Giulia Schneider

L'IMPATTO DELL'INTELLIGENZA ARTIFICIALE SULL'UNIVERSITÀ TRA TUTELA DEI DATI PERSONALI E DIRITTO ALL'ISTRUZIONE

1. *Introduzione*

L'avvento della tecnologia digitale automatizzata e, nello specifico, dell'intelligenza artificiale (IA), sta rivoluzionando prassi e consuetudini proprie di una vasta gamma di settori economici e culturali essenziali alla società europea contemporanea. Tra questi, il mondo della scuola e dell'università risulta tutt'altro che immune a tale fenomeno tecnologico. L'istruzione e la ricerca scientifica stanno infatti attraversando una storica fase di trasformazione digitale, accelerata dall'impellente necessità di proseguire le attività durante l'emergenza pandemica e permeata dalla spinta verso modelli educativi personalizzati e un sapere più inclusivo.

In tale ottica, le università rappresentano un crocevia importante nell'evoluzione tecnologica, in quanto per prime operano, promuovono e solitamente internalizzano alcuni degli elementi innovativi dal forte impatto sociale per quanto riguarda sia il diritto all'istruzione sia la libertà di ricerca scientifica. Entrambe tali aree di attività accademica presentano cambiamenti significativi e sviluppi promettenti, da corsi online personalizzabili all'*e-proctoring*, dagli strumenti di elaborazione automatica a nuove modalità di raccolta, gestione e condivisione di materiale scientifico.

Seppur mostrando il potenziale per una futura «università 2.0» più vicina ai bisogni del singolo studente e più ambiziosa nel porre rimedio alle grandi sfide globali, la traiettoria tecnologica intrapresa nell'ambiente accademico deve necessariamente fare fronte a nuovi problemi di tutela, *in primis* connessi alla necessità di proteggere i dati personali dei soggetti coinvolti. La discussione attorno ai diritti

Cap. XV di: ASTRID, *Intelligenza artificiale e diritto: una rivoluzione?*, vol.I, Il Mulino, 2022

fondamentali e, in particolare, al diritto alla protezione dei dati personali offre un'utile cartina di tornasole per analizzare fenomeni di possibile integrazione degli enti di formazione ed università «tradizionali» con nuove modalità di educazione e ricerca sia interne (per es. didattica da remoto, gestione telematica) che esterne (per es. diretta competizione con progetti imprenditoriali di grandi multinazionali). Il dato di partenza è che in assenza di adeguate infrastrutture digitali gli enti universitari sono costretti a reperire *facilities* tecnologiche in *outsourcing* affidandosi alle infrastrutture fornite da terze parti.

Per quanto riguarda l'insegnamento universitario, il superamento della resistenza alla digitalizzazione scolastica e i profondi cambiamenti indotti dall'emergenza pandemica portano ad interrogarsi su come le università si siano equipaggiate per tutelare i dati personali di docenti e studenti nella dimensione virtuale. Esposti a rischi di *cybercrime* e spesso inconsapevoli delle condizioni e prassi di gestione dei propri dati da parte di piattaforme e servizi digitali, entrambe le categorie di soggetti necessitano adeguata tutela ed interventi mirati e proattivi da parte delle amministrazioni e figure garanti negli atenei. Inoltre, la virtualizzazione dei servizi didattici e la relativa massimizzazione delle attività di raccolta e trattamento di dati personali impone un supplemento di riflessione in ordine ai rischi di trattamento ulteriore. Questi dati, di natura in gran parte sensibile, costituiscono materia preziosa per gli enti universitari per lo svolgimento di indagini riguardo alla partecipazione, agli interessi e alle modalità di comportamento dei soggetti coinvolti, primi tra tutti docenti e studenti. A tal fine possono essere impiegate tecniche di *machine learning* e pratiche di *data fusion* che contribuiscono ad ampliare i rischi per i diritti e le libertà delle persone fisiche interessate dal trattamento. Il valore commerciale dei dati così raccolti potrebbe inoltre indurre le stesse università a stipulare accordi di cessione con terze parti, quali piattaforme e *player* digitali.

Sulla base di queste premesse, il capitolo intende mettere a fuoco il ruolo delle università quali figure chiave di *data controller* nel contesto delle attività di insegnamento e di

trattamento ulteriore sui dati raccolti mediante strumenti digitali. Il mantenimento di un effettivo controllo sui dati relativi all'educazione è tanto più impellente di fronte ad un quadro in materia di protezione di dati personali che apre al riuso massivo di dati per scopi di ricerca latamente intesi, facilitandone lo sfruttamento commerciale. Dal quadro tratteggiato emerge dunque la necessità di operare una mappatura dei rischi connessi agli usi secondari dei dati raccolti attraverso strumenti di educazione digitale. Si tratta di esercizio preliminare all'individuazione di soluzioni regolatorie che possano marginare il potere delle grandi piattaforme nel settore dell'educazione a discapito dell'autonomia delle università e della libera determinazione dei contenuti educativi.

