Essays

Protezione dei dati personali e ricerca scientifica: un rapporto controverso ma necessario

Francesco Di Tano*

PROTECTION OF PERSONAL DATA AND SCIENTIFIC RESEARCH: A CONTROVERSIAL BUT NECESSARY RELATIONSHIP

ABSTRACT: In a social context of rapid technological evolution, scientific research must be inspired by respect for ethical principles, to protect the human rights and freedoms of research participants and to guarantee the lawful processing of their personal data, as also established by the ethical review process of the European scientific research framework programs. However, during the research activities, ethical and legal uncertainties and criticalities may be encountered, which require particular attention and intervention to remove any obstacles and make the pursuit of scientific research purposes more efficient while respecting the rights of the participants and data subjects involved.

KEYWORDS: Scientific research; ethics; privacy; data protection; artificial intelligence

SOMMARIO: 1. Introduzione – 2. I requisiti etici e di protezione dei dati personali dei progetti di ricerca scientifica – 3. Le principali criticità di carattere etico-giuridico – 3.1. L'inquadramento dei ruoli e delle responsabilità sul trattamento dei dati personali in ambito progettuale – 3.2. Il riuso dei dati personali a fini di ricerca – 3.3. L'intelligenza artificiale nella ricerca scientifica e il rispetto dei diritti e delle libertà delle persone – 4. Riflessioni conclusive.

1. Introduzione

La ricerca scientifica è stata, ed è tuttora, fortemente influenzata dalla rapida evoluzione tecnologica, che ha rivoluzionato le modalità di comunicazione e consentito l'utilizzo di strumenti sempre più sofisticati nelle attività umane. Se i benefici di questi nuovi sviluppi sono innegabili, sorgono, al tempo stesso, preoccupazioni di carattere etico per gli impatti imprevedibili che possono derivare dalle intense interazioni tra le nuove tecnologie e il tessuto sociale.

Nello specifico e delicato ambito della ricerca medica e biomedica sugli esseri umani, la sensibilità ai principi etici si è sviluppata in un percorso originatosi dalla Dichiarazione di Helsinki della World Medical Association, la cui prima edizione risale al 1964, che riconosce esplicitamente la prevalenza dei diritti e degli interessi dei singoli soggetti partecipanti alla ricerca sullo scopo della ricerca medica di generare nuove conoscenze non possa mai prevalere sui diritti e sugli interessi dei singoli soggetti partecipanti alla ricerca.

* *Assegnista di ricerca presso il Centro Interdipartimentale Alma Mater Research Institute for Human-Centered Artificial Intelligence – (Alma AI), Alma Mater Studiorum – Università di Bologna. Mail: francesco.ditano@unibo.it.* *Contributo sottoposto a doppio referaggio anonimo.*

ISSN 2284-4503

Ad essa, si sono poi affiancati strumenti giuridicamente vincolanti come la Convenzione 108 di Strasburgo per la protezione delle persone fisiche con riguardo al trattamento automatizzato dei dati personali del 1981, la Convenzione di Oviedo sui diritti umani e la biomedicina del 1997, la Carta dei diritti fondamentali dell'Unione Europea, che prevede principi giuridici applicabili anche alla ricerca medica, e, più di recente, il Regolamento (UE) 536/2014 sulla sperimentazione clinica di medicinali per uso umano e il Regolamento (UE) 679/2016 sulla protezione dei dati personali (General Data Protection Regulation – GDPR).

È particolarmente evidente, dunque, come l'Unione Europea abbia riposto sempre maggiore attenzione agli aspetti etici e privacy nella ricerca scientifica. E ciò si è riverberato ancor di più sui suoi programmi quadro di ricerca e innovazione, attraverso i quali, finanziando i progetti di ricerca più meritevoli, viene attuata la politica comunitaria in materia di scienza e innovazione.

La tutela dei diritti fondamentali alla privacy e alla protezione dei dati nei progetti finanziati da Horizon 2020, prima, e Horizon Europe, oggi, è difatti tra le principali priorità del processo di revisione etica.

Il GDPR ha rappresentato una svolta normativa dirompente, andando a introdurre nell'ordinamento giuridico degli Stati membri dell'Unione Europea nuovi principi ed elementi giuridici volti ad aumentare la trasparenza e la responsabilità del trattamento dei dati e rafforzare i diritti di protezione dei dati delle persone fisiche[1]. Trattandosi di Regolamento europeo, il GDPR è direttamente applicabile nell'ordinamento di ciascuno Stato membro, ma prevede deroghe e flessibilità, concedendo alle leggi degli Stati membri di intervenire in specifici punti. Ciò è avvenuto, ad esempio, in Italia con il decreto legislativo 10 agosto 2018, n. 101, che ha modificato sensibilmente il decreto legislativo 30 giugno 2003, n. 196 (meglio conosciuto come Codice in materia di protezione dei dati personali, o Codice Privacy), anche in relazione alla ricerca scientifica.

Proprio la ricerca scientifica ha ricevuto specifica cura dal legislatore europeo[2], essendo riconosciuta meritevole di incoraggiamento e sviluppo e, dunque, di un regime più favorevole rispetto ai generali oneri e obblighi sanciti in tema di protezione dei dati personali, comunque a fronte dell'adozione di adeguate garanzie tecniche e organizzative per i diritti e le libertà degli interessati (ai sensi dell'art. 89 GDPR).

[1] Basti pensare al principio di *accountability* e a quelli di *privacy by design* e *by default*, l'adempimento della valutazione d'impatto dei trattamenti, nonché i diritti riconosciuti in capo ai soggetti interessati, le procedure di gestione di tali richieste e dei *data breach* e, infine, le misure sanzionatorie.

[2] Nell'ambito del GDPR, ai sensi del Considerando 159, «il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE. Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica».

ISSN 2284-4503

Tale regime contempla, da un lato, eccezioni al principio di limitazione delle finalità[3], al principio di limitazione della conservazione[4] e al trattamento di dati rientranti nelle categorie particolari[5]; dall'altro lato, concede al diritto dell'Unione europea e degli Stati membri di prevedere deroghe ai diritti degli interessati di cui agli articoli 14, 15, 16, 18, 21 del GDPR[6].

Si vedrà, però, come la citata normativa nazionale italiana di dettaglio e i provvedimenti del Garante per la protezione dei dati personali rendano più complessi, rispetto alle previsioni del GDPR, i trattamenti di dati personali relativi a ricerche mediche, biomediche ed epidemiologiche, anche e soprattutto nell'ambito di consorzi intraeuropei.

Il presente contributo si concentra sulle dinamiche legate al trattamento e alla protezione dei dati personali nell'ambito della ricerca scientifica finanziata con fondi pubblici e, in particolare, nel più specifico contesto della progettazione europea caratterizzata da consorzi e partenariati. A partire dalla prassi quotidiana e alla luce dell'attuale impostazione derivante da norme, provvedimenti delle Autorità e orientamenti interpretativi, l'obiettivo principale è quello di portare in evidenza le criticità che i ricercatori incontrano, anche inconsapevolmente, sotto il profilo "privacy" e, più in generale, etico e giuridico, nonché tentare di fornire chiavi interpretative e riferimenti a modelli operativi utili al raggiungimento di soluzioni possibilmente adeguate

L'analisi prende avvio, nel successivo paragrafo, dai requisiti etico-giuridici e di *data protection* che, nei progetti di ricerca internazionali e non, sono oramai costantemente richiesti (o, meglio, imposti) dalle istituzioni finanziatrici e dunque rappresentano il paradigma di riferimento per un'accountability progettuale.

[3] Art. 5, par. 1, lett. d) GDPR: «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali».

[4] Art. 5, par.1, lett. e) GDPR: «i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato».

[5] Il trattamento dei dati personali rientranti in categorie particolari è vietato per difetto salvo che ricorra una delle condizioni previste dall'art. 9 GDPR, tra cui il fatto che il trattamento sia «necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

[6] Art. 89, par. 2 GDPR: «Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità». Nell'ordinamento italiano, così come previsto dall'art. 106, comma 2, lett. f) del Codice Privacy, le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, pubblicate il 19 dicembre 2018, prevedono un'unica lieve deroga all'esercizio dei diritti, all'articolo 12: «Qualora, in caso di esercizio dei diritti di cui agli art. 15 e ss del Regolamento, sono necessarie modifiche ai dati che riguardano l'interessato, il titolare del trattamento provvede ad annotare, in appositi spazi o registri, le modifiche richieste dall´interessato, senza variare i dati originariamente immessi nell´archivio». www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069637 (ultima consultazione, 07/01/2022)

Dal conseguente necessario adeguamento etico-privacy delle attività di ricerca emergono, soprattutto nel contesto dei consorzi di ricerca europei e internazionali, difficoltà e incertezze che, in questo contributo, si intende affrontare in maniera critica.

Dapprima, ci si soffermerà su un aspetto preliminare, ma fondante, dei progetti consorziati: il rapporto intercorrente tra i partner in relazione al trattamento dei dati personali, con precisa identificazione dei ruoli e delle connesse responsabilità. Ciò, come si può immaginare, ha rilevanti ricadute su dinamiche operative quali, ad esempio, la predisposizione delle informative, i rapporti con i soggetti interessati e la gestione degli eventuali *data breach*.

Successivamente, sarà affrontato il tema del riuso dei dati personali a fini di ricerca (o uso secondario). Grazie a una crescente capacità di digitalizzare e condividere, in un mondo interconnesso, sempre più dati personali[7], i ricercatori riescono a costituire una grande quantità di dati da analizzare per vari scopi di ricerca, tanto in campo medico quanto negli altri settori scientifici[8]. L'uso così esteso di dati preesistenti può avere vantaggi considerevoli alla ricerca scientifica, tra cui la capacità analitica propria dei *big data* e, potenzialmente, la possibilità di evitare problemi che caratterizzano, a livello per lo più pratico e amministrativo, la raccolta primaria di dati. Al tempo stesso, però, l'utilizzo secondario di grandi masse di dati personali implica opportune verifiche della sussistenza di idonee basi giuridiche e garanzie a salvaguardia dei diritti e delle libertà delle persone, che consentano il superamento del principio di limitazione delle finalità sancito dal GDPR[9].

Infine, tenuto conto che nell'attuale società basata sui dati (e come appena ricordato, sui *big data*) gli algoritmi di profilazione e processi decisionali automatizzati sono una realtà in forte crescita, il contributo tratterà il rapporto tra intelligenza artificiale nella ricerca scientifica e rispetto dei diritti e delle libertà delle persone. Il GDPR ha cercato di fornire una soluzione, trasversale a tutti gli ambiti sociali, attraverso diversi strumenti: dal diritto a ricevere informazioni su logiche, significato ed effetti previsti dei processi decisionali automatizzati (artt. 13, par. 2, lett. f, 14, par. 2, lett. g, 15, par. 1, lett. h) al diritto a non essere assoggettati a tali processi, con tutele e vincoli per le limitate ipotesi in cui è comunque consentito (art. 22). Alla luce di ciò, i ricercatori sono tenuti a sviluppare o utilizzare sistemi di intelligenza artificiale rispettosi dei diritti e delle libertà delle persone interessate, ma anche ad elaborare, prima del loro utilizzo, informazioni chiare, approfondite e precise sul funzionamento degli stessi.

2. I requisiti etici e di protezione dei dati personali dei progetti di ricerca scientifica

In letteratura, si sono sviluppate posizioni discordanti sul rapporto tra attività di ricerca scientifica e l'attuale disciplina europea in materia di protezione dei dati personali. Taluni autori vedono il GDPR

[7] J. Meszaros, C. Ho, *AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR?*, in *Computer Law & Security Review*, 41, 2021.

[8] J. van de Hoven, G. Comandè, S. Ruggieri, J. Domingo-Ferrer, F. Musiani, F. Giannotti, F. Pratesi, M. Stauch, *Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications*, in *Opinio Juris In Comparatione*, 1, 2021, 131-156; D. Peloquin, M. DiMaio, B. Bierer, M. Barnes, *Disruptive and avoidable: GDPR challenges to secondary research uses of data*, in *European Journal of Human Genetics*, 28, 2020, 697-705.

