Etica e protezione dei dati

giovedì 14 novembre 2018

Contenuto

I. Introduzione

La protezione dei dati è sia una questione centrale per l'etica della ricerca in Europa sia un diritto umano fondamentale. È intimamente legata all'autonomia e alla dignità umana e al principio che tutti dovrebbero essere valorizzati e rispettati. Affinché questo principio guidi lo sviluppo dell'attuale società dell'informazione, la protezione dei dati deve essere applicata rigorosamente dalla comunità della ricerca.

Il diritto alla protezione dei dati è sancito dalla Carta dei diritti fondamentali dell'UE e dal trattato sul funzionamento dell'Unione europea, che rendono effettivo il diritto alla privacy dei singoli fornendo loro il controllo sul modo in cui le informazioni su di essi vengono raccolte e utilizzate.[1]

Nel contesto della ricerca, la protezione dei dati impone ai ricercatori l'obbligo di fornire ai soggetti di ricerca informazioni dettagliate su ciò che accadrà ai dati personali che raccolgono. Richiede inoltre alle organizzazioni che trattano i dati di garantire che essi siano adeguatamente protetti, ridotti al minimo e distrutti quando non sono più necessari.

A seconda del contesto o delle informazioni in questione, la mancata protezione dei dati personali contro la perdita o l'uso improprio può avere conseguenze devastanti per gli interessati. Può anche avere gravi conseguenze legali, reputazionali e finanziarie per il Titolare del trattamento dei dati e/o il Responsabile del trattamento.[2] Molti esempi recenti di prassi di ricerca non etiche hanno riguardato la raccolta non autorizzata e/o (mis)uso dei dati personali, con conseguente azione di esecuzione da parte delle autorità di regolamentazione.

Mentre i singoli progetti di ricerca finanziati dall'UE che trattano i dati personali devono rispettare le leggi UE e nazionali sulla protezione dei dati, l'obiettivo di questo documento di orientamento è garantire che, oltre a rispettare gli obblighi legali, tutti i progetti siano guidati da considerazioni etiche e dai valori e dai principi su cui l'UE è fondata.

Particolare attenzione dovrebbe essere prestata alla ricerca che coinvolge categorie particolari di dati (precedentemente noti come dati sensibili), alla profilazione, al processo decisionale automatizzato, alle tecniche di data mining, all'analisi dei big data e all'intelligenza artificiale, in quanto tali trattamenti possono comportare rischi più elevati per i diritti e le libertà delle persone interessate (vedi Tabella 1). Il crescente impatto di queste e di altre nuove tecnologie sulla nostra vita e attività quotidiana si riflette nella lettera e nello spirito del Regolamento generale sulla protezione dei dati dell'UE – GDPR - del 2016)

Mentre il processo di revisione etica dell'UE si occupa principalmente di questioni etiche, il vostro progetto deve dimostrare la conformità con il GDPR. Tuttavia, il fatto che la vostra ricerca sia legalmente ammissibile non significa necessariamente che sarà considerata etica.

Fondamentale, se la vostra proposta di ricerca comporta il trattamento di dati personali, qualunque sia il metodo utilizzato, voi - e tutti i vostri partner, collaboratori e fornitori di servizi - dovete, se richiesto, essere in grado di dimostrare il rispetto di entrambi i requisiti legali ed etici
Tali richieste potrebbero provenire da interessati, agenzie di finanziamento o autorità di vigilanza sulla protezione dei dati.

[1] Articolo 8, Carta dei diritti fondamentali dell'UE.

[2] Le autorità di regolamentazione possono inflidire ammende fino a 20 milioni di euro o al 4 % del fatturato globale dell'entità (a seconda di quale sia più elevato).

Nello sviluppo e nell'attuazione della vostra proposta, è vostra responsabilità individuare le disposizioni giuridiche appropriate e garantire la conformità a queste. Tutti i progetti UE che trattano informazioni personali su soggetti di ricerca umana identificabili sono soggetti al GDPR. Il principio di responsabilizzazione (accountability) è fondamentale per il GDPR e richiede ai Titolari e Responsabili del trattamento di stabilire e documentare i processi di conformità alla protezione dei dati. Affrontare in modo globale le questioni relative alla protezione dei dati nella proposta di ricerca, che diventerà parte del vostro contratto se selezionati per il finanziamento, può dare un importante contributo all'*accountability* del progetto.