2. *La tutela dei dati personali nella didattica a distanza*

La progressiva digitalizzazione del settore educativo, accelerata dallo scoppio della pandemia di COVID-19 nel 2020, ha ampiamente messo in luce un vero e proprio «scontro tra Titani» nelle aule universitarie. Se, da una parte le nuove frontiere aperte dalle tecnologie digitali hanno incontrato l'esitazione e la difficoltà rispetto al superamento di pratiche consolidate ed efficacemente ponderate nel mondo *offline*, dall'altra l'introduzione di modelli educativi cosiddetti *student-tailored* e le modalità di insegnamento e valutazione digitali hanno ravvivato il dibattito sulle opportunità strettamente pedagogiche e di continuazione dell'insegnamento durante l'emergenza pandemica.

L'attenzione pubblica e dottrinale si è da ultimo concentrata su strumenti quali quelli di *e-proctoring*, scenario emblematico della rilevanza della tutela dei dati personali di studenti e docenti nell'ambiente didattico universitario digitalizzato. Si tratta di strumenti automatizzati di sorveglianza e vigilanza che tentano di riprodurre nella dimensione online ed in via automatizzata le tradizionali funzioni di supervisione nel corso di esami. Questi sistemi sono particolarmente sofisticati e diventano bacino di raccolta di una vasta quantità

di dati inerenti al video e all'audio, che vengono trattati al fine di individuare un comportamento sospetto o inusuale. Oltre a presentare alcuni preoccupanti elementi di *bias*[1], ad esempio nel riconoscimento e dunque nella sorveglianza di soggetti di colore, questi strumenti attuano un monitoraggio continuo ed automatizzato che può essere percepito dagli studenti come estremamente invasivo, con la connessa insorgenza di nuovi pregiudizi morali[2].

La legittimità dell'uso di questi strumenti è stata recentemente oggetto di numerose decisioni dei Garanti privacy europei nonché di alcune pronunce giurisprudenziali. È quest'ultimo il caso del Tribunale di Amsterdam, che è stato investito della questione inerente la legittimità di un sistema e-proctoring, ritenuto da due associazioni di studenti non conforme alla normativa in materia di protezione di dati personali sotto i profili della base giuridica del trattamento, della finalità del trattamento e del rispetto del principio di proporzionalità. Malgrado queste doglianze, il Tribunale di Amsterdam nel giugno 2020 ha decretato la conformità del sistema usato ai canoni dettati dalla normativa[3].

Più variegato è il panorama delle decisioni dei Garanti privacy che hanno ora ritenuto i sistemi *e-proctoring* usati aderenti al quadro normativo in materia di protezione di dati personali – è quanto affermato dall'Autorità danese[4] –

[1] D. Woldeab e T. Brothen, *21st Century Assessment: Online Proctoring, Test Anxiety, and Student Performance*, in «International Journal of E-Learning & Distance Education», 34, 2019, n. 1; M. Foulkes, *Exams that Use Facial Recognition May be Fair – But They Are Also Intrusive*, in «The Guardian», 22/7/2020, reperibile all'indirizzo https://www.theguardian.com/law/2020/jul/22/exams-that-use-facial-recognition-are-fair-but-they-re-alsointrusive-and-biased?CMP=Share_iOSApp_Other.

[2] M. Chin, *Exam Anxiety: How Remote Test-Proctoring is Creeping Students Out – As Schools go Remote, So Do Tests and So Does Surveillance*, in «TheVerge», 29/4/2020, reperibile all'indirizzo https://www.theverge.com/2020/4/29/21232777/examityremote-test-proctoring-online-class-education.

[3] Rb. Amsterdam - C/13/684665 / KG ZA 20-481.

[4] IT University of Copenhagen, *The Danish Data Protection Agency: IT University of Copenhagen has acted correctly in relation to the use of ProctorExam* (4/2/2021), reperibile online all'indirizzo https://en.itu.dk/about-itu/press/news-from-itu/2021/the-danish-data-protection-agency.

ora invece non adeguatamente protettivi della privacy degli studenti, ordinando la rettifica degli strumenti impiegati, come avvenuto in Norvegia[5], o comminando importanti sanzioni pecuniarie, come deciso dal Garante per la privacy italiano[6].

I diversi orientamenti ora richiamati in relazione alla legittimità dei sistemi *e-proctoring* in punto di protezione dei dati personali ben riflette l'incertezza regolatoria che ancora persiste nel settore dell'educazione digitale. Come i prossimi paragrafi dimostreranno, proprio questa situazione di incertezza economica è destinata a creare le condizioni che favoriscono l'accumulo di dati e la conseguente centralizzazione della gestione dei servizi di educazione digitale nelle infrastrutture tecnologiche di pochi attori operanti sul mercato rilevante per l'istruzione.