[9] P. Quinn, *Research under the GDPR – a level playing field for public and private sector research?, in Life Sciences, Society and Policy*, 17, 4, 2021, 2-3; G. Malgieri, *Data protection and research: A vital challenge in the era of COVID-19 pandemic*, in *Computer Law & Security Review*, 37, 2020.

come un ostacolo dannoso per la ricerca[10], altri lamentano la mancanza di chiare linee interpretative per questo specifico ambito[11], altri ancora riconoscono una particolare ricchezza di opzioni offerta alla ricerca dal GDPR, a seconda degli attori e dei contesti[12], o identificano nel GDPR stesso la pietra angolare attorno alla quale costruire un flusso di dati sicuro e libero per la ricerca[13].

È comunque incontrovertibile il fatto che il GDPR riconosca un ruolo fondamentale alla ricerca scientifica, a partire dai Considerando 157 e 159, con cui è esplicitamente dichiarato l'obiettivo di facilitare la ricerca ed è chiarita l'interpretazione in senso lato del concetto di ricerca scientifica, da considerarsi inclusivo, ad esempio, di sviluppo tecnologico e dimostrazione, della ricerca fondamentale, della ricerca applicata, di quella finanziata da privati, nonché gli studi svolti nell'interesse pubblico nel settore della sanità pubblica. Lo stesso ventaglio di basi giuridiche potenzialmente disponibili e applicabili (dal consenso all'assistenza e terapia sanitaria di cui alle lettere a ed i dell'art. 9, paragrafo 2, o proprio la necessità per fini di ricerca scientifica esplicitamente riconosciuta dalla lettera j della medesima norma) e le eccezioni legate al riuso dei dati personali (di cui si tratterà in seguito) rinforza tale convincimento[14].

Si sono però aperti interrogativi e dubbi interpretativi. Primo fra tutti, se esista un comune assoggettamento alle medesime regole in materia di trattamento di dati personali, e dunque parità di condizioni, tra le differenti tipologie di titolari del trattamento: dall'ente universitario all'azienda pubblica ospedaliera o sanitaria, dalle piccole e medie imprese ai grandi e potenti operatori commerciali. Ciascuno di essi, normalmente operante in ambienti caratterizzati da diversi livelli di risorse e in possesso di altrettanto diverse capacità di accesso ai dati personali[15], sulla base della natura giuridica (pubblica o privata), delle caratteristiche e soprattutto dello scopo della ricerca (pubblicistico o commerciale privato), può beneficiare o meno di determinate basi giuridiche o eccezioni[16]. Tuttavia, le divergenze si appiattiscono, a parere di chi scrive, nel contesto – principale oggetto d'esame – della ricerca scientifica finanziata, evidentemente correlata a comuni obiettivi di interesse pubblico.

In questo ambito, come accennato in precedenza, il rispetto dei principi etici, volti a garantire la salvaguardia dei diritti umani e delle libertà dei partecipanti alla ricerca e la liceità del trattamento dei loro dati personali, è stato correttamente imposto a tutti i beneficiari nel processo di revisione etica appli-

[10] D. Peloquin, M. DiMaio, B. Bierer, M. Barnes, *op. cit.*; B.A. Simell et al., *Transnational Access to Large Prospective Cohorts in Europe: Current Trends and Unmet Needs*, in *New Biotechnology*, 49, 2019, 98-103; A. Wiebe, N. Dietrich, *Open Data Protection: Study on Legal Barriers to Open Data Sharing – Data Protection and PSI*, Göttingen, 2017; L. Determan, *Healthy Data Protection Law*, in *Michigan Technology Law Review*, 26, 2020, 229-278.

[11] R. Eiss, *Confusion over Data-privacy Law Stalls Scientific Progress*, in *Nature*, 584, 2020, 498.

[12] P. Quinn, *op. cit.*, 21.

[13] G. Comandè, G. Schneider, *Can the GDPR make data flow for research easier? Yes it can, by differentiating! A careful reading of the GDPR shows how EU data protection law leaves open some significant flexibilities for data protection-sound research activities*, in *Computer Law & Security Review*, 41, 2021, 2.

[14] *ibidem*.

[15] J. Hartley, J. Alford, E. Knies, S. Douglas, *Towards an empirical research agenda for public value theory*, in *Public Management Review*, 19, 5, 2017, 670-685; A. Maroto, J. Gallego, L. Rubalcaba, *Publicly funded R&D for public sector performance and efficiency: Evidence from Europe*, in *R&D Management*, 46, 2016, 564-578.

[16] G. Comandè, G. Schneider, *op. cit.*, 4-5; P. Quinn, *op. cit.*, 21-29.

cato nei recenti programmi quadro in materia di ricerca scientifica europea. Tali requisiti sono evidentemente ispirati al principale postulato etico della ricerca, secondo il quale la partecipazione (e sottoposizione) ad attività di ricerca dovrebbe essere libera, volontaria, consapevole e informata[17].

La rilevanza e l'istituzionalità dei programmi quadro europei, unite all'autorevolezza della revisione etica attuata sui progetti ivi candidati, rendono i requisiti etico-giuridici sopra menzionati un modello estendibile a ogni livello, in quanto diretta manifestazione di regole e principi riconosciuti in atti e trattati internazionali e, come tali, applicabili nel nostro ordinamento indipendentemente dall'ambito territoriale dei bandi di finanziamento dei progetti di ricerca scientifica.

A seconda degli obiettivi della ricerca, dei soggetti reclutati, della tipologia e della natura dei dati personali trattati, della metodologia adottata e dei potenziali rischi per i partecipanti, i candidati e beneficiari dei bandi di Horizon 2020 e Horizon Europe devono rispettare una serie di standard etici e giuridici, valutati periodicamente da un'apposita commissione, riflettenti i loro corrispondenti obblighi.

Sotto lo specifico profilo della protezione dei dati personali, ogni qual volta un progetto di ricerca preveda il trattamento di dati personali di persone fisiche partecipanti, i beneficiari sono chiamati a fornire approfonditi chiarimenti sui seguenti temi e adempimenti:

- le responsabilità di ciascun partner e del consorzio nel suo insieme in relazione al trattamento dei dati personali nelle attività di progetto;
- le procedure attuate (o da attuarsi) per la raccolta dei consensi informati per la partecipazione delle persone e sul trattamento dei dati personali, se del caso anche riguardanti i minori;
- i modelli delle informative sulla partecipazione alla ricerca sul trattamento dei dati personali (in linguaggio e termini comprensibili), e relativi moduli di consenso, da produrre o conservare a seconda della richiesta;
- la giustificazione del trattamento di categorie particolari di dati, potendo potenzialmente esporre i partecipanti alla ricerca a rischi più elevati e dovendo pertanto essere garantito un livello di protezione più elevato per tali operazioni di trattamento, unitamente a una descrizione completa della politica di protezione dei dati e delle disposizioni in materia di sicurezza;
- la verifica in merito a deroghe particolari in materia di diritti degli interessati o di trattamento di dati genetici, biometrici e/o sanitari previsti dalla legislazione nazionale del Paese in cui si svolge la ricerca e una dichiarazione di conformità rispetto a ciascun quadro giuridico nazionale;
- l'illustrazione di come tutti i dati personali che si intenda trattare siano pertinenti e limitati alle finalità del progetto di ricerca, secondo il principio di minimizzazione dei dati sancito dal GDPR;
- la descrizione delle misure tecniche e organizzative attuate (o da attuarsi) per la salvaguardia dei diritti e le libertà degli interessati partecipanti alla ricerca;

[17] Il fondamento giuridico del consenso informato alla partecipazione ad attività di ricerca scientifica attiene al rispetto della dignità umana e della autonomia personale ed è esplicitamente riconosciuto dai già citati Carta dei diritti fondamentali dell'Unione Europea, Convenzione di Oviedo sui diritti umani e la biomedicina, Regolamento (UE) 536/2014 sulla sperimentazione clinica di medicinali per uso umano, nonché la Dichiarazione Universale sulla bioetica e i diritti umani dell'Unesco di Parigi, del 2005. Sul punto, si veda CNR, COMMISSIONE PER L'ETICA DELLA RICERCA E LA BIOETICA, *Il consenso informato nella ricerca scientifica: Ethical Toolkit*, 2017, che evidenzia come da tale principio discenda «il diritto dei partecipanti di essere informati e il dovere del ricercatore ad informarli adeguatamente e la vincolatività dei contenuti del consenso informato per la liceità dello svolgimento delle attività di ricerca condotte con o su di essi».

- la descrizione delle misure di sicurezza attuate (o da attuarsi) per prevenire l'accesso non autorizzato ai dati personali o alle apparecchiature utilizzate per il trattamento;
- la descrizione delle tecniche di anonimizzazione e pseudonimizzazione da implementarsi;
- la conferma della nomina del Responsabile della protezione dei dati (RPD) per ciascun beneficiario titolare o responsabile del trattamento e della messa a disposizione di tutti gli interessati dei relativi dati di contatto; per i soggetti non tenuti a nominare un Responsabile della protezione dei dati ai sensi del GDPR, è necessario presentare una policy dettagliata sulla protezione dei dati per il progetto;
- in caso di trasferimento di dati personali dall'Unione Europea verso un paese extra UE o un'organizzazione internazionale, la conferma che tali trasferimenti siano conformi al Capo V del GDPR;
- nel caso in cui i dati personali siano, invece, trasferiti da un paese extra UE verso l'Unione Europea (o altro stato terzo), la conferma che tali trasferimenti siano conformi alle leggi del paese in cui i dati sono stati raccolti;
- se il progetto si dovesse basare su un ulteriore trattamento dei dati personali raccolti in precedenza (il c.d. riuso o uso secondario di dati personali), la conferma che sussista un'idonea base giuridica e che siano in atto misure tecniche e organizzative adeguate per salvaguardare i diritti degli interessati;
- se la ricerca dovesse comportare la profilazione o un processo decisionale automatizzato, ai sensi dell'art. 22 del GDPR, l'illustrazione di come gli interessati ne siano informati, quali siano la logica ad essa sottostante e le possibili conseguenze, nonché come siano tutelati i loro diritti fondamentali;
- la valutazione dei rischi etici relativi alle attività di trattamento ed elaborazione dei dati del progetto, includendo un parere se la valutazione d'impatto sulla protezione dei dati debba essere, o meno, condotta ai sensi dell'articolo 35 del GDPR;
- in caso di trattamento dei dati integrante la profilazione, il monitoraggio sistematico delle persone o il trattamento su larga scala di categorie speciali di dati, metodi intrusivi di trattamento dei dati o qualsiasi altra operazione di trattamento dei dati che possa comportare un rischio elevato per i diritti e le libertà dei partecipanti alla ricerca, la descrizione completa di tali metodi di trattamento nel protocollo di ricerca, con una valutazione dei rischi etici associati alle attività di trattamento dei dati e dei potenziali danni ai diritti dei partecipanti alla ricerca e l'ideazione di misure di mitigazione del rischio.

I requisiti etico-giuridici in questione – non necessariamente tutti – sono imposti dalla Commissione Europea in fase successiva all'avvenuta sottomissione della proposta progettuale, e dunque dopo l'avvenuta valutazione etica del progetto. A seconda delle singole situazioni – senza poter ravvisare uno standard generalizzato – il loro soddisfacimento può essere richiesto entro la stipulazione del Grant Agreement, nel corso della sua fase di preparazione e negoziazione, con la loro integrazione all'interno dello stesso accordo, oppure successivamente, tramite la produzione di *deliverables* a scadenze fissate dalla medesima Commissione Europea. In ogni caso, deve comunque avvenire prima dell'avvio di attività di ricerca coinvolgenti esseri umani, con connesso trattamento dei relativi dati personali.

In ossequio al principio di *accountability*[18], il giusto bilanciamento tra l'esigenza di coinvolgimento di partecipanti e di trattamento dei relativi dati personali, da una parte, e la tutela dei loro diritti fondamentali, dall'altra, responsabilizza (o dovrebbe responsabilizzare) i ricercatori nel corso dell'intero progetto di ricerca. A tal fine, risulta necessaria la corretta applicazione, in concreto, di principi di *ethics by design* e *by default*, nonché di *privacy by design* e *by default*, con adozione di adeguate misure tecniche e organizzative[19].