Si noti che oltre al GDPR, potrebbero applicare alla vostra ricerca anche la legislazione nazionale o altre misure dell'UE:

- se la proposta utilizza dati trattati o forniti da autorità responsabili della prevenzione, dell'indagine, dell'accertamento o del perseguimento di reati, può essere applicata anche la Direttiva (UE) 2016/680;
- se il progetto utilizza dati personali generati o trattati da reti elettroniche (ad esempio dati relativi a "cookie", utilizzo di Internet o traffico di rete elettronica), può essere applicata anche la Direttiva UE relativa alla vita privata e alle comunicazioni elettroniche (attualmente in fase di revisione);
- se li Stati membri dell'UE hanno stabilito le proprie norme sul trattamento dei dati, ad esempio il trattamento di categorie particolari di dati (come i dati genetici, biometrici e/o sanitari) il progetto potrebbe essere soggetto a ulteriori requisiti legali nazionali, come la notifica preventiva delle autorità di regolamentazione o delle autorità di protezione dei dati. È vostra responsabilità garantire che la vostra proposta sia conforme alle leggi sulla protezione dei dati in tutti gli Stati membri in cui vengono trattati i vostri dati di ricerca, nonché al GDPR.[3]

[3] Si vedano in particolare gli articoli 9(4), 8 e 89(3) del GDPR.

[Box 1] Questioni, concetti e definizioni chiave

"**I Dati personali**" sono definiti in modo estremamente ampio e comprendono **"qualsiasi informazione relativa a una persona fisica identificata o identificabile".** Una **"persona fisica identificabile",** o **"interessato",** è **"una persona che può essere identificata, direttamente o indirettamente, in particolare facendo riferimento a un identificativo come un nome, un numero di identificazione, dati relativi alla posizione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"** (articolo 4 (1) GDPR).

I dati personali includono dati quali indirizzi IP (Internet Protocol) (identificatori univoci che possono essere utilizzati per identificare il proprietario dei dispositivi connessi a Internet) e dati provenienti da "contatori intelligenti" che monitorano l'utilizzo di energia da parte di indirizzi collegati a persone identificabili.

Le "categorie particolari di dati personali" (precedentemente note come "dati sensibili") sono soggette a misure di protezione dei dati più rigorose. Essi comprendono "**dati personali che rivelano l'origine razziale o etnica, opinioni politiche, credenze religiose o filosofiche, o appartenenza sindacale, e il trattamento dei dati genetici, dati biometrici allo scopo di identificare in modo univoco una persona fisica, dati riguardanti la salute o i dati riguardanti la vita sessuale di una persona fisica o l'orientamento sessuale**" (articolo 9(1) GDPR).

Se il vostro progetto comporta il trattamento di categorie particolari di dati, è più probabile che sollevi problemi etici significativi. Dovete quindi giustificare l'inclusione di questo tipo di dati nel vostro progetto.

La definizione di **"trattamento dei dati"** è molto ampia. Essa comprende **"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"** (articolo 4(2) del GDPR).

È molto probabile che se il vostro progetto coinvolge dati relativi a persone identificabili, anche se non partecipano direttamente alla ricerca, state elaborando dati personali e dovete rispettare il diritto dell'UE e nazionale. Solo i dati che sono stati completamente e irreversibilmente resi anonimi sono esenti da tali requisiti. È importante sottolineare che, sebbene la **pseudonimizzazione** possa fornire un certo grado di protezione e anonimato alle singole persone interessate, i dati pseudonimizzati rientrano ancora nell'ambito dei dati personali perché è possibile identificare nuovamente la persona interessata (vedi sotto).

Anche se il progetto utilizza solo dati anonimi, l'origine o l'acquisizione dei dati può comunque sollevare problemi etici significativi.

Il GDPR impone obblighi su entrambi:

- il **"Titolare del trattamento",** che **"da solo, o congiuntamente ad altri, determina le finalità e i mezzi del trattamento dei dati personali"** e
- il **"Responsabile del trattamento",** che **"elabora i dati personali per conto del Titolare".**

È necessario assicurarsi che tutti i partner, appaltatori o fornitori di servizi che elaborano i dati di ricerca su vostra richiesta e per vostro conto rispettino il GDPR e gli standard etici H2020. Se si condivide con i partner del consorzio la responsabilità del trattamento di dati personali raccolti nel corso del progetto di ricerca, il progetto può essere oggetto di **contitolarità.** In questo caso, voi e vostri partner dovete stabilire le vostre rispettive responsabilità in un accordo a disposizione degli interessati e fornire loro un unico punto di contatto.