3. *La tutela dei dati personali nelle attività di trattamento ulteriore: il problema della ricerca sui dati raccolti e della cessione dei dati a piattaforme terze*

La pandemia da COVID-19 ha decretato l'impiego di strumenti digitali e di intelligenza artificiale in ambito universitario non solo per quanto concerne lo svolgimento delle attività didattiche svolte sempre più in modalità da remoto, ma anche come supporto alle altre realtà consustanziali alla dimensione universitaria, prime tra tutte quelle amministrative e quelle connesse alla ricerca scientifica. Un primo, evidente, corollario fattuale di queste trasformazioni è dato

[5] «DataGuidance», *Norway: Datatylsinet issues order to IBO to rectify unfairly processed and incorrect personal data in relation to exam results*, 10/8/2020, reperibile online all'indirizzo https://www.dataguidance.com/news/norway-datatilsynet-issues-order-ibo-rectify-unfairly-processed-and-incorrect-personal-data.

[6] «Corriere Milano», *Università Bocconi, volti degli studenti spiati durante gli esami a distanza: multa di 200 mila euro*, 29/9/2021, reperibile online all'indirizzo https://milano.corriere.it/notizie/cronaca/21_settembre_29/universita-bocconi-volti-studenti-spiati-gli-esami-distanza-multa-200-mila-euro-6928018c-20e6-11ec-924f-1ddd15bf71fa.shtml.

dall'incremento del *volume* e della *varietà* delle interazioni virtuali riconducibili all'istituzione dell'università, ben oltre l'orizzonte dei servizi di insegnamento[7].

Proprio questi due parametri suggeriscono un supplemento di riflessione circa le implicazioni della digitalizzazione della didattica e della ricerca universitaria in presenza sulla tutela del diritto alla protezione dei dati personali e sul connesso diritto all'istruzione. La questione si pone in particolare rispetto al rischio di trattamenti ulteriori dei dati personali raccolti in occasione delle attività universitarie «tradizionali». Invero, sembra che i processi di trasformazione digitale dell'università amplifichino i rischi di riutilizzo dei dati personali riferibili ai principali soggetti coinvolti, come studenti e insegnanti.

In primo luogo, l'enorme quantità di dati digitali, in gran parte dati sensibili, ora a disposizione degli enti universitari, costituiscono materia preziosa per questi ultimi per condurre indagini sull'andamento delle proprie attività, ad esempio riguardo alla partecipazione, agli interessi e alle modalità di comportamento di studenti e insegnanti. Si tratta, evidentemente, di nuovi scenari di (meta-)analisi, con le quali gli istituti accademici potrebbero procedere alla valutazione dei propri percorsi formativi e di ricerca, al loro perfezionamento e finanche alla loro personalizzazione[8].

Essenziale per un'adeguata estrazione del valore informativo dei dati raccolti è l'applicazione di tecniche di *machine learning*, in grado di identificare i *pattern* rilevanti tra i dati immessi e di emettere valutazioni predittive sui *trend* futuri. Come noto, maggiore è il bacino di dati a cui gli strumenti di analisi algoritmica possono attingere, maggiore sarà la precisione degli output predittivi di questi ultimi.

[7] R. Ducato, C. Angiolini, A. Giannopoulou e G. Schneider, *Remote Teaching During the Pandemic and Beyond: Data Protection and Privacy of EdTech*, in «Opinio Juris in Comparatione», 2020, n. 1, pp. 43-72.

[8] *The Atlantic, Artificial Intelligence Promises a Personalised Education for All*, https://www.theatlantic.com/sponsored/vmware-2017/personalized-education/1667/. S. Tsai *et al.*, *Precision Education with Statistical Learning and Deep Learning: a Case Study in Taiwan*, in «International Journal of Educational Technology in Higher Education», 17, 2020, n. 12, https://doi.org/10.1186/s41239-020-00186-2.

Da ciò deriva l'opportunità di aggregare dati provenienti da fonti – e quindi da attività – differenti, mediante pratiche cosiddette di *data fusion*, con cui dati provenienti da varie fonti vengono aggregati e analizzati.

Sotto un profilo distinto, il valore commerciale – e segnatamente di marketing – dei dati derivanti dalle attività universitarie condotte online potrebbe indurre le stesse università a stipulare specifici accordi di cessione con terze parti, quali piattaforme e altri *player* digitali, al fine di monetizzare il patrimonio informativo raccolto e aprire così una fonte di finanziamento aggiuntiva. Tali accordi sarebbero ragionevolmente stipulati con soggetti terzi diversi da coloro che già forniscono le infrastrutture digitali utilizzate per svolgere le attività curriculari da remoto. Oltre alla rilevanza di nuovi strumenti utili all'erogazione di servizi di insegnamento, la digitalizzazione dell'università comporta dunque anche l'ingresso di nuovi *stakeholders* sin qui estranei al settore dell'istruzione: imprese e piattaforme digitali[9].

