) in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, secondo le modalità indicate in allegato, entro trenta giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

b) ai sensi dell'art. 58, par. 2, lett. f) del Regolamento, la limitazione del trattamento, vietando all'Università ogni ulteriore operazione di trattamento con riguardo ai dati biometrici degli studenti e ai dati sulla cui base viene effettuata la profilazione degli interessati mediante il sistema "Respondus", nonché vietando il trasferimento dei dati personali degli interessati negli Stati Uniti d'America in assenza di adeguate garanzie per gli stessi;

c) ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, di comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione a quanto sopra ordinato ai sensi del citato art. 58, par. 2, lett. f), nonché le eventuali misure poste in essere per assicurare la conformità del trattamento alla normativa in materia di protezione dei dati personali.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione del presente provvedimento sul sito web del Garante, ritenendo che ricorrano i presupposti di cui all'art. 17 del Regolamento del Garante n. 1/2019;

l'annotazione del presente provvedimento nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u), del Regolamento, delle violazioni e delle misure adottate in conformità all'art. 58, par. 2, 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, 16 settembre 2021