ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Privacy e data protection nella ricerca scientifica

10 Ottobre 2023

Francesco Di Tano Ph.D.

Ricercatore a tempo determinato a)

Dipartimento di Scienze Giuridiche

La dimensione etica dei progetti

Quando si progetta una ricerca scientifica:

- opportuno **modellare** l'idea progettuale su solide basi etiche (*ethics by design*) e garantirne il rispetto nel corso di tutto il progetto (*ethics by default*)
- riconoscere **questioni e criticità di rilievo etico e giuridico** in relazione a obiettivi, metodologia e impatti del progetto di ricerca
- prevedere (e dimostrare) il **rispetto dei principi etici e delle normative** a fronte delle questioni etiche rilevate

La dimensione etica dei progetti

Ricerca con esseri umani:

- Coinvolgimento di individui/gruppi vulnerabili (es. minoranze, minori, disabili, pazienti, migranti, ecc…)
- Possibili interventi sui partecipanti allo studio (fisici anche comprensivi di tecnologia di imaging, trattamenti comportamentali, utilizzo di dispositivi o sensori, prelievo di campioni biologici, ecc…)
- Trattamento di dati personali

La dimensione etica dei progetti

Privacy:

- elemento preponderante dell'etica
- più fonti normative:
  - GDPR (Regolamento UE 2016/679)
  - Codice Privacy (d. lgs. 196/2003)
  - Provvedimenti del Garante Privacy
- plurimi principi ispiratori
- uso di dati personali per fini di ricerca scientifica presenta molte sfaccettature e, di conseguenza, rischi per l'interessato

L'ambito di applicazione del GDPR

Si applica ai trattamenti di dati personali:

- interamente o parzialmente automatizzati e non automatizzati di dati personali contenuti in archivio
- effettuati **da un titolare del trattamento o responsabile del trattamento che risiede nell'Unione**, indipendentemente dal fatto che il trattamento stesso sia effettuato o meno nell'UE
- **di persone fisiche che si trovano nell'Unione**, effettuato da un titolare o responsabile del trattamento al di fuori dell'Unione quando:
  - offrono beni e servizi ai residenti UE
  - monitorano il comportamento dei residenti UE

L'ambito di applicazione del GDPR

<u>Non</u> si applica ai trattamenti di dati personali:

- relativi a persone giuridiche (in quanto non personali)
- relativi ad attività che non sottostanno al diritto dell'Unione
- effettuati da una persona fisica per attività personali o domestiche
- effettuati dalle autorità competenti ai fini di prevenzione, indagine, accertamento o perseguimento di reati

I dati personali

- **dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")
- **identificabile**: persona fisica che può essere identificata, direttamente o indirettamente, attraverso altri elementi:
  - nome
  - numero di identificazione
  - ubicazione
  - identificativo online
  - altri elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Il trattamento di dati personali

- qualsiasi **operazione** o **insieme di operazioni applicate a dati personali o insiemi di dati personali**

I dati appartenenti a categorie particolari

- origine razziale o etnica
- opinioni politiche
- convinzioni religiose o filosofiche
- appartenenza sindacale
- dati genetici
- dati biometrici intesi a identificare in modo univoco una persona fisica
- dati sulla salute
- dati relativi alla vita sessuale o all'orientamento sessuale della persona

I soggetti del trattamento

- **Interessato**: **persona fisica** identificata o identificabile a cui si riferiscono i dati personali

- **Titolare del trattamento**: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le **finalità** e i **mezzi** del trattamento di dati personali
    - **possibile contitolarità del trattamento**

- **Responsabile del trattamento**: persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali **per conto** del titolare del trattamento; soggetto, **distinto dal titolare** e da lui designato, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato

I soggetti del trattamento

- **Persona autorizzata**: **persona fisica** autorizzata dal titolare o dal responsabile a compiere le singole **operazioni di trattamento** (ad esempio: dipendenti)

- **Responsabile della protezione dei dati personali (RPD – DPO)**: **consulente esperto** che osserva, valuta e organizza la gestione del trattamento di dati personali (e dunque la loro protezione) di un titolare, affinché questi siano trattati nel rispetto delle normative vigenti