II. Individuare e affrontare le questioni etiche nella proposta di ricerca

Tutte i progetti di ricerca che comportano il trattamento dei dati personali devono fornire informazioni sulle disposizioni in materia di protezione dei dati nella loro proposta. È più probabile che il vostro progetto aumenti rischi etici se coinvolge:

- Il trattamento di "categorie particolari" di dati personali (precedentemente noti come "dati sensibili");
- Il trattamento di dati personali riguardanti bambini, persone vulnerabili o persone che non hanno dato il loro consenso a partecipare alla ricerca;
- complesse operazioni di trattamento e/o la diffusione di dati personali su larga scala e/o il monitoraggio sistematico di un'area accessibile al pubblico su larga scala;
- tecniche di elaborazione dei dati che sono invasive e ritenute un rischio per i diritti e le libertà dei partecipanti alla ricerca, o tecniche che sono vulnerabili ad abusi; e
- la raccolta di dati al di fuori dell'UE o trasferimento dei dati personali raccolti nell'UE a entità in paesi terzi.

[Tabella 1] Indicatori delle operazioni di trattamento dei dati che possono comportare rischi etici più elevati

Tipi di dati personali	* origine razziale o etnica * opinioni politiche, credenze religiose o filosofiche * dati genetici, biometrici o sanitari * vita sessuale o orientamento sessuale * appartenenza sindacale
Tipologia di interessati	* bambini * persone vulnerabili * persone che non hanno dato il loro esplicito consenso a partecipare al progetto
Scala o complessità dell'operazioni di trattamento dei dati	* trattamento su larga scala dei dati personali * monitoraggio sistematico di un'area accessibile al pubblico su larga scala * coinvolgimento di più set di dati e/o fornitori di servizi, o la combinazione e l'analisi di diversi set di dati (ad es. big data)
Tecniche di raccolta o elaborazione dei dati	* metodi o tecnologie invasive per la privacy (ad es. osservazione segreta, sorveglianza, monitoraggio o inganno di individui) * utilizzo di sistemi di telecamere per monitorare il comportamento o registrare informazioni sensibili * data mining (compresi i dati raccolti dalle reti di social media), "web crawling" o l'analisi dei social network * profilazione di individui o gruppi (in particolare profilazione comportamentale o psicologica)

	* utilizzo dell'intelligenza artificiale per analizzare i dati personali * utilizzo di un processo decisionale automatizzato che ha un impatto significativo sull'interessato o sugli interessati
Coinvolgimento di paesi terzi	* trasferimento di dati personali a paesi terzi * raccolta di dati personali al di fuori dell'UE

Ulteriori indicatori dei tipi di progetto e di operazioni di elaborazione dei dati che possono essere considerati a rischio più elevato sono forniti nel presente documento (vedi in particolare le sezioni sulla valutazione d'impatto sulla protezione dei dati e quella sulla profilazione, monitoraggio, sorveglianza, processo decisionale automatizzato e big data).

Se la vostra ricerca comporta un'elaborazione dei dati ad alto rischio, dovete fornire un'analisi dettagliata delle questioni etiche sollevate dalla metodologia del vostro progetto. Ciò dovrebbe comprendere:

- una panoramica di tutte le operazioni pianificate di raccolta ed elaborazione dei dati;
- l'identificazione e l'analisi delle questioni etiche sollevate; E
- una spiegazione di come s'intende mitigare questi problemi in pratica.

È necessario assicurarsi che tali questioni siano debitamente incluse e affrontate nel protocollo di ricerca che si sottopone al comitato etico per la ricerca. Potrebbe anche essere richiesto di condurre una valutazione d'impatto sulla protezione dei dati (DPIA) in linea con l'articolo 35 GDPR e le indicazioni supplementari sulle DPIA (vedi sotto).