Come anticipato in precedenza, proprio i requisiti etico-giuridici previsti dalla Commissione Europea possono costituire un modello di riferimento per un compiuto e responsabile adeguamento delle attività di ricerca, in esecuzione un processo di *accountability* in relazione al trattamento dei dati personali, ed etico in generale, a partire dall'ideazione fino a giungere alla conclusione del progetto.

3. Le principali criticità di carattere etico-giuridico

Sin dalla fase di progettazione, ma soprattutto nel corso delle attività progettuali, quando si concretizza la necessità di soddisfare i requisiti etici e di protezione dei dati, si possono riscontrare situazioni di incertezza e particolare criticità sotto il profilo etico-giuridico.

Prima fra tutte, l'inquadramento dei ruoli legati al trattamento dei dati personali, e delle connesse responsabilità di chi partecipa al progetto. In particolar modo, nei consorzi, ove solitamente vi è una diversificazione delle attività di ricerca da svolgere e una relativa attribuzione delle stesse a più partner, l'identificazione di questi ultimi quali titolari autonomi, responsabili del trattamento oppure contitolari rappresenta una fondamentale necessità per la correttezza di tutte le operazioni di trattamento e può essere, al tempo stesso, oggetto di difficoltose e lunghe trattative.

In secondo luogo, il riuso dei dati personali, che nella ricerca scientifica costituisce un elemento ricorrente e di strategica importanza, porta con sé la necessità di adeguare giuridicamente siffatto trattamento, con idonee basi di legittimità compatibili non solo con il GDPR, ma anche con gli ordinamenti nazionali degli eventuali enti di ricerca coinvolti. Tale aspetto si presenta non solo nell'attualità, in relazione al singolo progetto in corso, ma anche in funzione prospettica, per quella che dovrebbe essere la lungimirante esigenza di preparare la base giuridica per il lecito riutilizzo dei dati personali nelle future attività di ricerca.

Da ultimo, lo sviluppo e l'eventuale successiva applicazione di sistemi decisionali basati interamente sull'intelligenza artificiale, che si ricollegano inevitabilmente al riutilizzo dei dati personali, spesso di ingenti quantità (*big data*) per una alimentazione il più possibile completa del sistema. Tuttavia, la necessità di tutela dei diritti delle persone coinvolte e dei relativi dati personali, non si esaurisce nella

[18] *Accountability*, in questo contesto, è inteso non solo come diretta espressione del principio sancito dal GDPR all'articolo 5, bensì, più in generale, anche come responsabilità etica e scientifica nell'intero processo di ricerca. Si vedano anche B. WAGNER, *Accountability by design in technology research*, in *Computer Law & Security Review*, 37, 2020; C.D. RAAB, *Information privacy, impact assessment, and the place of ethics*, in *Computer Law & Security Review*, 37, 2020.

[19] M, KOŠČÍK, M. MYŠKA, *Data protection and codes of conduct in collaborative research*, in *International Review of Law, Computers & Technology*, 32, 1, 2018, 141-154; D. AMRAM, *Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks*, in *Computer Law & Security Review*, 37, 2020, 2.

prima fase di raccolta, ma emerge anche e soprattutto là dove il trattamento può produrre effetti significativi sul singolo interessato. Ciò comporta, come si osserverà, oneri informativi e di intervento in capo all'ente di ricerca titolare, ai sensi degli articoli 13, 14 e 22 del GDPR, che richiedono consapevolezza dei requisiti etico-giuridici e piena padronanza dei sistemi di intelligenza artificiale per un loro sviluppo e utilizzo adeguato ed eticamente affidabile.
Per una maggior chiarezza espositiva, le suddette questioni saranno di seguito affrontate e approfondite singolarmente.

3.1. L'inquadramento dei ruoli e delle responsabilità sul trattamento dei dati personali in ambito progettuale

La conduzione di attività di ricerca scientifica eticamente e giuridicamente corrette, in linea con i principi e i requisiti prima osservati, non può prescindere da un primo, basilare, adempimento: l'identificazione del flusso di dati personali (dalla raccolta alla distruzione, passando per l'eventuale comunicazione o condivisione) abbinato all'effettiva funzione progettuale e dunque al ruolo dei soggetti coinvolti. Si tratta di stabilire i ruoli e le responsabilità di questi ultimi, ai sensi del GDPR, con ricadute anche operative sulle informazioni da fornire sul trattamento di dati personali ai soggetti partecipanti.
Come ha chiarito il Comitato europeo per la protezione dei dati (già Gruppo di Lavoro ex art. 29), i concetti di titolare, contitolare e responsabile del trattamento svolgono un ruolo cruciale nell'applicazione della normativa, poiché determinano chi sarà responsabile del rispetto delle diverse disposizioni sulla protezione dei dati e come gli interessati possano esercitare loro diritti nella pratica.
In particolare, il GDPR qualifica, all'articolo 4, n. 7, il titolare del trattamento come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri (contitolari del trattamento), determina le finalità e i mezzi del trattamento di dati personali[20]. Il responsabile del trattamento è, invece, ai sensi del successivo n. 8 del medesimo articolo, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Nei consorzi progettuali europei e internazionali, dove tra l'altro è spesso prevista una condivisione di dati personali transfrontaliera, l'assegnazione dei ruoli è altresì essenziale per individuare le leggi nazionali di adeguamento al GDPR da applicarsi alle attività dei singoli partner coinvolti e, con esse, le (eventuali) relative estensioni o deroghe alla disciplina comunitaria.
L'assegnazione di ruoli, e connesse responsabilità, in materia di protezione dei dati personali nel contesto di un consorzio di progetto è una sfida particolarmente ostica, che necessita di una competente analisi dei molti elementi fattuali e sostanziali. L'incertezza, anche giuridica, che può derivarne rappresenta un potenziale e serio ostacolo ai negoziati tra i partner all'inizio del progetto o, nelle situazioni

[20] Il Comitato europeo per la protezione dei dati ha riconosciuto, nelle sue *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (versione 2.0 del 7 luglio 2021), un'ulteriore distinzione tra i mezzi essenziali trattamento, che sono determinati dal titolare, e i mezzi non essenziali, che possono essere determinati da un responsabile: tra i primi, vi rientrano il tipo di dati personali trattati, la durata del trattamento, le categorie di destinatari dei dati e dei soggetti interessati; tra i mezzi non essenziali, invece, le misure di sicurezza, edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (ultima consultazione, 07/01/2022).

più critiche, ad attività progettuali già avviate, nel momento in cui sono chiamati a farlo[21]. Non è raro, infatti, imbattersi in enti che, per scarsa conoscenza della materia o per mero opportunismo, rifuggano da qualsivoglia responsabilità e rifiutino, o comunque ostacolino, l'assunzione formale di ruoli che prevedano la stipula di specifici contratti (come, ad esempio, la nomina del responsabile del trattamento o l'accordo di contitolarità). Eppure, nel contesto della protezione dei dati personali e del relativo quadro normativo, la sostanza prevale sulla forma, quale diretta manifestazione del principio di *accountability*[22].

Dunque, nella ricerca scientifica coinvolgente più soggetti, lo status e la qualifica di titolare, contitolare o responsabile del trattamento sono determinati osservando direttamente le effettive attività da svolgere e tutte le circostanze fattuali relative al trattamento.

Oltretutto, lo stesso soggetto può agire contemporaneamente come titolare per determinati trattamenti e come responsabile per altri, anche all'interno del medesimo progetto di ricerca, e la qualifica deve essere valutata in relazione a ciascuna specifica attività di trattamento dei dati. Non è da escludere, difatti, che in un unico progetto possano emergere più operazioni di trattamento sugli stessi dati, diverse tra loro e aventi contitolarità o titolarità anch'esse differenti.

Analogamente, anche la valutazione della contitolarità dovrebbe essere effettuata sulla base di un'analisi sostanziale, piuttosto che formale, dell'effettiva influenza sulle finalità e sui mezzi del trattamento. Un criterio unicamente formale non sarebbe idoneo poiché, in alcuni casi, potrebbe mancare la nomina formale di un contitolare, mentre, in altri, tale nomina, seppur esistente, potrebbe non rispecchiare la realtà ad attribuire formalmente il ruolo di contitolare a un soggetto che di fatto non è in grado di determinare le finalità e i mezzi del trattamento.

Ovviamente, non tutti i trattamenti che coinvolgono più soggetti danno luogo a contitolarità, in special modo in ambito progettuale. Anche in questo caso, il criterio fondamentale per determinare la sussistenza di una contitolarità è la partecipazione congiunta di due o più soggetti alla definizione delle finalità e dei mezzi di un trattamento, che incida in maniera decisiva su se e come debba avvenire. Come suggerito dalla Corte di Giustizia dell'Unione Europea[23], la convergenza delle decisioni su finalità

[21] R. BECKER, A. THOROGOOD, J. BOVENBERG, C. MITCHELL, A. HALL, *Applying GDPR Roles and Responsibilities to Scientific Data Sharing*, 2021, ssrn.com/abstract=3851128 (ultima consultazione, 07/01/2022).

[22] Il Comitato europeo per la protezione dei dati ha esplicitamente chiarito, nelle già citate *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, che «*the concept of controller is a functional concept, it is therefore based on a factual rather than a formal analysis*». In ogni caso, anche il Garante per la protezione dei dati personali, nella vigenza della previgente disciplina legislativa nazionale, era già intervenuto in casi concreti prescrivendo la formale designazione, quali responsabili del trattamento, di soggetti identificati come autonomi titolari del trattamento, sebbene nella sostanza fossero effettivamente dei responsabili esterni. Si vedano, in particolare, i provvedimenti del 29 aprile 2009, www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1617709 (ultima consultazione, 07/01/2022), e n. 230 del 15 giugno 2011, www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1821257 (ultima consultazione, 07/01/2022).

[23] *Ex multis*: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie (C-210/16), Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta (C-25/17), Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV (C-25/17), -40/17). È, comunque, da precisare che tali sentenze sono state emesse dalla Corte sull'interpretazione del concetto di contitolare riguardo alla Direttiva 95/46/CE, ma gli elementi qualificanti rimangono i medesimi anche nel vigore dell'attuale normativa europea.

e mezzi si ha laddove esse si completino a vicenda e abbiano un impatto tangibile sulla determinazione finale.

Nelle situazioni più semplici, ove è un unico soggetto (proponente o coordinatore) a condurre un progetto di ricerca coinvolgente esseri umani, e uno o più terzi si limitano a fornire dati personali senza interessarsi o beneficiare dei risultati della ricerca, è abbastanza agevole identificare il primo come titolare del trattamento e i secondi quali suoi responsabili del trattamento ai sensi dell'art. 28 del GDPR.

Il proponente (o coordinatore), difatti, determina autonomamente gli obiettivi della ricerca progettuale, identifica la popolazione oggetto di studio e le categorie di dati da raccogliere ed elaborare, e stabilisce infine la metodologia. Il fornitore dei dati personali, invece, non ha alcuna influenza sugli obiettivi scientifici che indirizzano le finalità del trattamento, né tantomeno sui mezzi essenziali della ricerca e del relativo trattamento, in quanto non partecipa alla definizione della metodologia, specificando le categorie di interessati oi tipi di dati da raccogliere o comunque processare.

Vi possono, però, essere fattispecie nelle quali un partner di progetto non si limiti a fornire unicamente dati personali, ma abbia interesse a beneficiare dei risultati della ricerca. In tali situazioni, l'attenta valutazione dell'effettivo beneficio perseguito, che si tratti dell'arricchimento del proprio know-how, di riconoscimenti di contributi scientifici o della proprietà intellettuale sui risultati, può rappresentare un elemento discretivo importante per determinare la sussistenza di un rapporto di contitolarità. Ma, ancor di più, è decisiva l'effettiva partecipazione, nella fase di progettazione dell'attività di ricerca, all'identificazione degli obiettivi e degli impatti da conseguire, nonché dei metodi di svolgimento delle operazioni correlate a tutto il flusso di dati personali, dalla raccolta alla distruzione, passando per la loro conservazione.