Queste ultime raccolgono e trattano per conto delle stesse università i dati personali rilasciati nel contesto delle attività accademiche, tramite i sofisticati strumenti tecnologici che forniscono agli enti universitari per lo svolgimento dei relativi servizi. Questi soggetti sono pertanto già in possesso dei dati originanti dalle attività universitarie virtuali e non avrebbero dunque l'interesse o – più precisamente – l'incentivo a emettere un corrispettivo per l'utilizzo dei medesimi. Anche e soprattutto rispetto alle imprese che sono contraenti diretti degli enti universitari e che forniscono a questi servizi digitali quali i servizi di videoconferenza, forum, registrazione e conservazione dei dati, si profila il rischio di trattamenti ulteriori di dati personali per scopi segnatamente commerciali, nei vari settori di mercato in cui queste piattaforme sono sovente attive (cd. *multisided platforms*).

Dal quadro sin qui tracciato è dunque possibile identificare tre principali ipotesi di trattamento ulteriore di dati personali nell'ambito dell'università, come virtualizzata

[9] T. Fiebig *et al.*, *Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds*, 2021, in «arXiv», 2104.09462.

dall'esperienza dell'emergenza sanitaria: *i*) il riutilizzo dei dati da parte delle università per scopi di ricerca riguardante i servizi di istruzione; *ii*) il riutilizzo dei dati da parte delle università per scopi di cessione a terze parti; *iii*) il riutilizzo dei dati da parte di piattaforme digitali fornitrici di servizi digitali alle università[10].

In via generale, il riconoscimento di queste occasioni di trattamento ulteriore di dati variamente riguardanti l'educazione rivela la struttura progressivamente aperta del nuovo ecosistema universitario, configurantesi come una rete contrattuale in cui assumono rilievo sempre maggiore imprese digitali specificamente attive nel settore dell'istruzione, come Moodle o Discord, ma anche più grandi piattaforme digitali, come Google, Facebook, YouTube[11], che fanno dell'educazione uno dei propri molteplici segmenti di attività commerciale. Come facilmente intuibile, nella maggior parte di queste ipotesi, il modello di business di queste società è incompatibile con il pubblico interesse posto a fondamento delle istituzioni universitarie. Questa nuova configurazione strutturale comporta innanzitutto uno snaturamento del settore dell'istruzione, ora più che mai esposto al rischio di «cattura» delle logiche di mercato lungo inedite declinazioni dei processi di privatizzazione dell'università già in atto.

La «delega di funzioni» attribuita alle imprese digitali dalle università e riguardante la definizione dei mezzi digitali per lo svolgimento delle attività accademiche, si traduce, *de facto*, in una perdita di controllo da parte delle università medesime sui servizi educativi da queste rese. Da un primo angolo prospettico, l'ormai nota espressione *code is law*

[10] S. Vincent-Lancrin e R. van der Vlies, *Trustworthy Artificial Intelligence (AI) in Education: Promises and Challenges*, OECD Working Papers n. 218, 6/4/2020, https://www.oecd-ilibrary.org/education/trustworthy-artificial-intelligence-ai-in-education_a6c90fa9-en.

[11] R. Ducato, G. Priora, C. Angiolini, A. Giannopolou, B.J. Jütte, G. Noto La Diega, L. Pascault e G. Schneider, *Emergency Remote Teaching: A study of copyright and data protection terms of popular online services (Part II)*, 4/6/2020, http://copyrightblog.kluweriplaw.com/2020/05/27/emergency-remote-teaching-a-study-of-copyright-and-data-protection-terms-of-popular-online-services-part-ii/.

suggerisce come in ambito universitario, il «codice» delle piattaforme utilizzate finisca per determinare le «leggi» dell'educazione digitale, influendo, in prima battuta, sui contenuti della stessa[12], e quindi sull'autonomia e l'indipendenza delle università[13]. Basti pensare ad una piattaforma di didattica a distanza, che permetta, per assurdo, solo il caricamento di contenuti multimediali ma non di file scritti. E se, nella dimensione digitale, i contenuti sono in larga parte costituiti da ovvero associati a dati (ad. es. il dato di quante volte uno studente ha riprodotto un dato contenuto multimediale), un ulteriore corollario della delega di funzioni ora richiamata è esattamente da rinvenirsi nella perdita di controllo da parte delle università dei dati associati alle proprie attività di ricerca e istruzione[14].

Alla luce di quanto precede, si profila dunque la questione se le università e le imprese fornitrici di servizi digitali alle università forniscano adeguate garanzie in punto di trattamenti ulteriori dei dati personali.

3.1. *Le attività di trattamento ulteriore dei dati personali da parte delle università*

Prima di esaminare il regime giuridico applicabile alle ipotesi di trattamento ulteriore di dati personali da parte

[12] Per le implicazioni in punto di tutela del diritto d'autore, cfr. L. Pascault *et al.*, *Copyright and Remote Teaching in the Time of Covid-19: A Study of Contractual Terms and Conditions of Selected Online Services*, in «European Intellectual Property Review», 42, 2020, pp. 548 ss.; C. Rapanta *et al.*, *Online University Teaching During and After the Covid-19 Crisis: Refocusing Teacher Presence and Learning Activity*, in «Postdigital Science and Education», 2020, n. 2, pp. 923-945.