Se la vostra istituzione ha nominato un Responsabile della Protezione dei Dati (RPD), dovreste coinvolgerlo in tutte le fasi del progetto e chiedere la sua consulenza su questioni relative alla privacy dei dati. Ciò contribuirà all'attuazione della proposta e della Convenzione di sovvenzione (le sovvenzioni dell'UE sono soggette al pieno rispetto delle norme sulla privacy dei dati).

In caso di trattamento di dati complessi, sensibili o su larga scala o di trasferimento di dati al di fuori dell'UE, è opportuno consultare il responsabile della protezione dei dati sulla compatibilità degli accordi sulla protezione dei dati con le politiche dell'istituzione ospitante e la legislazione applicabile.

Si dovrebbe includere il parere e/o la consulenza del Responsabile della protezione dei dati nella proposta. Se l'istituto ospitante non dispone di un responsabile della protezione dei dati, si raccomanda di consultare un esperto adeguatamente qualificato.

III. Pseudonimizzazione e anonimato

Uno dei modi migliori per attenuare le preoccupazioni etiche derivanti dall'uso dei dati personali è quello di anonimizzarli in modo che non si riferiscano più a persone identificabili. I dati che non si riferiscono più a persone identificabili, quali dati aggregati e statistici, o dati altrimenti resi anonimi in modo che l'interessato non possa essere nuovamente identificato, non sono dati personali e pertanto non rientrano nell'ambito di applicazione della legge sulla protezione dei dati.

Tuttavia, anche se si prevede di utilizzare solo set di dati resi anonimi, la proposta può comunque sollevare importanti questioni etiche. Questi potrebbero riguardare l'origine dei dati o il modo in cui sono stati ottenuti. È quindi necessario specificare la fonte dei set di dati che si intende utilizzare

nella proposta e affrontare eventuali problemi etici che si presentano. È inoltre necessario considerare il potenziale di abuso della metodologia di ricerca o dei risultati, e il rischio di danno per il gruppo o la comunità cui i dati si riferiscono.

Qualora sia necessario mantenere un collegamento tra i soggetti di ricerca e i loro dati personali, è necessario, ove possibile, pseudonimizzare i dati al fine di proteggere la privacy dell'interessato e ridurre al minimo il rischio per i suoi diritti fondamentali in caso di accesso non autorizzato La pseudonimizzazione e l'anonimizzazione non sono la stessa cosa ed è importante che voi siate consapevoli della differenza tra esse, in quanto il GDPR vi impone di utilizzarle laddove possibile o fattibile (articolo 89 del GDPR).

[Box 2] Pseudonimizzazione e anonimizzazione: comprendere la differenza

La pseudonimizzazione comporta la sostituzione di informazioni personali (come il nome di un individuo) con un identificatore univoco che non è collegato all'identità reale degli interessati, utilizzando tecniche come la codifica o l'hashing. Tuttavia, se è possibile identificare nuovamente le singole persone interessate invertendo il processo di pseudonimizzazione, si applicano ancora gli obblighi in materia di protezione dei dati. Esse cessano di essere applicate solo quando i dati sono completamente e irreversibilmente anonimizzati..

L'anonimizzazione comporta tecniche che possono essere utilizzate per convertire i dati personali in dati anonimi. L'anonimizzazione è sempre più difficile a causa del potenziale di re-identificazione.

La re-identificazione è il processo di trasformazione di dati pseudonimizzati o resi anonimi in dati personali mediante l'abbinamento di dati o tecniche simili.

Sebbene i dati anonimi non siano più considerati dati personali, i processi di anonimizzazione sono difficili, in particolare quando si tratta di grandi set di dati contenenti un'ampia gamma di dati personali. Questo perché è molto difficile creare set di dati completamente anonimi che conservano le informazioni granulari necessarie per gli scopi di ricerca.[4] Per quanto riguarda la vostra proposta di ricerca, se vi è una prospettiva significativa di re-identificazione delle persone i cui dati sono stati raccolti, le informazioni dovrebbero essere trattate come dati personali. È difficile valutare il rischio di re-identificazione con assoluta certezza e si dovrebbe sempre sbagliare sul lato della cautela. Un crescente numero di studi e di pubblicazioni di ricerca in cui gli individui sono identificati a partire da insiemi di dati anonimi ha dimostrato i limiti fondamentali all'anonimizzazione come tecnica per proteggere la privacy degli individui.