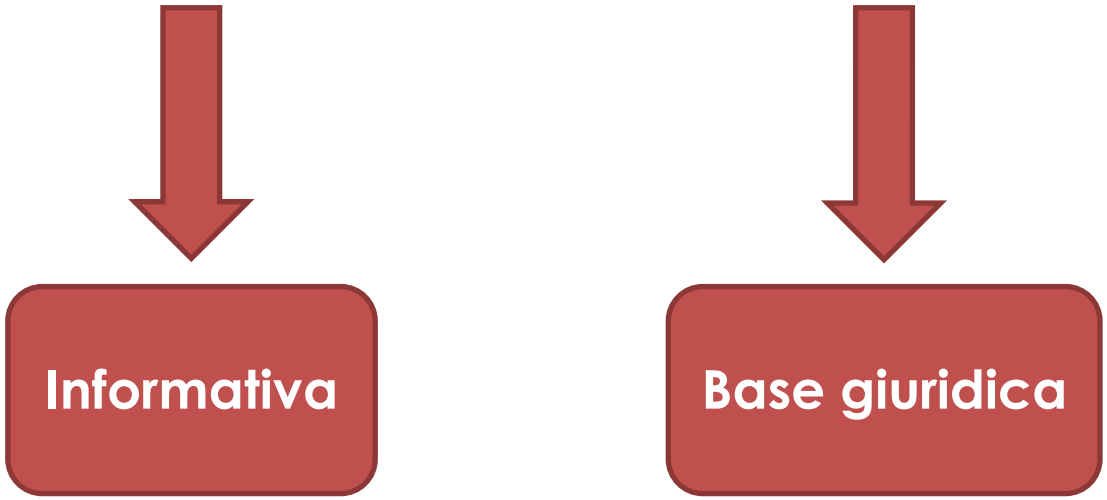
Privacy by design e by default

Il **titolare del trattamento**:

- per dimostrare la conformità alla normativa, deve adottare **politiche interne** e attua **misure** che soddisfano in particolare i principi della protezione dei dati **fin dalla progettazione** (privacy by design) e della protezione dei dati **per impostazione predefinita** (privacy by default)
- deve configurare il trattamento **prevedendo fin dall'inizio le garanzie** indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del **contesto complessivo** ove il trattamento si colloca e dei **rischi** per i diritti e le libertà degli interessati

Liceità, trasparenza e correttezza

- i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato



L'informativa: un esempio

- **Informativa generale sul trattamento dei dati personali dell'Alma Mater Studiorum – Università di Bologna**

https://www.unibo.it/it/ateneo/privacy-e-note-legali/privacy/informativa-generale-sul-trattamento-dei-dati-personali

La base giuridica

Il trattamento dei **dati personali** è **lecito** solo se (art. 6 GDPR):

a) l'interessato ha espresso il **consenso**
b) il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso
c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento
d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica
e) il trattamento è necessario per l'**esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento
f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi

La base giuridica

Il trattamento dei **dati personali appartenenti a categorie particolari** è **lecito** solo se è (art. 9 GDPR):

a) basato sul **consenso esplicito** dell'interessato

b) necessario per assolvere obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale

c) necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica, in caso di incapacità fisica o giuridica di prestare il proprio consenso

d) effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, sui membri, gli ex membri o le persone che hanno regolari contatti con tali enti

La base giuridica

a) relativo a dati personali resi manifestamente pubblici dall'interessato
b) necessario per accertare, esercitare o difendere un diritto in sede giudiziaria
c) necessario per motivi di **interesse pubblico rilevante**
d) necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali
e) necessario per motivi di interesse pubblico nel settore della sanità pubblica
f) necessario a fini di archiviazione nel pubblico interesse, di **ricerca scientifica** o storica o a fini statistici

La base giuridica: il consenso

- da prestarsi mediante un **atto positivo** inequivocabile (**scritto**, anche attraverso mezzi elettronici, od **orale**)
- intenzione **libera**, **specifica**, **informata** e **inequivocabile** di accettare il trattamento
- da prestarsi **per ogni finalità**
- se l'interessato è un minore, il consenso deve essere espresso da chi esercita la responsabilità genitoriale

La compliance privacy dei progetti

- ogni trattamento di dati personali deve possedere un'idonea **base giuridica** (artt. 6 e 9 GDPR)
- per la **finalità di ricerca scientifica**, solitamente la base giuridica è il **consenso** esplicito dell'interessato
- **Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica**: categorie particolari di dati trattabili per scopi scientifici solo previo **consenso**
- da **non confondere** consenso al trattamento dei dati personali con consenso alla partecipazione alla ricerca/allo studio
- è necessario prevedere un **distinto consenso «privacy»** per altre finalità comunque connesse alla ricerca, quali la pubblicazione di dati/interviste e la conservazione di dati di contatto del partecipante per future attività di ricerca

La compliance privacy dei progetti

- prestare grande attenzione al **riuso di dati personali** da precedenti progetti/attività necessario verificarne la liceità prima che sia troppo tardi
- non è da considerarsi lecito il c.d. ***broad consent*** il consenso deve essere specifico per ciascun singolo progetto
- necessario verificare la liceità (base giuridica) anche del **riuso** di dati personali forniti **da terzi soggetti** opportuno regolamentare tale fornitura

La compliance privacy dei progetti

Art. 110 del Codice Italiano Privacy:

- il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di **ricerca scientifica in campo medico, biomedico o epidemiologico**, **non** è necessario quando:
  - la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione, oppure
  - a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca
- il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato
- il programma di ricerca è oggetto di motivato **parere favorevole del competente comitato etico** a livello territoriale e deve essere sottoposto a **preventiva consultazione del Garante** ai sensi dell'art. 36 GDPR

La compliance privacy dei progetti

Art. 110 *bis* del Codice Italiano Privacy:

- il Garante **può autorizzare** il trattamento ulteriore di dati personali a fini di **ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività** quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, comprese forme preventive di minimizzazione e di anonimizzazione dei dati
- il Garante comunica la decisione adottata sulla richiesta di autorizzazione **entro 45 giorni**, decorsi i quali la mancata pronuncia equivale a rigetto

Minimizzazione dei dati

- i dati personali devono essere **adeguati**, **pertinenti e limitati** a **quanto necessario** rispetto alle **finalità** per le quali sono trattati

Limitazione della conservazione

- i dati personali devono essere conservati per un **tempo non superiore al conseguimento delle finalità** per le quali sono trattati
- 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

Trasferimenti di dati extra UE

- il trasferimento dei dati verso paesi extra UE è possibile solo in caso di sussistenza di almeno una delle condizioni di garanzia di cui al Capo V del GDPR

Decisione di adeguatezza (art. 45 GDPR)

- la Commissione Europea può decidere che il Paese terzo, un territorio o uno o più settori specifici all'interno del Paese terzo, o l'organizzazione internazionale in questione, garantiscono un **adeguato livello di protezione dei dati personali**
- in presenza di tale decisione, il trasferimento dei dati è possibile senza altre autorizzazioni specifiche
- esempi: USA, Svizzera, UK, Giappone, Israele (www.gpdp.it/temi/trasferimento-di-dati-all-estero)

Trasferimenti di dati extra UE

Garanzie adeguate (art. 46 GDPR)

- in mancanza di decisione di adeguatezza, il trasferimento può essere effettuato in presenza di **garanzie adeguate** (con diritti azionabili e mezzi di ricorso effettivi)
- senza autorizzazione da parte del Garante:
  - **strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici**
  - norme vincolanti d'impresa
  - **clausole contrattuali standard**
  - **codici di condotta**
  - **meccanismi di certificazione**
- previa autorizzazione del Garante:
  - **clausole contrattuali ad hoc**
  - **disposizioni in accordi amministrativi tra autorità o organismi pubblici**

Trasferimenti di dati extra UE

Deroghe (art. 49 GDPR)

- in mancanza di garanzie adeguate, è possibile trasferire i dati personali solo se si verificano specifiche **situazioni residuali**, tra cui:
  - **consenso esplicito e specifico sul trasferimento**, dopo informazione dei possibili rischi per mancanza di decisione di adeguatezza e garanzie adeguate
  - trasferimento necessario per **importanti motivi di interesse pubblico**, deducibili dal diritto dell'Unione o dello Stato membro

Trasferimenti di dati extra UE

- Quando non è possibile applicare alcuna garanzia o deroga ex artt. 46 e 49 (neanche il consenso), il trasferimento è comunque ammesso se:
  - **non è ripetitivo**
  - riguarda un **numero limitato di interessati**
  - è necessario per il perseguimento degli **interessi legittimi cogenti** del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato
- **non ripetitività**: trasferimenti in circostanze non ordinarie, al manifestarsi di condizioni casuali o ignote e a intervalli di tempo arbitrari
- è ripetitivo, ad esempio, se l'importatore di dati ottiene un accesso diretto generalizzato a una banca dati (tramite interfaccia IT)

Limitazione della finalità

- i dati personali devono essere **raccolti** per **finalità determinate, esplicite e legittime**, e trattati in modo compatibile con esse
- il trattamento per **finalità diverse** da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere **consentito solo se compatibile con le finalità** per le quali i dati personali sono stati **inizialmente raccolti**
- **in Italia:** attenzione comunque alle Regole deontologiche e agli articoli 110 e 110 bis del Codice Privacy

Integrità e riservatezza dei dati

- i dati personali devono essere trattati in maniera da **garantire un'adeguata sicurezza dei dati personali**
- deve essere garantita la protezione, mediante **misure tecniche e organizzative** adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

Misure di sicurezza

Il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative** per garantire un livello di sicurezza adeguato al rischio, tra cui, se del caso:

- **Pseudonimizzazione** e **Cifratura** dei dati
- Capacità di assicurare **riservatezza, integrità, disponibilità e resilienza dei sistemi** e dei servizi di trattamento
- Capacità di **ripristinare tempestivamente la disponibilità e l'accesso dei dati** personali in caso di incidente fisico o tecnico
- Procedura per **testare, verificare e valutare regolarmente l'efficacia delle misure** tecniche e organizzative

I diritti degli interessati

Diritti degli interessati

- Diritto di accesso
- Diritto di rettifica
- Diritto di cancellazione
- Diritto di limitazione del trattamento
- Diritto alla portabilità dei dati
- Diritto di opposizione

Il *data breach*

Violazione dei dati personali (*data breach*)

violazione di sicurezza che comporta accidentalmente o in modo illecito la **distruzione**, la **perdita**, la **modifica**, la **divulgazione non autorizzata** o l'**accesso ai dati personali** trasmessi, conservati o comunque trattati.

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Grazie per l'attenzione

Francesco Di Tano Ph.D.

Ricercatore a tempo determinato a)

Dipartimento di Scienze Giuridiche

francesco.ditano@unibo.it