Nella prassi, l'impegno profuso dagli enti di ricerca, all'interno dei singoli progetti, nell'inquadrare correttamente il loro ruolo può richiedere anche duraturi e complessi periodi di analisi, ragionamento e negoziazione[24].

Tutto ciò, però, può andare a discapito del rispetto delle norme previste dal GDPR e dalle singole discipline nazionali di dettaglio, oltre che dei diritti e delle libertà dei soggetti interessati, nel momento in cui la proposta progettuale si concretizza nello svolgimento delle attività. Basti pensare alla necessità di informare in maniera chiara e corretta i soggetti interessati (i partecipanti), tra le altre cose, sull'identità e i dati di contatto di titolari o contitolari del trattamento. Senza contare, oltretutto, il rispetto delle scadenze eventualmente poste dall'istituzione o ente finanziatore del progetto, come avviene per i bandi Horizon 2020 e Horizon Europe, per la dimostrazione dell'avvenuto adeguamento ai requisiti privacy richiesti.

In attesa di un'auspicabile enunciazione di linee guida e standard più precisi sul tema da parte del Comitato europeo per la protezione dei dati, una maggiore e soprattutto tempestiva attenzione a questo aspetto preliminare e propedeutico si rende necessaria da parte di chi intenda condurre o partecipare ad attività di ricerca scientifica.

[24] Una volta condiviso l'inquadramento dei ruoli, difatti, subentra la contrattazione legata alla stipulazione dei contratti di contitolarità, ai sensi dell'art. 26 del GDPR, o di nomina di responsabili del trattamento, ai sensi dell'art. 28 GDPR.

3.2. Il riuso dei dati personali a fini di ricerca

In stretta connessione con il tema della corretta identificazione, sotto il profilo della protezione dei dati personali, di ciascun ente partecipante a un progetto di ricerca, nell'ambito della ricerca scientifica emerge, con tutta la sua portata critica, il cosiddetto riuso (o uso secondario) di dati personali.
Con tale concetto si fa usualmente riferimento a ricerche condotte utilizzando (*rectius*: riutilizzando) dati personali o campioni biologici già raccolti per precedenti e differenti ricerche oppure non per scopi di ricerca, come ad esempio nel corso della pratica clinica da parte di enti ospedalieri.
Nella prassi, dati personali e campioni biologici riutilizzati nella ricerca sono solitamente codificati mediante identificatori univoci applicati delle informazioni identificative (nomi, cognomi e altri dati simili). Procedendo in questo modo, il gruppo di ricerca che li rielabora non sarebbe materialmente in grado di identificare direttamente i relativi soggetti interessati, non essendo in possesso della chiave di reidentificazione ed essendo altresì vincolato – quantomeno, si suppone – a divieti di accesso ai (o di ricezione dei) dati primari identificativi, in virtù di formali accordi con i fornitori.
Tali dati, però, sono qualificati come "pseudonimizzati" ai fini della normativa europea in materia di protezione dei dati personali. Innanzitutto, ai sensi dell'art. 4, n. 5 del GDPR, per pseudonimizzazione si intende «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». In secondo luogo, il Considerando 26 evidenzia che è «auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile». E che «i principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca».
Lo stesso Comitato europeo per la protezione dei dati ha inequivocabilmente confermato tale impostazione nel recente *Documento del Comitato europeo per la protezione dei dati sulla risposta alla domanda di chiarimenti della Commissione europea in merito all'applicazione coerente del GDPR, con un'attenzione particolare alla ricerca in campo sanitario*[25].
Conseguentemente, dovendo considerare i dati pseudonimizzati come dati personali a tutti gli effetti, ricadenti nell'ambito di applicazione della normativa in materia, il loro utilizzo (o riutilizzo) a fini di ricerca scientifica deve poggiare su una adeguata base giuridica.

[25] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Documento del Comitato europeo per la protezione dei dati sulla risposta alla domanda di chiarimenti della Commissione europea in merito all'applicazione coerente del GDPR, con un'attenzione particolare alla ricerca in campo sanitario* (2 febbraio 2021), edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf (ultima consultazione, 07/01/2022).

I problemi maggiori sorgono, in particolare per i titolari del trattamento italiani, in relazione al riuso di dati personali sanitari o genetici per finalità di ricerca scientifica, e ancor più per quella medica, biomedica o epidemiologica. Rispetto a tali tipologie di dati deve sussistere non solo una base giuridica per il trattamento, ai sensi dell'art. 6 del GDPR, ma anche una deroga, ai sensi dell'art. 9 del GDPR, al divieto generale del loro trattamento quali categorie particolari di dati.

Rispetto agli altri Paesi europei, l'ordinamento italiano prevede norme, anche contenute in provvedimenti del Garante privacy, più rigide di quelle contemplate dal GDPR. Ciò crea, come emerge nella prassi quotidiana, particolari problemi di coordinamento e omogeneizzazione delle attività di ricerca, che prevedano il riuso di dati personali appartenenti a categorie particolari, condotte presso più Paesi europei nell'ambito dei consorzi di ricerca progettuale.

Per quel che concerne il riuso di dati personali (non appartenenti a categorie particolari *ex* art. 9 del GDPR) per finalità diverse da quelle per le quali i dati siano stati inizialmente raccolti, gli ostacoli parrebbero pochi: il Considerando 50 del GDPR ne riconosce la liceità laddove il nuovo trattamento sia «compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti» e in tal caso «non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali», ma aggiunge anche che «l'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile». Inoltre, l'articolo 5, paragrafo 1, lettera b) del GDPR prevede un'eccezione al principio di limitazione delle finalità, specificando che «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali».

L'art. 89 del GDPR, in particolare, assoggetta il trattamento a fini di ricerca scientifica o storica (oltre che per fini statistici o di archiviazione nel pubblico interesse) a garanzie adeguate per i diritti e le libertà dell'interessato, che assicurino la predisposizione di misure tecniche e organizzative e, in special modo, il rispetto del principio di minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché tali finalità possano essere così conseguite. Se ugualmente possibile, però, è necessario condurre un trattamento che non preveda l'identificazione dell'interessato. Inoltre, se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione europea o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21 del GDPR se ritenute necessarie per conseguire tali finalità e nella misura in cui tali diritti rischino di rendere impossibile o di pregiudicarne gravemente il conseguimento, fatte comunque salve le condizioni e le garanzie sopra specificate[26].

L'art. 89 del GDPR è stato identificato, in letteratura, come il cardine normativo del trattamento dei dati personali per le finalità di ricerca scientifica o storica (e di archiviazione nel pubblico interesse o statistiche)[27], avente natura sia programmatica che precettiva. Programmatica, perché indirizza i legi-

[26] Per una panoramica più dettagliata sull'articolo 89 del GDPR e relativi profili controversi e questioni interpretative, si vedano: R. DUCATO, *Commento all'articolo 89 del Regolamento UE 2016/679*, in R. D'ORAZIO, G. DE GREGORIO (a cura di), *Codice della privacy e data protection*. Milano, 2021, 957-975; A. MACINATI, *Commento all'articolo 89 del Regolamento UE 2016/679*, in L. BOLOGNINI, E. PELINO (a cura di), *Codice della disciplina privacy*, Milano, 2019, 491-495.

[27] R. DUCATO, *op. cit.*, 959.

slatori nazionali ed europeo, per le loro eventuali discipline integrative, verso la realizzazione del principio di minimizzazione e il conseguimento dell'obiettivo, giuridicamente sussidiario rispetto all'interesse generale alla conoscenza, della non identificabilità dell'interessato. È, allo stesso tempo, una norma precettiva, poiché impone immediatamente il rispetto delle indicate garanzie adeguate per i diritti e le libertà dell'interessato, della minimizzazione dei dati e (se possibile) della non identificabilità degli interessati[28].

Benché, in piena coerenza con il principio di *accountability*, le garanzie non siano dettagliate puntualmente, il chiaro richiamo all'art. 32 del GDPR mediante l'esplicito riferimento alle misure tecniche e organizzative pone principalmente l'attenzione sulla sicurezza dei dati e dei processi di trattamento[29]. In questa direzione si pongono azioni come il rispetto di standard internazionali (ISO/IEC), la previsione di obblighi di segretezza e confidenzialità in capo al personale, l'implementazione dei principi di *privacy by design* e *privacy by default*, l'applicazione di tecniche di pseudonimizzazione e anonimizzazione, l'adozione di strumenti di prevenzione e *policies* interne, nonché – come rilevato dal Comitato europeo per la Protezione dei Dati[30] – aggiornamenti informativi costanti o la predisposizione di un piano di ricerca esaustivo da mettere a disposizione degli interessati[31].

L'adozione delle garanzie adeguate in questione costituisce, dunque, condizione necessaria ai fini dell'operatività dell'eccezione al principio di limitazione delle finalità riconosciuta dall'art. 5, par. 1, lett. b) del GDPR. Il Garante europeo della protezione dei dati ha, per primo, fornito un chiarimento sul concetto di presunzione di compatibilità introdotto da quest'ultima norma, escludendo che essa possa costituire un'autorizzazione generale a riutilizzare i dati, in tutti i casi, per finalità storiche, statistiche o scientifiche. Ogni fattispecie deve essere debitamente considerata in relazione alle sue specifiche circostanze e garanzie tecniche e organizzative eventualmente implementate. In linea di principio, però, i dati personali raccolti in un contesto commerciale o sanitario possono essere ulteriormente trattati per scopi di ricerca scientifica, dall'originario o da un nuovo titolare, se sono poste in essere le menzionate garanzie adeguate *ex* art. 89 del GDPR. A tal fine, il Garante ha promosso un test di compatibilità per il riutilizzo dei dati, specialmente nel contesto in cui i dati sono stati originariamente raccolti per scopi diversi o al di fuori dell'ambito della ricerca scientifica[32].

Lo stesso Comitato europeo per la protezione dei dati, intervenuto sulle sperimentazioni cliniche, pur riservandosi cautamente di intervenire in maniera specifica sul tema del riuso dei dati per fini scientifici, ha al momento ritenuto di non escludere in via generale la presunzione di compatibilità, fatte salve

[28] G.M. UDA, *Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 573-578.

[29] P. GUARDA, *Il regime giuridico dei dati della ricerca scientifica*, Napoli, 2021, 135.

[30] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679* (4 maggio 2020), edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_it.pdf (ultima consultazione, 07/01/2022).

[31] R. DUCATO, *op. cit.*, 966-967.

[32] GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *A Preliminary Opinion on data protection and scientific research* (6 gennaio 2020), edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf (ultima consultazione, 07/01/2022)

le condizioni di cui all'articolo 89 del GDPR, per l'uso secondario dei dati di sperimentazione clinica al di fuori del protocollo di sperimentazione clinica per altri fini scientifici[33].

Anche il GDPR prevede, all'art. 6, par. 4, una sorta di test per verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti. A tal fine, il titolare dovrebbe tenere conto di: (i) ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; (ii) il contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; (iii) la natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali, oppure se siano trattati dati relativi a condanne penali e a reati; (iv) le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; (v) l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Tuttavia, il GDPR non specifica come tale valutazione debba essere eseguita ed eventualmente documentata e controllata. È stato correttamente rilevato, in letteratura, come i titolari del trattamento dovrebbero condurre la valutazione seguendo le linee guida a livello europeo (come quelle del Garante europeo e del Comitato europeo) e che i risultati dovrebbero essere poi esaminati dalle autorità di controllo nazionali, con l'eventuale supporto delle eventuali autorità o comitati etici responsabili della ricerca scientifica in relazione ai singoli casi[34]. Tuttavia, attualmente non è stata ancora raggiunta, all'interno dell'Unione Europea, un'intesa comune su come disciplinare queste attività.