Se intendete rendere anonimi i dati raccolti per l'utilizzo nel vostro progetto di ricerca, la tempistica del processo di anonimizzazione è fondamentale. Si raccolgono dati "anonimizzati" solo se l'anonimizzazione avviene nel momento in cui i dati sono raccolti presso l'interessato della ricerca, in modo che nessun dato personale sia effettivamente trattato. Se l'anonimizzazione avviene in una fase successiva, ad es. l'utente intende rimuovere le informazioni personali durante la trascrizione di registrazioni audio o nel momento in cui i dati del sondaggio vengono inseriti in una banca dati, i dati grezzi sono ancora dati personali e la vostra proposta deve includere disposizioni per la loro protezione fino al momento in cui sono cancellati o resi anonimi.

In alcuni casi, l'istituto ospitante, l'ente finanziatore o l'editore potrebbe richiedere di conservare i dati grezzi per scopi di controllo, responsabilità o integrità della ricerca. Ci possono essere altri scenari in cui un istituto ospitante dispone di un set di dati grezzi che mette a disposizione dei suoi

[4] Vedere anche parere 05/2014 sulle tecniche di anonimizzazione, Gruppo di lavoro articolo 29 (adottato il 10 aprile 2014)

ricercatori e partner in forma anonima. In questi casi, mentre i destinatari dei dati resi anonimi possono - fatta salva l'attenuazione del rischio di re-identificazione - essere esentati dagli obblighi in materia di protezione dei dati, l'istituzione ospitante continua a trattare dati personali e deve pertanto garantire un'adeguata protezione dei dati grezzi (personali). Ciò include misure tecniche e organizzative per proteggere i dati e i mezzi per identificare le persone interessate (ad es. le chiavi, i codici o le applicazioni utilizzate per anonimizzare i dati) contro l'accesso o l'uso non autorizzato.
Se siete in dubbio circa l'adeguatezza delle tecniche che si intendono utilizzare, si dovrebbe chiedere il parere del proprio Responsabile della protezione dei dati o di un esperto adeguatamente qualificato Come indicato di seguito (si veda il BOX 5), per gli scenari di trattamento sensibili o complessi che comportano la pseudonimizzazione o l'anonimizzazione, può anche essere necessario condurre una DPIA al fine di garantire un livello adeguato di protezione dei dati e ridurre al minimo i rischi per i diritti delle persone interessate.

IV. Protezione dei dati fin dalla progettazione e per impostazione predefinita (Protezione dati by design and default)

Per innovare eticamente e responsabilmente, i ricercatori e gli sviluppatori sono stati a lungo incoraggiati ad applicare il concetto di privacy by design, che fornisce un quadro per focalizzare la progettazione di sistemi, banche dati e processi nrll rispetto dei diritti fondamentali degli interessati. Un concetto più ampio di protezione dei dati fin dalla progettazione, ora incluso nel GDPR, richiede ai titolari del trattamento di attuare misure tecniche e organizzative appropriate per dare effetto ai principi fondamentali del GDPR in materia di protezione dei dati (articoli 5 e 25 del GDPR). La protezione dei dati fin dalla progettazione è uno dei modi migliori per affrontare le questioni etiche che derivano dalla vostra proposta di ricerca nella fase di progettazione del vostro progetto.

In un contesto di ricerca e sviluppo, le misure volte a garantire la protezione dei dati fin dalla progettazione potrebbero comprendere;

- pseudonimizzazione o anonimato dei dati personali;
- minimizzazione dei dati (cfr. BoX 3);
- crittografia applicata (ad es. crittografia e hashing);
- l'utilizzo di fornitori di servizi e piattaforme di storage che garantiscono livelli adeguati di sicurezza sulla protezione dei dati; E
- consentire ai soggetti di esercitare i loro diritti fondamentali (ad esempio per quanto riguarda l'accesso diretto ai loro dati personali e il consenso al loro utilizzo o trasferimento).

Quando si valuta se e come applicare il principio della protezione dei dati fin dalla progettazione, è necessario prendere in considerazione:

- la natura, la portata, il contesto e le finalità del trattamento;
- la gravità dei rischi per i diritti fondamentali degli interessati in caso di mancata protezione delle loro informazioni; E
- il costo e la disponibilità delle tecnologie e delle applicazioni di cui potreste aver bisogno.