[13] R. Colaiori, *L'insegnamento accademico in presenza, a distanza e i principi costituzionali connessi*, in «Politica del diritto», 2020, n. 2, pp. 259-289. Cfr. anche S. Prisco, *La didattica universitaria a distanza: «filosofia», opportunità, limiti e rischi*, in «Dirittifondamentali», 19/6/2020, http://dirittifondamentali.it/2020/06/19/la-didattica-universitaria-a-distanza-filosofia-opportunita-limiti-e-rischi/.

[14] Fiebig *et al.*, *Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds*, cit.

degli enti universitari, è necessario premettere come la maggior parte dei dati originanti dalle attività di istruzione siano dati relativi all'«origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale», nonché dati relativi allo stato di salute, tra cui eventualmente anche dati biometrici, dei soggetti interessati dal trattamento. Si tratta dunque, per larga parte, di «categorie particolari di dati personali» soggette al regime speciale di protezione dei dati personali di cui all'art. 9 GDPR. E se, come alcuni studi hanno dimostrato[15], la combinazione tra diversi dati personali, come ad es. dati sulla geolocalizzazione, sull'alimentazione o sul ritmo sonno-veglia, può dare origine a informazioni relative allo stato di salute fisica o mentale attuale o futuro di un soggetto, è facilmente comprensibile come molte delle informazioni relative a studenti e insegnanti rilasciate in occasione di attività di istruzione condotte da remoto possano essere indicative di condizioni sensibili e dunque soggette in larga parte alla disciplina speciale di cui all'art. 9 GDPR. La questione non è irrilevante, perché l'individuazione della tipologia dei dati oggetto del trattamento influisce in larga misura sui due parametri di liceità e di finalità, dapprima del trattamento primario posto in essere ed in secondo luogo del trattamento ulteriore.

Esattamente come per le attività di trattamento originario, anche il riutilizzo di dati personali deve essere contraddistinto da una autonoma base giuridica in ossequio al principio di liceità *ex* art. 5, comma 1 lett. *a* GDPR, e da una finalità determinata, esplicita e legittima *ex* art. 5, comma 1 lett. *b* GDPR. Per quanto attiene alla scelta della base giuridica per il trattamento ulteriore di dati sensibili, questa dovrà essere individuata nella combinazione tra le basi giuridiche

[15] G. Comandè e G Malgieri, *Sensitive by Distance: Quasi Health Data in the Algorithmic Era*, in «Information & Communication Technology Law», 26, 2017, n. 3, pp. 229-249. Cfr. anche G. Comandè e G. Schneider, *Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of «Health Data»*, in «European Journal of Health Law», 25, 2018, n. 3, pp. 284-307.

generali di cui all'art. 6 GDPR e le basi giuridiche speciali di cui all'art. 9, comma 2 GDPR[16].

Sulla base di queste generali premesse deve dunque distinguersi l'ipotesi del trattamento ulteriore dei dati personali da parte delle stesse università per scopi di ricerca, in particolare statistica, riguardante i propri servizi di insegnamento ovvero le proprie attività di ricerca. Potrebbero rientrare in questa ipotesi, ad esempio, lo svolgimento di analisi relative all'andamento dell'insegnamento, al grado di gradimento o attenzione degli studenti alle lezioni, al livello di coinvolgimento attivo dei ricercatori nei progetti di ricerca, al calcolo dei risultati scientifici conseguiti o infine di indagini condotte per attività promozionali. Queste indagini potrebbero ben qualificarsi come attività di ricerca statistica e ricadere nella specifica ipotesi di cui all'art. 9, comma 2 lett. *j* GDPR.

Per essere legittime queste attività di ricerca devono essere fondate in una delle basi giuridiche di cui all'art. 6 GDPR. Rilevano per la fattispecie considerata in particolare il consenso dell'interessato *ex* art. 6, comma 1 lett. *a* GDPR ovvero il legittimo interesse dell'università *ex* art. 6, comma 1 lett. *f* GDPR.

Per quanto riguarda il consenso si pongono tuttavia alcune delicate questioni, ben poste in luce dalle linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679 dello European Data Protection Board[17]: in particolare, laddove il rilascio del consenso a questi trattamenti ulteriori sia condizione per l'accesso a servizi di istruzione

[16] G. Schneider, *Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence?*, in «Journal of Intellectual Property, Information Technology and E-Commerce Law», 11, 2020, n. 1, https://www.jipitec.eu/issues/jipitec-11-1-2020/5082/#ftn.N1060F. Per la medesima soluzione interpretativa cfr. E.S. Dove, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, in «The Journal of Law, Medicine & Ethics», 2018, pp. 1013 ss., in part. 1024.