In Italia, in misura ora circoscritta alle ricerche mediche, biomediche ed epidemiologiche[35], il consenso è riconosciuto implicitamente, dall'Autorizzazione generale n. 9/2016 del Garante, come modificata e adeguata al GDPR mediante il Provvedimento n. 497 del 13 dicembre 2018, come la principale base giuridica per il trattamento di dati personali. In particolare, al punto 5.3 (rubricato "Consenso") del provvedimento di adeguamento di tale Autorizzazione generale al GDPR è precisato che il consenso dell'interessato «non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea» e che «quando non è possibile acquisire il consenso degli interessati, i titolari del trattamento devono documentare, nel progetto di ricerca, la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta

[33] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati (articolo 70, paragrafo 1, lettera b))* (23 gennaio 2019), edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_it.pdf (ultima consultazione, 07/01/2022).

[34] J. MESZAROS, C. HO, *op. cit.*, 2-3; D. AMRAM, *op. cit.*, 7; C. HO, *Challenges of the EU General Data Protection Regulation for Biobanking and Scientific Research*, in *Journal of Law, Information and Science*, 25, 1, 2018, 1-20.

[35] Il 13 dicembre 2018, il Garante per la protezione dei dati personali ha pubblicato il Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice. In particolare, l'Autorizzazione generale n. 9/2016 così prevede: «concernono il trattamento effettuato da: a) università, altri enti o istituti di ricerca e società scientifiche, nonché ricercatori che operano nell'ambito di dette università, enti, istituti di ricerca e ai soci di dette società scientifiche; b) esercenti le professioni sanitarie e gli organismi sanitari; c) persone fisiche o giuridiche, enti, associazioni e organismi privati, nonché soggetti specificatamente preposti al trattamento quali designati o responsabili del trattamento (ricercatori, monitor, commissioni di esperti, organizzazioni di ricerca a contratto, laboratori di analisi, ecc.) (art. 2-quaterdecies del Codice; 28 del Regolamento UE 2016/679)», www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972 (ultima consultazione, 07/01/2022).

impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca». Tra tali ragioni vi rientrano esplicitamente:

(i) motivi etici riconducibili alla circostanza che l'interessato ignori la propria condizione;

(ii) motivi di impossibilità organizzativa nel ricontattare i soggetti interessati, all'esito di ogni ragionevole sforzo compiuto, tenendo conto delle modalità di arruolamento, della numerosità del campione, del tempo trascorso dalla prima raccolta, ivi compresi ovviamente i soggetti deceduti[36];

(iii) motivi di salute dell'interessato, impossibilitato a comprendere il contenuto dell'informativa e a prestare validamente il consenso; in tali casi, però, la ricerca deve essere volta al miglioramento dello stesso stato clinico in cui versa l'interessato e deve essere dimostrato che le finalità non possano essere conseguite mediante il trattamento di dati di persone in grado di comprendere l'informativa e prestare validamente il consenso oppure con altre metodologie di ricerca.

Tali motivi di impossibilità sono da valutarsi in maniera oggettiva e assoluta, posta la fondamentale importanza del diritto alla protezione dei dati personali, in special modo quelli relativi alla salute, e il semplice dubbio sull'incapacità di comprensione dell'interessato per motivi di salute o la difficoltà, seppur alta, nel ricontattare gli interessati, non possono soddisfare i requisiti in questione.

Quanto al trattamento di dati appartenenti alle categorie particolari per finalità di ricerca scientifica, l'articolo 9 del GDPR contempla espressamente, tra le condizioni di liceità, la sua necessità «a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

Da una prima lettura, anche superficiale, parrebbe già di per sé concesso alle attività di ricerca scientifica il trattamento di dati rientranti nelle categorie particolari. In realtà, prevedendo come base il «diritto dell'Unione o nazionale», è comunque richiesto l'intervento del legislatore europeo o, in alternativa, di quello nazionale, tramite adozione di norme specifiche, con potenziali condizioni differenti tra Stato membro e Stato membro. Inoltre, è da considerarsi comunque necessario il raggiungimento degli scopi di cui all'art. 89, con applicazione di misure tecniche e organizzative appropriate rispetto alla particolare sensibilità dei dati oggetto di trattamento.

Più nello specifico, anche in relazione a tali categorie di dati personali, nell'ordinamento italiano si erge un altro provvedimento del Garante, intervenuto anch'esso in epoca antecedente al GDPR e successivamente adattato con aggiornamenti *ad hoc* al GDPR: le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018. All'articolo 7 di tali Regole, è previsto che i soggetti rientranti nell'ambito di applicazione[37] possano

[36] In tali casi, resta comunque «fermo l'obbligo di raccogliere il consenso al trattamento dei dati degli interessati inclusi nella ricerca in tutti i casi in cui, nel corso dello studio, sia possibile rendere loro un'adeguata informativa e, in particolare, laddove questi si rivolgano al centro di cura, anche per visite di controllo».

[37] Le Regole Deontologiche si applicano, secondo l'articolo 2, comma 1, «all'insieme dei trattamenti effettuati per scopi statistici e scientifici – conformemente agli standard metodologici del pertinente settore disciplinare –,

trattare le particolari categorie di dati per scopi statistici e scientifici esclusivamente quando l'interessato abbia espresso liberamente il proprio consenso sulla base degli elementi previsti nell'informativa. È, dunque, inequivocabilmente sancito il consenso quale base giuridica del trattamento di categorie particolari di dati per finalità di ricerca scientifica.

Ad ogni modo, con il D. Lgs. 10 agosto 2018, n. 101, il legislatore italiano ha introdotto nel Codice in materia di protezione di dati personali l'art. 110[38], che esclude l'obbligo del consenso per il solo trattamento di dati sanitari, a fini di ricerca scientifica in ambito medico, biomedico o epidemiologico, quando: (i) la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'UE ed è condotta e resa pubblica una valutazione di impatto; (ii) a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, e sono adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, mentre il programma di ricerca è stato oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e viene sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del GDPR.

Si tratta di una sostanziale replica del contenuto dell'Autorizzazione generale n. 9/2016, seppur in misura strettamente circoscritta.

A ciò, si deve aggiungere anche l'art. 110 *bis* del Codice[39], che prevede la facoltà del Garante di autorizzare, anche mediante provvedimenti generali, il trattamento ulteriore di dati personali a fini di ricerca scientifica da parte di soggetti terzi che svolgano principalmente tali attività quando, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione che siano adottate misure per la tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, ai sensi dell'art. 89 del GDPR. L'Autorizzazione generale n. 9/2016, così come modificata e adattata al GDPR con il citato Provvedimento n. 497/2018, rientra in tale previsione normativa. In tutti gli altri casi, in mancanza di autorizzazioni generali, il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto.

Ciò può rappresentare, innanzitutto, una preoccupante incertezza in capo al ricercatore italiano, che si vede costretto a una trepidante attesa di una valutazione decisiva, da parte del Garante, riguardo alle stesse prospettive di ricerca, laddove il riuso dei dati costituisca un elemento essenziale[40]. In se-

di cui sono titolari università, altri enti o istituti di ricerca e società scientifiche, nonché ricercatori che operano nell'ambito di dette università, enti, istituti di ricerca e soci di dette società scientifiche».

[38] E. PELINO, *Commento all'articolo 110 del D.lgs. 196/2003*, in L. BOLOGNINI, E. PELINO (a cura di), *Codice della disciplina privacy*, Milano, 2019, 121-126.

[39] E. PELINO, *Commento all'articolo 110-bis del D.lgs. 196/2003*, in L. BOLOGNINI, E. PELINO (a cura di), *Codice della disciplina privacy*, Milano, 2019, 155-158.

[40] P. GUARDA, *op. cit.*, 167-168, il quale ha rilevato come la procedura di autorizzazione *ex* art. 110 *bis* del Codice Privacy, oltre ad andare in contrasto con la disciplina prevista a livello europeo (artt. 9 e 89 del GDPR) subordinante il trattamento dei dati sanitari per finalità di ricerca alla sola adozione di misure tecniche e organizzative per rispettare il principio di minimizzazione, sia particolarmente pretenziosa, essendovi un concreto rischio di rigetto delle richieste non per motivi di merito quanto per l'oggettiva impossibilità di valutarle nel dettaglio nel termine indicato.

condo luogo, comunque connesso al primo, l'incertezza può essere trasferita anche su tutto il consorzio di progetto, nel caso in cui l'ente di ricerca italiano ne faccia parte. E, in contesti internazionali, governati da forte competizione e tempi particolarmente ristretti, ciò può non essere tollerato[41].

In ogni caso, l'ultimo comma dell'art. 110 *bis* del Codice Privacy esplicitamente chiarisce come non costituisca trattamento ulteriore da parte di terzi il riuso a fini di ricerca dei dati personali raccolti per l'attività clinica da parte degli Istituti di ricovero e cura a carattere scientifico (IRCCS), pubblici e privati, in ragione del carattere strumentale della loro attività di assistenza sanitaria rispetto alla ricerca. Si tratta, però, in tutta evidenza, di una disposizione estremamente circoscritta di cui solo pochi enti possono beneficiare e, oltretutto, esclusivamente per il riuso di dati personali raccolti nel corso della pratica clinica.

Nei contesti progettuali internazionali, questa rigorosa disciplina italiana si scontra con altre regolamentazioni nazionali, in particolar modo con quelle che, seguendo la traccia del GDPR, presentano maggiori flessibilità, come ad esempio Spagna[42], Germania[43] o Danimarca[44].

Può infatti accadere che, in un progetto internazionale congiunto, enti partner stranieri abbiano la possibilità di riutilizzare dati personali, nel rispetto del GDPR e delle rispettive normative nazionali, condividendoli all'interno del consorzio per le finalità progettuali[45]. In tali situazioni, ciascun ente di ricerca, diverso dal fornitore, che debba trattare (e, dunque, riutilizzare) tali dati è tenuto a munirsi di un'idonea base giuridica, sia che si tratti di titolarità autonoma che di contitolarità.

Pertanto, prim'ancora di confermare la partecipazione a un siffatto progetto di ricerca, e così assumere rilevanti impegni e responsabilità, il ricercatore italiano è chiamato al difficile compito di individuare la sussistenza di una base di legittimità al trattamento dei dati, nella consapevolezza che un nuovo consenso dell'interessato possa essere un'opzione alquanto remota, poiché dipendente da soggetti terzi

[41] E.B. VAN VEEN, *Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate*, in *European Journal of Cancer*, 104, 2018, 75, ha evidenziato il rischio di disomogeneità normativa derivante dalla discrezionalità degli Stati membri, che potrebbe portare a determinare contesti di maggior flessibilità e con minori limitazioni in materia di protezione dei dati personali nella ricerca scientifica, e causare dunque problemi nei progetti di ricerca internazionali, ove alcuni enti potrebbero ritenere di non poter partecipare l'impossibilità di utilizzo dei dati di loro titolarità.

[42] Disposición adicional decimoséptima (Tratamientos de datos de salud), Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, per cui il riuso dei dati personali per finalità di ricerca biomedica è considerato lecito e compatibile quando, ottenuto il consenso per una determinata finalità, i dati sono utilizzati per finalità o ambiti di ricerca attinenti all'area della ricerca originaria.

[43] § 27 (Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken), Bundesdatenschutzgesetz, per il quale il trattamento di categorie particolari di dati personali è permesso, per finalità scientifiche o finalità di ricerca storica o finalità statistiche, anche senza consenso, se tale trattamento è necessario per tali finalità e gli interessi del titolare al trattamento prevalgono sostanzialmente rispetto a quelli dell'interessato non trattare i dati.

[44] Section 10, Act No. 502 of 23 May 2018, che consente il trattamento dei dati personali senza il consenso dell'interessato al solo ed esclusivo scopo di effettuare studi statistici o scientifici di significativa importanza per la società e purché tale trattamento sia necessario per eseguire tali studi.

[45] Si pensi, ad esempio, ai progetti di ricerca finalizzati allo sviluppo di un sistema di Intelligenza Artificiale per finalità mediche o biomediche: gli enti clinici raccolgono e forniscono i dati sanitari necessari per lo sviluppo di tale sistema, solitamente riutilizzando dati clinici già a disposizione, mentre gli enti incaricati dello sviluppo devono necessariamente accedere a tutti i dati condivisi dagli enti clinici per perseguire tale finalità.