È necessario applicare il principio della protezione dei dati fin dalla progettazione, laddove ciò possa attenuare i rischi etici derivanti dall'elaborazione dei dati nel progetto di ricerca, e spiegare nella proposta di ricerca come ciò sarà realizzato. Questo approccio è sottolineato anche dal principio della **protezione dei dati per impostazione predefinita**. **Qualora abbiate la possibilità di migliorare il livello di protezione dei dati offerto ai vostri soggetti di ricerca, dovreste applicare tali misure per**

impostazione predefinita piuttosto che considerarle o renderle disponibili come un extra facoltativo

Qualora la vostra ricerca comporti un trattamento dei dati complesso, sensibile o su larga scala, la vostra proposta dovrebbe includere una descrizione delle misure che adotterete per applicare i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, e/o per migliorare la sicurezza in modo da impedire l'accesso non autorizzato a dati personali o attrezzature.

[Box 3] Minimizzazione dei dati

Il trattamento dei dati deve **essere lecito, equo e trasparente**. **Esso dovrebbe riguardare solo i dati necessari e proporzionati** per realizzare il compito specifico o la finalità per cui sono stati raccolti (articolo 5(1) GDPR).

È quindi necessario raccogliere **solo i dati necessari per raggiungere gli obiettivi della ricerca**. La raccolta di dati personali di cui non avete bisogno per il vostro progetto di ricerca può essere considerata non etica e illegale.

In caso di dubbio sul fatto che siano effettivamente necessari tutti i dati che si intende raccogliere, è necessario effettuare **una valutazione della minimizzazione dei dati**. Questa dovrebbe essere progettata e condotta dal team di ricerca per garantire che i dati siano raccolti sulla base di una **necessità di conoscenza**, i.e. i dati sono necessari per uno scopo specifico che è rilevante e limitato agli obiettivi del progetto e alla metodologia.

La minimizzazione dei dati si applica non solo alla quantità di dati personali raccolti, ma anche nella misura in cui possono essere consultati, ulteriormente trattati e/o condivisi, alle finalità per le quali sono utilizzati e al periodo per il quale sono conservati. È necessario ridurre al minimo il trattamento per quanto possibile.

Se non siete in grado di identificare pienamente la finalità del trattamento dei dati al momento della raccolta dei dati o avete bisogno di conservare i dati oltre la durata del progetto, è necessario **spiegare e giustificare le modalità di raccolta e conservazione dei dati.**

È inoltre necessario spiegare come applicare i principi di minimizzazione dei dati e di protezione dei dati fin dalla progettazione nella pratica. In particolare, è necessario garantire che:

- sì pseudonimizzano o anonimizzano i dati, ove possibile (vedi Box 2);
- i dati sono memorizzati in modo sicuro; E
- se del caso, vengono stabilite politiche e procedure per limitare l'uso dei dati e proteggere i diritti fondamentali delle persone interessate.

V. Consenso informato al trattamento dei dati

Il consenso informato è la pietra angolare dell'etica della ricerca. Richiede di spiegare ai partecipanti alla ricerca di cosa tratta il vostro progetto, cosa comporterà la loro partecipazione ad esso e gli eventuali rischi che potrebbero essere implicati. Solo dopo aver trasmesso queste informazioni ai partecipanti – e loro le hanno pienamente comprese – potrete chiedere e ottenere il loro esplicito permesso di includerli nel vostro progetto (articoli 4 (11) e 7 GDPR).[5]

[5] Per le ricerche che comportano sperimentazioni cliniche, l'elaborazione dei dati dovrebbe inoltre essere conforme al Regolamento (UE) n 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, relativo alla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE) (OJ L 158, 27.5.2014, p. 1).

In linea di principio, gli individui non dovrebbero essere oggetto di un progetto di ricerca senza essere informati, anche nei casi relativamente rari in cui i metodi di ricerca, le condizioni o gli obiettivi impongono di non essere pienamente consapevoli della natura dello studio fino al suo completamento. Tuttavia, l'avvento di Internet e l'uso diffuso di piattaforme di social media e di altre ICTs hanno notevolmente ampliato le opportunità di ricerca sul comportamento umano senza il consenso esplicito dei soggetti. A sua volta, ciò ha creato una serie di dilemmi etici e sfide per la comunità della ricerca

Ogni volta che si raccolgono dati personali direttamente dai partecipanti alla ricerca, è necessario chiedere il loro consenso informato attraverso una procedura che soddisfi gli standard minimi del GDPR. Ciò richiede che il consenso sia dato mediante un chiaro atto affermativo che stabilisca un'indicazione libera, specifica, informata e inequivocabile del consenso dell'interessato al trattamento dei suoi dati personali. [6] Questo può assumere la forma di una dichiarazione scritta, che può essere raccolto con mezzi elettronici, o una dichiarazione orale.