[17] European Data Protection Board, *Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679*, 4/5/2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_it.pdf.

ovvero alle attività di ricerca, il consenso non sarebbe prestato liberamente e sarebbe dunque invalido. Inoltre, gli enti universitari dovrebbero correttamente individuare e informare i soggetti interessati degli specifici trattamenti ulteriori previsti.

Non è sottoposta a queste rigide condizioni la base giuridica connessa all'interesse legittimo dell'ente universitario[18]: a riguardo, tuttavia il Gruppo di lavoro articolo 29 per la protezione dei dati ha precisato come, per essere valida base giuridica di trattamento, l'interesse legittimo debba essere reale, specifico e «accettato dalla legge». Infine, le attività di trattamento ulteriore delle università concernenti la ricerca sui servizi educativi e di ricerca da queste rese potrebbero essere configurate alla stregua di un «compito di interesse pubblico». Se tuttavia questo inquadramento, come recentemente suggerito dal nostro Garante per la protezione dei dati personali[19], è più correttamente ravvisabile per quanto concerne il trattamento primario di dati personali allo scopo di fornire, ad esempio, il servizio di didattica a distanza, la sussistenza di un interesse pubblico appare più difficilmente configurabile nel caso di trattamento ulteriore dei dati raccolti per finalità di affinamento e perfezionamento delle attività di istruzione e di ricerca.

Sulla scorta di queste possibili basi giuridiche, le attività di trattamento ulteriore sui dati personali da parte delle università per scopi di ricerca statistica «ad uso interno» potrebbero beneficiare del regime speciale in materia di ricerca, anche statistica, secondo le previsioni dell'art. 9,

[18] Article 29 Data Protection Working Party, *Opinion 06/2014 on the «Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9/4/2020, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Cfr. anche I. Kamara e P. De Hert, *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*, Bruxelles Privacy Hub Working Paper 4, 12, 2018, https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf.

[19] Garante per la protezione dei dati personali, *Didattica a distanza: prime indicazioni*, atto del 26/3/2020, n. 9300784, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9300784.

comma 2 lett. *j* GDPR. Questo regime speciale prevede innanzitutto la deroga al principio di limitazione della finalità del trattamento, sancito dal combinato disposto degli artt. 5, comma 1 lett. *b* e art. 6, comma 4 GDPR, che istituisce una presunzione di compatibilità del trattamento di dati condotto a scopi di ricerca scientifica con le finalità originarie. Ulteriori deroghe sono previste in caso di attività di ricerca per alcuni diritti dell'interessato quali il diritto alla cancellazione (art. 17, comma 3 lett. *d* GDPR) e all'accesso alle informazioni riguardanti il trattamento (art. 14, comma 5 lett. *b* GDPR). Queste deroghe dovranno tuttavia essere bilanciate attraverso «adeguate garanzie per la protezione dei diritti e delle libertà fondamentali dell'interessato». Per la definizione di queste garanzie, che ben dovrebbero andare oltre la mera applicazione di tecniche di pseudonimizzazione, sarebbe utile l'emanazione di un Codice di condotta del trattamento dei dati personali delle università «digitali» in conformità alla previsione dell'art. 40 GDPR[20].

Nel rispetto dei limiti del quadro normativo ora tracciato deve infine ricordarsi come le ipotesi di trattamento ulteriore da parte delle università qui considerate devono rispettare previsione di cui all'art. 22 GDPR, relativo al divieto di processi decisionali automatizzati relativi alle persone fisiche, compresa la profilazione. Anche per le università si pone pertanto il divieto di condurre attività di trattamento ulteriore condotte per finalità di profilazione degli studenti o degli insegnanti. Profili che, invero, potrebbero costituire materiale ambito da terze parti, in particolare nel settore privato[21].

Sennonché, proprio la cessione a terzi a titolo oneroso dei dati sensibili non appare ammessa da alcuna delle basi

[20] G. Schneider e G. Comandè, *Differential Data Protection Regimes in Data-driven Research: Why the GDPR is More Research-friendly Than You Think*, in «German Law Journal», 2021 (in corso di pubblicazione). E cfr. già G. Schneider e G. Comandè, *Can the GDPR Make Data Flow for Research Easier? Yes it Can! By Differentiating!*, in «Computer Law & Security Review», 41, 2021, 105539.

[21] Vincent-Lancrin e van der Vlies, *Trustworthy Artificial Intelligence (AI) in Education: Promises and Challenges*, cit., p. 15.

giuridiche speciali di cui all'art. 9, comma 2 GDPR: l'unica ipotesi legittima sarebbe quella del conseguimento da parte delle università di un consenso esplicito, adeguatamente informato e libero dei soggetti interessati a questo specifico trattamento ulteriore. Si tratta, tuttavia, di un'ipotesi residuale, soggetta eventualmente alla possibilità di revoca del medesimo consenso da parte dei soggetti interessati. Inoltre, la diffusione di pratiche di commercializzazione dei dati relativi all'istruzione o alla ricerca si porrebbe in contrasto con l'interesse pubblico che le università pubbliche dovrebbero perseguire; potrebbe essere, inoltre, fonte di danni reputazionali, anche per le istituzioni private.