(i partner fornitori) che non sempre conservano dati di contatto degli interessati o raccolgono, a monte, il loro consenso ad essere ricontattati per nuove e ulteriori attività di ricerca.
Da ultimo, in aggiunta – anzi, parallelamente – a quanto sopra, il riuso dei dati personali si intreccia con il tema della determinazione dell'effettiva titolarità del soggetto riutilizzatore.
Specialmente nell'ambito della ricerca medica e biomedica, i ricercatori possono essere contemporaneamente legati a due o più enti distinti, gestendo personalmente per conto di questi ultimi determinate moli di dati personali, per finalità di ricerca o altro. I casi più evidenti riguardano, ad esempio, i medici universitari, legati sia all'università di riferimento come ricercatori o professori, sia all'ospedale universitario presso cui svolgono attività assistenziale, didattica e di ricerca[46].
Ebbene, è proprio in tali contesti, dai contorni un po' sfumati, che il ricercatore può confondersi nel comprendere quale sia esattamente l'ente titolare dei dati personali, ancor più se non consapevole – in maniera comunque negligente – dei principi e degli istituti basilari della normativa in materia.
Nella prassi, i set di dati sono materialmente raccolti, analizzati, conservati ed eventualmente distrutti dal ricercatore stesso, il quale può commettere l'errore di personalizzare (su di sé) la titolarità dei dati e ignorare quelli che sono, invece, anche e soprattutto gli aspetti anche formali che governano il trattamento dei dati personali. Un caso di scuola può riguardare proprio il medico universitario che, dopo aver raccolto dati personali sulla salute per conto dell'ente ospedaliero nel corso della normale pratica clinica assistenziale, intenda liberamente riutilizzare tali dati per finalità di ricerca, per conto dell'ente universitario.
Può, dunque, portare a gravi conseguenze il riuso di dati personali condotto per conto di un ente, là dove invece l'effettivo titolare sia un altro: *in primis*, l'illiceità del trattamento, con possibili sanzioni amministrative, oltre all'obbligo di risarcimento degli eventuali danni cagionati; da un punto di vista strettamente scientifico – non meno importante – l'annullamento o l'interruzione del progetto di ricerca eventualmente già avviato, con annessa distruzione dei dati raccolti ed elaborati. Senza contare, infine, gli eventuali impegni contrattuali assunti in seno a consorzi di progetto, che costituiscono un vincolo affatto esclusivamente morale.

3.3. L'intelligenza artificiale nella ricerca scientifica e il rispetto dei diritti e delle libertà delle persone

La ricerca scientifica, specialmente nell'ultimo decennio, si è dedicata con particolare attenzione allo sviluppo e all'applicazione di sistemi di intelligenza artificiale per i più disparati settori sociali ed economici: comunicazione, educazione, medicina, trasporti, giustizia, ecc.
Sfruttando un'estesa base di dati (personali e non), l'intelligenza artificiale è infatti capace di fornire risultati utili a fini scientifici e statistici. In medicina, per la diagnosi e la prognosi di malattie; nelle scienze sociali, per comprendere il comportamento sociale, economico o politico; nel commercio, per rilevare, categorizzare e prevedere le preferenze e le tendenze dei consumatori.

[46] Per un approfondimento, I. DEL GIGLIO, *La struttura del rapporto di lavoro del medico universitario*, in *Sanità Pubblica e Privata*, 3, 2017; S. LANDINI, *I medici universitari. Problemi di inquadramento del rapporto di lavoro*, in *Diritto e Salute*, 3, 2017, 1-11.

I risultati di tali elaborazioni possono avere, in molti casi, un carattere generale, non essendo legati a individui specifici ma ad analisi aggregate e anonime, e dunque non costituire dati personali nell'accezione definita dal GDPR. In altri casi, invece, come per la diagnostica sanitaria, l'applicazione è necessariamente personalizzata sul singolo paziente.

In ogni situazione, comunque, l'elaborazione statistica e scientifica può riguardare gli individui, esponendo i loro dati personali a rischi per la sicurezza e abusi. Anche non prevedendo un'applicazione individuale sul singolo soggetto, difatti, il sistema di intelligenza artificiale può essere alimentato e addestrato, in fase di sviluppo, tramite i *big data*, o comunque a set di dati costituiti da informazioni di persone fisiche identificate o identificabili[47].

Inoltre, anche i risultati meramente statistici possono influenzare indirettamente gli individui, poiché forniscono informazioni sui gruppi a cui un individuo appartiene e sulla base delle quali il singolo può subire determinate decisioni automatizzate, o comunque conseguenze rilevanti[48].

L'Information Commissioner's Office, l'autorità di controllo sui dati personali del Regno Unito, per agevolare il focus sulle funzionalità che hanno implicazioni per la privacy e la protezione dei dati, ha delineato gli elementi distintivi, rispetto alle elaborazioni più tradizionali, dei trattamenti massivi di dati personali in relazione all'intelligenza artificiale (definiti "*big data analytics*"). Tutti potenzialmente incisivi sui dati personali e sulla loro protezione. Si tratta, in particolare, di: uso di algoritmi; opacità del trattamento; tendenza a raccogliere "tutti i dati"; riutilizzo dei dati; uso di nuovi tipi di dati (come quelli forniti dai dispositivi, anziché direttamente dall'interessato, o comunque)[49].

In relazione alla tutela dei dati personali, l'intelligenza artificiale assume rilievo quando è posta alla base dei cosiddetti processi decisionali automatizzati[50], compresa la profilazione automatizzata[51]. È lo stesso GDPR a ravvisare possibili significativi rischi per i diritti e le libertà degli individui riconnessi alla tendenziale opacità dei processi, degli algoritmi e dei meccanismi automatizzati, che spesso impediscono all'interessato di conoscerne i dettagli e poter, se del caso, intervenire[52].

---

[47] G. SARTOR, F. LAGIOIA, Le decisioni algoritmiche tra etica e diritto, in U. RUFFOLO (a cura di), *Intelligenza artificiale - il diritto, i diritti, l'etica*, Milano, 2020.

[48] Si pensi, ad esempio, alla pubblicità online, ritagliata su misura o sulla base di categorizzazioni per gruppi, nonché alle decisioni automatizzate di compagnie assicurative o istituti bancari finalizzate alla promozione di offerte e premi o alla stipulazione di contratti, anch'esse basate sulla profilazione del cliente.

[49] INFORMATION COMMISSIONER'S OFFICE, Big data, artificial intelligence, machine learning and data protection, ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (ultima consultazione, 07/01/2022).

[50] GRUPPO DI LAVORO EX ART. 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* (versione del 6 febbraio 2018), secondo cui il «processo decisionale esclusivamente automatizzato consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano». Per un approfondimento sui processi decisionali automatizzati basati sull'intelligenza artificiale, si veda T. ARAUJO, N. HELBERGER, S. KRUIKEMEIER, C.H. DE VREESE, *In AI we trust? Perceptions about automated decision-making by artifcial intelligence*, in AI & Society, 35, 2020, 611-623.

[51] Art. 4, punto 4 GDPR: «la profilazione è qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

[52] Si veda, per un'estesa analisi della relazione tra il GDPR e l'intelligenza artificiale, G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, Brussels, 2020.

Alla luce di ciò, l'articolo 22, paragrafo 1 del GDPR stabilisce un divieto generale all'adozione di un processo decisionale unicamente automatizzato relativo alle persone fisiche e produttivo di effetti giuridici, o incidente in modo analogo in maniera significativa, a meno che la decisione non sia necessaria per la conclusione o l'esecuzione di un contratto, oppure sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, o infine si basi sul consenso esplicito dell'interessato. Nell'ulteriore ipotesi di trattamento di categorie particolari di dati, devono essere adottate misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato e, soprattutto, devono sussistere, come base giuridica, il consenso esplicito dell'interessato o, in alternativa, motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.

Deve trattarsi, in ogni caso, di una decisione basata unicamente sul trattamento automatizzato che abbia un effetto giuridico o incida in modo analogo significativamente su una persona fisica[53]. In caso contrario, se anche solo vi fosse un parziale intervento umano nel processo decisionale, il divieto di cui all'art. 22 del GDPR non si applicherebbe.

Ad ogni modo, in considerazione dei potenziali rischi che la decisione interamente automatizzata pone sui diritti degli interessati, il titolare del trattamento dovrebbe prestare particolare attenzione agli obblighi in materia di trasparenza. A tal fine, gli articoli 13, paragrafo 2, lettera f), e 14, paragrafo 2, lettera g) del GDPR, impongono di fornire informazioni specifiche e facilmente accessibili sul processo decisionale automatizzato.

Innanzitutto, il titolare deve comunicare all'interessato che sta svolgendo tale tipo di attività. In secondo luogo, deve fornire informazioni significative sulla logica utilizzata. Non è necessaria una spiegazione complessa degli algoritmi utilizzati, o la loro divulgazione per esteso, ma quantomeno le informazioni devono essere rese in modo tale da far comprendere agevolmente i motivi alla base della decisione. Da ultimo, il titolare è tenuto a illustrare l'importanza e le conseguenze previste di tale trattamento, fornendo esempi concreti e il più possibile chiari all'interessato.

Per i processi decisionali automatizzati basati sul consenso, quali quelli adottati nel contesto di progetti di ricerca, è inoltre imposto al titolare del trattamento di attuare misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi degli interessati. Tra tali misure, il Gruppo di Lavoro ex art. 29 ha

[53] Il Gruppo di Lavoro ex art. 29, nelle già menzionate *Linee guida sul processo decisionale automatizzato*, chiarisce, comunque, che «il titolare del trattamento non può eludere le disposizioni dell'articolo 22 creando coinvolgimenti umani fittizi. Ad esempio, se qualcuno applica abitualmente profili generati automaticamente a persone fisiche senza avere alcuna influenza effettiva sul risultato, si tratterà comunque di una decisione basata unicamente sul trattamento automatico. Per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico. Il controllo dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza per modificare la decisione».

precisato, basandosi sul Considerando 71 del GDPR[54], che debbano rientrare almeno le seguenti facoltà in capo all'interessato: richiedere e ottenere l'intervento umano, esprimere il proprio punto di vista e contestare la decisione[55].

Come è stato evidenziato in letteratura, si configura un vero e proprio principio alla conoscibilità dei dati, accompagnato dal diritto alla spiegabilità dei processi decisionali automatizzati e, in generale, dei sistemi di intelligenza artificiale[56].

D'altronde, solo una persona informata in maniera trasparente e comprensibile, e nelle condizioni di poter esercitare il proprio diritto di accesso, è in grado di esprimere il proprio parere sulla decisione automatizzata, eventualmente opponendosi ad essa, nonché verificare la presenza di errori e richiedere l'intervento per la rettifica e la correzione. Tali misure, tra l'altro, non costituiscono esclusivamente una garanzia per l'interessato, ma favoriscono anche lo stesso corretto sviluppo del processo decisionale automatizzato e la sua conseguente applicazione.

Questi limiti e adempimenti, in quanto generali, ricadono inevitabilmente anche in capo ai ricercatori, e relativi enti di ricerca, che intendono sviluppare e applicare sistemi decisionali automatizzati, in particolar modo mediante uso di intelligenza artificiale. Sebbene possano rappresentare un significativo ostacolo per l'applicazione dell'intelligenza artificiale, la ricerca scientifica può, sotto certi aspetti, esserne meno colpita, poiché l'obiettivo principale delle attività di ricerca è soprattutto – ma non solo –

[54] Il Considerando 71 del GDPR specifica, inequivocabilmente, che «tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore. Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni».

[55] GRUPPO DI LAVORO EX ART. 29, *op. cit.*, 30.

[56] M. PALMIRANI, *Big Data e conoscenza*, in *Rivista di filosofia del diritto*, 1, 2020, 85; G. MALGIERI, *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, in *Computer Law & Security Review*, 35, 2019, 3-5. Si veda anche G. MALGIERI, *"Just" Algorithms: Justification (Beyond Explanation) of Automated Decisions Under the General Data Protection Regulation*, in *Law and Business*, 1, 2021, 19-20, secondo il quale in processi decisionali automatizzati più complessi, basati sull'intelligenza artificiale, potrebbe essere difficile raggiungere un adeguato livello di spiegabilità, affrontando le cause, i fattori determinanti e i controfattuali. Una spiegazione né causale né contestuale è ritenuta inadeguata a mostrare all'interessato possibili motivi di impugnazione della decisione e quindi non è idonea ai sensi dell'articolo 22, paragrafo 3 del GDPR. Per superare questo limite della spiegazione dell'algoritmo, l'autore propone la giustificazione della decisione automatizzata, attraverso cui spiegare non solo la logica sottostante, ma anche perché sia legalmente accettabile e conforme al GDPR.

quello di produrre nuova conoscenza, piuttosto che prendere decisioni automatizzate aventi effetti sugli individui[57].

Da una parte, è senz'altro possibile che la ricerca produca decisioni basate su dati personali. Ad esempio, quando un sistema di intelligenza artificiale analizza immagini a raggi X, decide quale paziente potrebbe avere un'alta probabilità di cancro e necessita di ulteriori esami clinici.

Dall'altra parte, come già evidenziato, il trattamento è esclusivamente automatizzato e ricade, in quanto tale, nell'alveo dell'art. 22 del GDPR solo nel caso in cui la decisione, eventualmente assunta nell'ambito delle attività di ricerca o sperimentazione, sia esclusivamente automatizzata. Dunque, nel medesimo esempio, se il sistema di intelligenza artificiale dovesse assumere, in totale autonomia, una decisione in base alle immagini a raggi X, allora si tratterebbe di una decisione esclusivamente automatizzata. Laddove invece, come più spesso accade, il sistema fornisse informazioni, pur approfondite e innovative, al medico, che poi andrebbe ad assumere la decisione finale, allora non si tratterebbe di una decisione esclusivamente automatizzata, poiché il sistema di intelligenza artificiale avrebbe una funzione (anche fondamentale) di supporto a un intervento comunque umano.

Alla luce di quanto sopra, la prima importante operazione che il ricercatore deve svolgere è determinare la portata dell'applicazione dell'intelligenza artificiale e l'eventuale esclusiva automatizzazione del relativo processo decisionale.

In caso positivo, sotto il profilo della privacy e della protezione dei dati personali, entrerebbe in gioco l'articolo 22 del GDPR, con i menzionati obblighi informativi, di trasparenza e di intervento, posti in capo all'ente di ricerca titolare del trattamento. Tali adempimenti, di per sé apparentemente banali, in realtà richiedono al titolare (o ai contitolari) una precoce e piena consapevolezza delle dinamiche governanti il processo decisionale automatizzato, dal momento che le dettagliate informazioni sul funzionamento, sulla logica utilizzata e sulle conseguenze dovrebbero, a rigore di norma, essere fornite all'interessato partecipante alle attività di ricerca prima che fornisca i suoi dati e acconsenta al relativo trattamento.

Nei progetti di ricerca, questo momento può però precedere di molto l'avvio dello sviluppo o dell'applicazione del sistema decisionale automatizzato e, dunque, non è raro assistere a mutamenti, anche sensibili, degli algoritmi e delle logiche poste alla sua base rispetto alla fase di progettazione, oltre al variare delle possibili conseguenze in capo agli interessati partecipanti. In tali casi, poiché il consenso dell'interessato al trattamento dei suoi dati personali deve essere sempre informato, attuale e specifico[58], i ricercatori sono tenuti a porre un particolare attenzione sugli obblighi informativi in questione, garantendo un costante ed esatto aggiornamento della descrizione del sistema e, parallelamente, la possibilità, per l'interessato stesso, di confermare o revocare il proprio consenso a sottoporsi al processo decisionale automatizzato.

Inoltre, nel corso del progetto, eventuali errori o distorsioni nei dati raccolti o condivisi, o nello stesso sviluppo del processo decisionale automatizzato, possono portare a risultati scientificamente inesatti e a valutazioni basate su proiezioni imprecise, che possono incidere negativamente sui partecipanti

[57] J. MESZAROS, C. HO, *op. cit.*, 5.

[58] Art. 4, n. 11) GDPR: ««consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento».

alle attività progettuali. Ogni gruppo di ricerca dovrebbe, pertanto, prevedere e implementare un sistema di controllo ricorrente dei dataset raccolti e utilizzati, in modo da accertare tempestivamente eventuali distorsioni e riesaminare esattezza e pertinenza dei dati e, parallelamente, del sistema in via di progettazione o di applicazione.

Più in generale, dovendolo considerare un trattamento di dati personali vero e proprio, l'intero sviluppo del sistema decisionale basato su intelligenza artificiale deve rispettare tutti i principi in materia di protezione dei dati personali. A partire dalla *privacy by design*, che richiede, sin dalla fase di progettazione, la predisposizione di soluzioni tecniche a tutela dei dati dei soggetti interessati, in stretta correlazione con il principio di integrità e riservatezza e con la *privacy by default*, in virtù della quale tali misure devono essere garantite lungo tutto il ciclo di vita del sistema. Senza dimenticare, ovviamente, i principi fondamentali di liceità, correttezza e trasparenza, nonché di minimizzazione ed esattezza dei dati oggetto del trattamento.

Di ciò è ben consapevole, d'altronde, la stessa Unione Europea, dal momento che il Gruppo Indipendente di Esperti di Alto Livello sull'Intelligenza Artificiale, nominato dalla Commissione Europea nel giugno 2018 nell'ambito della propria strategia politica sull'intelligenza artificiale, ha elaborato gli Orientamenti Etici per un'Intelligenza Artificiale affidabile[59], presto divenute un modello di riferimento anche nell'ambito dei progetti europei finanziati dai bandi Horizon 2020 e Horizon Europe[60].

In particolare, tali linee guida promuovono una serie di sette requisiti chiave che i sistemi di intelligenza artificiale dovrebbero soddisfare per essere considerati affidabili:

- intervento e sorveglianza umani: i sistemi di intelligenza artificiale dovrebbero consentire agli esseri umani di prendere decisioni informate, promuovendo i loro diritti fondamentali, e, al tempo stesso, dovrebbero essere garantiti meccanismi di supervisione adeguati, attraverso approcci *human-in-the-loop*, *human-on-the-loop* e *human-in-command*[61];
- robustezza tecnica e sicurezza: i sistemi di intelligenza artificiale devono essere resilienti e sicuri, garantendo un piano di riserva in caso di problemi, oltre ad essere precisi, affidabili e riproducibili, al fine di garantire la prevenzione e la riduzione massima anche dei danni involontari;

[59] Gruppo Indipendente di Esperti di Alto Livello sull'Intelligenza Artificiale, *Orientamenti Etici per un'Intelligenza Artificiale affidabile* (8 aprile 2019), ec.europa.eu/newsroom/dae/document.cfm?doc_id=60430 (ultima consultazione, 07/01/2022).

[60] È la stessa Commissione Europea a prevedere, talvolta, nell'ambito della revisione etica dei progetti, l'inserimento di un apposito deliverable dedicato alla dimostrazione di un piano di affidabilità del sistema di Intelligenza Artificiale, in linea con le Ethics Guidelines for Trustworthy Artificial Intelligence del High-Level Expert Group on Artificial Intelligence.

[61] Gruppo Indipendente di Esperti di Alto Livello sull'Intelligenza Artificiale, *op. cit.*, secondo cui: «La sorveglianza può avvenire mediante meccanismi di governance che consentano approccio con intervento umano (human-in-the-loop - HITL), con supervisione umana (human-on-the-loop - HOTL) o con controllo umano (human-in-command - HIC). L'approccio HITL prevede la possibilità di intervento umano in ogni ciclo decisionale del sistema, che in molti casi non è né possibile né auspicabile. L'approccio HOTL prevede l'intervento umano durante il ciclo di progettazione del sistema e il monitoraggio del funzionamento del sistema. L'approccio HIC prevede il controllo dell'attività del sistema di IA nel suo complesso (compresi i suoi effetti generali a livello economico, sociale, giuridico ed etico) e la capacità di decidere quando e come utilizzare il sistema in qualsiasi particolare situazione».

- privacy e governance dei dati: oltre a garantire il pieno rispetto della privacy e della protezione dei dati personali, devono essere assicurati anche adeguati meccanismi di *data governance*, tenendo conto della qualità e integrità dei dati, oltre a garantire un accesso legittimo ai dati da parte di chi ne abbia diritto;
- trasparenza: i dati, il sistema di intelligenza artificiale e le logiche sottostanti dovrebbero essere trasparenti, anche grazie a meccanismi di tracciabilità e ad adeguate spiegazioni alle parti interessate; gli esseri umani devono essere consapevoli che stanno interagendo con un sistema di intelligenza artificiale e devono essere informati delle capacità e dei limiti del sistema;
- diversità, non discriminazione ed equità: devono essere evitati i pregiudizi ingiusti, che potrebbero avere molteplici implicazioni negative (emarginazione dei gruppi vulnerabili, pregiudizio, stigmatizzazione e discriminazione), e devono essere promosse la diversità e l'accessibilità generale, oltre ogni disabilità, coinvolgendo le parti interessate durante l'intero ciclo di vita;
- benessere sociale e ambientale: i sistemi di intelligenza artificiale dovrebbero essere sostenibili, rispettosi dell'ambiente e avvantaggiare tutti gli esseri umani, comprese le generazioni future;
- responsabilità (*accountability*): dovrebbero essere attuati metodi per garantire l'accountability dei sistemi di intelligenza artificiale e dei loro risultati, prima e dopo l'attuazione, quali la verificabilità di algoritmi, dati e processi di progettazione, nonché meccanismi accessibili e adeguati di ricorso in caso di effetti negativi ingiusti.

Tuttavia, la traduzione in pratica di questi requisiti e condizioni di carattere etico-giuridico, spesso sottoposta al vaglio delle istituzioni finanziatrici i progetti di ricerca, in mancanza di metodi condivisi di comprovata efficacia per lo sviluppo di sistemi affidabili di intelligenza artificiale[62], rappresenta una delle attuali maggiori sfide per i ricercatori e i relativi enti di appartenenza.

4. Riflessioni conclusive

Come si è potuto osservare, nell'ambito della ricerca scientifica finanziata, spesso coinvolgente grandi consorzi di enti pubblici e privati, sono emerse difficoltà su più fronti connessi al trattamento dei dati personali.

Da un lato, il GDPR ha in parte rivoluzionato i concetti e le definizioni dei soggetti del trattamento (superamento del responsabile interno del trattamento), imponendo al tempo stesso formalità contrattuali piuttosto articolate per le contitolarità del trattamento e le nomine dei responsabili.

Su tale preliminare aspetto, è onere dei ricercatori interrogarsi tempestivamente in merito al ruolo assunto da ciascun ente partner di progetto, analizzando con le dovute competenze tutte le sfaccettature dei trattamenti di dati personali previsti nelle attività di ricerca, e provvedere, sempre nei tempi opportuni e prima di qualsivoglia avvio di raccolta o utilizzo di dati personali, al corretto adeguamento ai sensi della normativa (contratti di contitolarità o responsabilità, informative, valutazioni d'impatto, ecc.).

[62] B. MITTELSTADT, *Principles alone cannot guarantee ethical ai*, in *Nature Machine Intelligence*, 1, 11, 2019, 501-507.

Senz'altro, gioverebbero linee guida fornite dalle competenti autorità – il Garante europeo della protezione dei dati e il Comitato europeo per la protezione dei dati, che ha disatteso l'annunciata pubblicazione entro il 2021[63] – sui trattamenti di dati personali previsti in questo specifico e delicato settore, con esempi e casistiche che aiuterebbero a orientare i ricercatori entro confini finalmente delineati, senza permettere quella frammentazione interpretativa che governa il panorama attuale.

Tale esigenza si ricollega all'altra questione critica del riutilizzo dei dati personali nell'ambito della ricerca scientifica, che sconta fortemente la diversificazione normativa in Europa tra Stato e Stato, comunque consentita dal GDPR, rappresentando un ostacolo piuttosto evidente nella prassi quotidiana[64].