3.2. *Le attività di trattamento ulteriore dei dati personali da parte di terzi*

La seconda ipotesi da prendere in considerazione è relativa agli usi secondari da parte delle piattaforme che raccolgono i dati nell'ambito dei servizi digitali che forniscono alle istituzioni universitarie. Questo diverso scenario riguarda pertanto il perseguimento di finalità di trattamento autonome, quali finalità di marketing, da parte di soggetti terzi in conformità al proprio modello di business.

Come evidente, la scelta del servizio, ad esempio, di didattica a distanza, non dovrebbe in alcun modo avere come conseguenza quella di sottoporre studenti e docenti alla raccolta e all'ulteriore trattamento dei dati per finalità slegate da quelle educative e di didattica. A tal fine, risulta fondamentale il ruolo delle università non solo nella scelta, bensì anche nella definizione dei limiti giuridici entro i quali i terzi contraenti possono utilizzare i dati raccolti.

In via di premessa, deve rilevarsi come le *privacy policies* di molti dei fornitori di servizi digitali a cui si sono rivolte le università allo scoppio della pandemia prendono in espressa considerazione la fattispecie del trattamento ulteriore, informando i propri utenti che usi secondari dei dati saranno previsti per finalità di «miglioramento del

servizio»[22]. Questa formula altro non apre che a usi secondari di natura commerciale.

Cosa potrebbero fare dunque le università per arginare i rischi di questi usi secondari? Il Regolamento generale sui dati personali fornisce alcune interessanti indicazioni a riguardo, lasciando tuttavia aperte delle lacune che potrebbero rivelarsi insidiose se non adeguatamente risolte mediante l'introduzione di presidi regolatori supplementari.

Innanzitutto, nella ripartizione dei ruoli tra università e terze piattaforme, le prime sono da qualificarsi quali «titolari del trattamento» *ex* art. 4, comma 1, n. 7 RGDP in quanto determinano le finalità e i mezzi del trattamento, mentre le seconde sono da considerarsi quali «responsabili del trattamento» in quanto sono i soggetti scelti dal titolare per svolgere il trattamento «per conto» dello stesso titolare secondo l'art. 4, comma 1, n. 8 RGDP.

L'art. 28 RGDP richiede al titolare del trattamento di ricorrere a responsabili che «presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato». La medesima disposizione precisa, al suo comma 2, che il ricorso da parte del responsabile del trattamento a un ulteriore responsabile – il che implica indirettamente un trattamento ulteriore dei dati verso quest'ultimo – deve essere autorizzato per scritto da parte dell'università. In virtù di un'applicazione estensiva di questa previsione al caso dei trattamenti ulteriori da parte dei responsabili del trattamento, il ministero dell'Istruzione ha stabilito come i trattamenti ulteriori da parte delle piattaforme digitali dovranno essere specificamente autorizzati dalle università titolari del trattamento. Il ministro dell'educazione suggerisce a riguardo una stretta collaborazione tra i DPO delle istituzioni e delle

[22] Così le *privacy policies* di Jitsi e G-suite; cfr. Ducato, Priora, Angiolini, Giannopolou, Jütte, Noto La Diega, Pascault e Schneider, *Emergency Remote Teaching: a study of copyright and data protection terms of popular online services (Part II)*, cit. Cfr. più in generale Noyb, *Report on privacy policies of video conferencing services*, 2020.

imprese per garantire che i trattamenti rimangano nell'alveo di quanto stabilito dall'università titolare del trattamento[23].

L'inquadramento delle imprese terze contraenti alla stregua di responsabili del trattamento potrebbe tuttavia essere sconfessato da una valenza in concreto delle stesse come titolari del trattamento. In pratica, infatti, sono proprio le piattaforme digitali ad avere ampi poteri di scelta dei mezzi e delle finalità del trattamento: la determinazione degli strumenti digitali che queste mettono a disposizione delle università comporta infatti in prima battuta la determinazione dei mezzi; inoltre, il modo in cui questi mezzi sono strutturati incide di riflesso anche sulla definizione delle finalità del trattamento. Questo vale per i trattamenti primari ma in particolare per quelli secondari, in relazione ai quali queste imprese diventerebbero titolari del trattamento a tutto tondo, determinandone non solo i mezzi ma in particolare le finalità «ulteriori».