Si possono considerare maturi, pertanto, i tempi per l'elaborazione di soluzioni per facilitare il riuso dei dati personali, o comunque per agevolarlo in maniera uniforme nell'Unione Europea, per importanti ricerche scientifiche (a partire da quelle mediche e biomediche), pur mantenendo adeguate protezioni sulla privacy e sulla protezione dei dati personali degli interessati.

Su questo specifico tema, se, nel breve periodo, è oltremodo difficile ambire a interventi normativi a livello europeo o dei singoli Stati membri, si attendono quantomeno con fiducia le ulteriori indicazioni promesse dal Comitato europeo per la protezione dei dati. L'intervento chiarificatore sarebbe particolarmente utile nelle aree in cui sono emersi ostacoli e rallentamenti per la comunità della ricerca, e quindi: (i) il concetto di anonimizzazione e l'eventuale riconducibilità ad esso, in determinate circostanze, dei dati pseudonimizzati[65]; (ii) la base giuridica (o le basi giuridiche) per il riuso dei dati personali per finalità di ricerca scientifica; (iii) la base giuridica per l'eventuale trasferimento transfrontaliero di dati personali a fini di ricerca scientifica[66].

Lo stesso Garante italiano avrebbe la possibilità di intervenire, mediante una nuova autorizzazione generale al trattamento dei dati personali per finalità di ricerca scientifica – in ogni area e non esclusivamente in relazione a quella medica, biomedica ed epidemiologica – come si ha attualmente con la già citata Autorizzazione generale n. 9/2016. Tale limitazione, d'altronde, non avrebbe più ragion d'essere, considerando che in ogni ambito di ricerca è oramai previsto il trattamento di dati sensibili (dati sulla salute, opinioni politiche, convinzioni religiose, origine razziale o etnica, su tutti), anche di persone vulnerabili (quali minori, anziani, migranti), e il loro uso secondario.

Anche in relazione all'intelligenza artificiale sarebbero senz'altro utili modelli e protocolli istituzionali, validati dalle autorità, che guidino i ricercatori, da un punto di vista prettamente operativo, alla realiz-

[63] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Documento del Comitato europeo per la protezione dei dati sulla risposta alla domanda di chiarimenti della Commissione europea in merito all'applicazione coerente del GDPR, con un'attenzione particolare alla ricerca in campo sanitario*, cit., 3.

[64] D. PELOQUIN, M. DIMAIO, B. BIERER, M. BARNES, *op. cit.*, 697-698.

[65] E. PODDA, M. PALMIRANI, *Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data*, in V. RODRÍGUEZ-DONCEL, M. PALMIRANI, M. ARASZKIEWICZ, P. CASANOVAS, U. PAGALLO, G. SARTOR (a cura di), *AI Approaches to the Complexity of Legal Systems XI-XII. AICOL 2020, AICOL 2018, XAILA 2020. Lecture Notes in Computer Science, vol 13048*, Cham, 2021, 279, che evidenzia, oltretutto, come l'attuale stato dell'arte sembri confermare che la pseudonimizzazione abbia un maggiore potenziale di protezione dei dati rispetto all'anonimizzazione.

[66] D. PELOQUIN, M. DIMAIO, B. BIERER, M. BARNES, *op. cit.*, 704.

zazione di sistemi affidabili e rispettosi tanto della normativa in materia di protezione dei dati personali, quanto dei principi etici sanciti dal Gruppo Indipendente di Esperti di Alto Livello sull'Intelligenza Artificiale, non sufficientemente specifici per un'applicazione pratica.

Emergono, nella recente letteratura, metodologie e modelli proposti indirizzare utilmente la progettazione, lo sviluppo e l'implementazione di sistemi di intelligenza artificiale affidabili e rispettosi dei principi etici in questione[67]. Alcuni si concentrano sugli interventi nelle prime fasi dei processi di sviluppo, attraverso l'aumento della consapevolezza delle questioni etiche tra gli sviluppatori[68], la composizione di gruppi di lavoro diversificati[69], l'incorporazione di valori etici nei sistemi attraverso una progettazione proattiva[70], la verifica dei modelli decisionali e del relativo codice sottostante[71]. Altri metodi, come le valutazioni d'impatto[72], tengono in considerazione i risultati delle applicazioni dei sistemi decisionali automatizzati, o, ancora, si preoccupano del contesto, prevedendo il coinvolgimento diretto di operatori umani[73]. Ulteriori processi, invece, si basano sulla valutazione basata sull'etica, con un costante raffronto con i principi e le norme rilevanti, al fine di controllare o influenzare il comportamento dei sistemi di intelligenza artificiale[74].

Sotto altro versante, è stato promosso un metodo per l'adeguamento etico dei sistemi di intelligenza artificiale ritenuto più potente rispetto a quello attuale dell'intelligenza artificiale "spiegabile" (eXplainable AI), incentrato su un approccio generalizzato (definito *one-size-fits-all*) e dunque incapace di

[67] J. MÖKANDER, J. MORLEY, M. TADDEO, L. FLORIDI, *Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations*, in *Science and Engineering Ethics*, 27, 4, 2021, 3-4.

[68] L. FLORIDI, J. COWLS, M. BELTRAMETTI, R. CHATILA, P. CHAZERAND, V. DIGNUM, C. LUETGE, R. MADELIN, U. PAGALLO, F. ROSSI, B. SCHAFER, P. VALCKE, E. VAYENA, *AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations*, in *Minds and Machines*, 28, 4, 2018.

[69] J. SÁNCHEZ-MONEDERO, L. DENCIK, L. EDWARDS, *What does it mean to 'solve' the problem of discrimination in hiring? Social, technical and legal perspectives from the UK on automated hiring systems*, in *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020.

[70] E. AIZENBERG, J. VAN DEN HOVEN, *Designing for human rights in AI*, in *Big Data & Society*, 7, 2, 2020; I. VAN DE POEL, *Embedding Values in Artifcial Antelligence (AI) Systems*, in *Minds and Machines*, 30(3), 2020.

[71] L.A. DENNIS, M. FISHER, N.K. LINCOLN, A. LISITSA, S.M. VERES, *Practical verifcation of decision-making in agent-based autonomous systems*, in *Automated Software Engineering*, 23, 3, 2016.

[72] ECP, *Artifcial intelligence impact assessment*, 2018, ecp.nl/wp-content/uploads/2019/01/Artificial-Intelligence-Impact-Assessment-English.pdf (ultima consultazione, 07/01/2022).

[73] F. JOTTERAND, C. BOSCO, *Keeping the "Human in the Loop" in the Age of Artificial Intelligence: Accompanying Commentary for "Correcting the Brain?" by Rainey and Erden*, in *Science and Engineering Ethics*, 26(5), 2020; I. RAHWAN, *Society-in-the-loop: programming the algorithmic social contract*, in *Ethics and Information Technology*, 20, 1, 2018.

[74] J. MÖKANDER, J. MORLEY, M. TADDEO, L. FLORIDI, *op. cit.*, 9-17; R.V. ZICARI ET AL, *Z-Inspection®: A Process to Assess Trustworthy AI*, in *IEEE Transactions on Technology and Society*, 2, 2, 2021, 83-97. Z-Inspection®, in particolare, partendo dai sette requisiti chiave che i sistemi di intelligenza artificiale dovrebbero soddisfare per essere considerati affidabili, prevede la loro concreta applicazione proponendo un processo di valutazione, praticabile e adattabile ai più disparati settori e casi d'uso, composto da tre fasi principali: una prima fase di impostazione, dedicata all'identificazione dei presupposti e dell'ambito di valutazione, oltre alla creazione di un protocollo; una fase centrale di valutazione, che prevede l'analisi dell'utilizzo del sistema di intelligenza artificiale, l'individuazione di possibili criticità etiche, tecniche e giuridiche e la loro riconduzione ai requisiti individuati dal Gruppo Indipendente di Esperti di Alto Livello sull'Intelligenza Artificiale, con annessa verifica; infine, una fase di risoluzione, che affronta le questioni etiche, tecniche e giuridiche emerse, producendo raccomandazioni e prescrizioni anche per garantire, se necessario, una costante affidabilità etica dell'intelligenza artificiale nel tempo.

soddisfare le specifiche esigenze dei singoli utenti e illustrare in maniera concreta e pragmatica il processo decisionale automatizzato, contrariamente a quanto richiesto dal GDPR e dalle linee guida del Gruppo di Esperti di Alto Livello sull'Intelligenza Artificiale. Questo metodo alternativo dell'intelligenza artificiale "esplicativa" (explanatorY AI), pur basandosi sulla "spiegabilità", intende muovere oltre, organizzando e articolando tutte le informazioni "spiegabili" in narrazioni esplicative centrate sull'utente all'interno di uno "spazio esplicativo", affinché sia l'utente stesso, nell'esplorarlo in modo interattivo attraverso un'apposita interfaccia, a prodursi la spiegazione più adatta alle proprie necessità[75].

Ad ogni modo, oltre all'adozione di promettenti modelli di questo tipo, più in generale è raccomandabile perseguire nuovi approcci e strategie per il supporto dei ricercatori nella tutela dei dati personali e nello sviluppo di sistemi di intelligenza artificiale affidabili nel corso di attività di ricerca. Formazione (anche obbligatoria) dei ricercatori sui principi etici e giuridici che governano la ricerca, composizione di gruppi di ricerca interdisciplinari che siano in grado di coprire tutti gli aspetti etico-giuridici rilevanti, assistenza da parte di personale specializzato in privacy ed etica, valutazioni da parte di comitati etici interni o esterni agli enti di ricerca[76], sono alcune delle soluzioni di immediata attuabilità che possano contribuire al necessario incremento di consapevolezza e competenza tra i ricercatori sui temi privacy ed etici, affinché possano ridursi sempre più criticità ed errori e, al contempo, anche i rischi per i diritti e le libertà delle persone coinvolte nelle attività di ricerca scientifica.

[75] M. PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in U. RUFFOLO (a cura di), *XXVI lezioni di Diritto dell'Intelligenza Artificiale*, Torino, 2021, 66-79; F. SOVRANO, F. VITALI, M. PALMIRANI, *Making Things Explainable vs Explaining: Requirements and Challenges Under the GDPR*, in V. RODRÍGUEZ-DONCEL, M. PALMIRANI, M. ARASZKIEWICZ, P. CASANOVAS, U. PAGALLO, G. SARTOR (a cura di), *op. cit.*, 173-180, i quali forniscono un esempio chiarificatore su un'applicazione di intelligenza artificiale "esplicativa": l'art. 8 del GDPR, com'è noto, fissa a 16 anni l'età minima per prestare il consenso senza l'autorizzazione del genitore o legale rappresentante, con possibilità di deroga a tale limite dal diritto interno di ciascuno Stato membro (in Italia, il limite è stato abbassato a 14 anni). In tale situazione, supponendo che un adolescente italiano di 14 anni utilizzi WhatsApp, e che suo padre voglia rimuovere l'iscrizione del figlio dalla piattaforma poiché preoccupato per la privacy, il sistema decisionale automatizzato respingerebbe la richiesta del padre a fronte della normativa italiana vigente. Laddove il padre volesse conoscere i motivi del rifiuto della sua richiesta, grazie allo strumento esplicativo incentrato sull'utente, potrebbe scegliere quali informazioni espandere (attraverso uno specifico pulsante, ad esempio) e considerare, costruendo dunque la propria spiegazione personalizzata a partire da uno spazio esplicativo predefinito.

[76] Per un approfondimento sul tema, con specifico riferimento allo sviluppo di sistemi di intelligenza artificiale affidabili nella ricerca scientifica, C. GALLESE, *Developing a Trustworthy AI culture in Scientific Research*, Conferenza "The Culture of Trustworthy AI. Public debate, education, practical learning", 2-3 Settembre 2021, Venezia, Italia, www.unive.it/pag/fileadmin/user_upload/progetti_ricerca/osai/img/grafica/OSAI21_paper_15.pdf (ultima consultazione, 07/01/2022).