Sul piano della disciplina dei dati personali, la configurazione alla stregua di titolare del trattamento dell'impresa terza non de-responsabilizza totalmente l'università: è quanto desumibile dall'art. 26 RGDP che disciplina la fattispecie della contitolarità del trattamento, che si ha quando «due o più titolari del trattamento determinano *congiuntamente* le finalità e i mezzi del trattamento»[24]. Lo European Data Protection Board[25] ha interpretato estensivamente la nozione di contitolarità per ricomprendervi non solo le situazioni in cui i due soggetti effettuano delle decisioni comuni, ma anche quelle in cui le decisioni circa i mezzi e le finalità sono il risultato di decisioni convergenti: ciò avverrebbe quando il trattamento non sarebbe stato possibile senza la

[23] Ministero dell'Istruzione e della Ricerca, *Emergenza sanitaria da nuovo Coronavirus. Prime indicazioni operative per la didattica a distanza*, nota n. 388, 17/3/2020, https://www.miur.gov.it/-/coronavirus-emanata-la-nota-con-le-indicazioni-operative-per-la-didattica-a-distanza.

[24] Corsivo aggiunto.

[25] European Data Protection Board, *Guidelines 7/2020 on the Concepts of Controller and Processors in the GDPR*, 2/9/2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

partecipazione di entrambe le parti poiché le operazioni di entrambe le parti sono strutturalmente e inestricabilmente connesse. A tal fine rileva che una delle parti – nel caso qui preso in esame l'università – partecipi nella definizione di quali dati sono raccolti e di quali interessati del trattamento sono coinvolti negli utilizzi secondari da parte del contitolare – in specie, una terza piattaforma. L'accertamento deve avvenire in concreto alla luce delle circostanze specifiche e non sulla base di mere dichiarazioni formali[26].

Quel che appare più interessante è che, laddove si verifichi una situazione di contitolarità, la previsione di cui all'art. 26 RGDP richiede una ripartizione delle rispettive responsabilità in punto di protezione dei dati personali, «mediante un accordo interno». Ciò significa, dunque, che sia per quanto riguarda il trattamento originario sia – soprattutto – per quanto concerne gli usi secondari, il riparto delle responsabilità tra università e imprese terze è da definirsi per via contrattuale. Ciò potrebbe sembrare rassicurante in una situazione nella quale le università potrebbero efficacemente imporre alle piattaforme terze clausole limitative della facoltà di queste ultime di eseguire trattamenti ulteriori. Il rilievo dato allo strumento contrattuale dal Regolamento generale in materia di dati personali è tuttavia più problematico in una dimensione quale quella del mercato dell'educazione digitale, in cui si registrano notevoli asimmetrie di potere contrattuale e in cui l'imposizione delle *privacy policies* standardizzate delle grandi piattaforme sono suscettibili di comprimere gli spazi di autonomia delle università: in assenza di strumenti di contrattazione collettiva volti a rafforzare il potere contrattuale delle università ovvero, ancor più in radice, in assenza di soluzioni alternative alle infrastrutture digitali private, come infrastrutture digitali pubbliche e open source per le università, il rischio che si profila è quello del libero gioco degli usi secondari dei dati sull'educazione nel più ampio – e sconfinato – territorio dei mercati digitali,

[26] Corte di giustizia, *Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629.

governato dal potere – di mercato e contrattuale – delle grandi imprese digitali.

4. *Conclusioni: verso una ponderata apertura all'IA in università*

Gli scenari tracciati in questo contributo rivelano i rischi connessi all'esternalizzazione di servizi digitali a soggetti terzi che non perseguono finalità pubbliche bensì commerciali. Questi rischi si riducono, da ultimo, alla «libera» circolazione di dati sull'educazione dei cittadini europei in mercati che possono essere molto lontani da quelli dell'educazione. Al contempo, si è suggerito come l'ingresso di piattaforme digitali e degli strumenti digitali e di intelligenza artificiale nel campo dell'educazione sia destinato a consolidare alcuni processi, in parte già in atto, di privatizzazione e commercializzazione delle istituzioni di istruzione.

Queste derive del sistema appaiono essere direttamente facilitate dall'attuale quadro normativo offerto dal Regolamento generale in materia di protezione di dati personali, che – ad un esame più attento – fornisce alcune flessibilità che ben potrebbero essere impropriamente sfruttate sia dalle società fornitrici di servizi digitali (e ciò ad esempio attraverso *privacy policies* vaghe) sia dalle stesse università che potrebbero vedere nel riuso dei dati occasioni di perfezionamento (o personalizzazione) del sistema educativo di cui queste fanno parte ma anche – soprattutto in caso di università private – ulteriori occasioni di sfruttamento commerciale.

Alla luce di queste possibili derive dei processi di digitalizzazione dell'università, risulta quanto più urgente la riflessione circa la contestualizzazione degli standard normativi offerti dalla disciplina in materia di protezione dei dati personali nel settore specifico dell'educazione digitale. È questo il primo passo necessario per mantenere – o recuperare – il controllo sugli spazi digitali di insegnamento e di istruzione. Lo sbilanciamento (contrattuale) a tutto favore delle piattaforme digitali fornitrici dei servizi di

comunicazione, archiviazione e sorveglianza in cui questi spazi si articolano rischia, altrimenti, di preludere ad una standardizzazione dei contenuti culturali e, da ultimo, ad uno svuotamento dall'esterno della missione pubblica delle università.