Ove possibile, questo processo dovrebbe essere integrato in una più ampia procedura di consenso informato che soddisfi gli standard stabiliti nella *Nota di orientamento della Commissione Europea sul consenso informato.* Tuttavia, per i progetti che comportano operazioni di trattamento dei dati particolarmente complesse o sensibili o metodi intrusivi quali la profilazione comportamentale, la registrazione audio/video o il tracciamento geo-localizzato, è opportuno attuare uno specifico processo di consenso informato che copra la componente di elaborazione dati del progetto.

È necessario conservare le registrazioni che documentano la procedura di consenso informato, comprese le schede informative e i moduli di consenso forniti ai partecipanti alla ricerca, e l'acquisizione del loro consenso al trattamento dei dati. Tali informazioni possono essere richieste dagli interessati, dalle agenzie di finanziamento o dalle autorità di controllo per la protezione dei dati.

Affinché il consenso al trattamento dei dati sia "informato", all'interessato devono essere fornite informazioni dettagliate sul trattamento dei dati previsto in una forma intelligibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice. Come minimo, questo dovrebbe includere:

- l'identità del Titolare dei dati e, se del caso, i recapiti del DPO;
- gli scopi specifici del trattamento per il quale saranno utilizzati i dati personali;
- i diritti del soggetto garantiti dal GDPR e dalla Carta dei diritti fondamentali dell'UE, in particolare il diritto di ritirare il consenso o di accedere ai dati, le procedure da seguire qualora si desiderasse farlo e il diritto di presentare un reclamo a un'autorità di vigilanza;
- informazioni sulla possibilità di condivisione o di trasferimento dei dati a terzi e per quali finalità; E
- per quanto tempo i dati verranno conservati prima di essere distrutti.

Gli interessati devono inoltre essere informati se i dati devono essere utilizzati per ulteriori finalità, condivisi con partner di ricerca o trasferiti a organizzazioni al di fuori dell'UE (vedere l'articolo 13 GDPR).

Come per qualsiasi progetto di ricerca che coinvolge soggetti umani, **se il trattamento dei dati comporta rischi potenziali per i diritti e le libertà degli interessati, questi devono essere informati di tali rischi durante la procedura di consenso informato**.

[6] Vedi anche articolo 7 GDPR e *Linee guida sul consenso ai sensi del regolamento 2016/679*, articolo 29 Gruppo di lavoro (adottato il 28 novembre 2017).

La procedura di ottenimento del consenso e le informazioni fornite agli interessati dovrebbero riguardare tutte le attività di trattamento dei dati relative alla loro partecipazione alla vostra ricerca. Dal punto di vista etico della ricerca, e in conformità con i principi di un trattamento dei dati equo e trasparente, se si intende utilizzare o rendere i loro dati disponibili per i futuri progetti di ricerca, è consigliabile ottenere consenso esplicito all'uso secondario dei dati. [7] Se si prevede di utilizzare i dati in più progetti o per scopi diversi dalla ricerca, è necessario dare alle persone interessate la possibilità di rifiutare esplicitamente le ulteriori operazioni di ulteriore trattamento.

Se nel corso del vostro progetto di ricerca desiderate apportare modifiche significative alla vostra metodologia o alle sue modalità di trattamento dati che incidano sui diritti degli interessati o sull'uso dei loro dati, dovete rendere questi ultimi consapevoli delle modifiche previste e ottenere il loro consenso esplicito; non è sufficiente offrire loro la possibilità di rinunciare. Questa operazione deve essere eseguita **prima** di apportare le modifiche.

Se il progetto comporta un trattamento di dati complesso e su larga scala, se si prevede di utilizzare i dati in più progetti o per molteplici scopi o se non è possibile identificare completamente la finalità del trattamento dei dati al momento della raccolta dei dati, potrebbe essere opportuno utilizzare un'applicazione di gestione del consenso. Vari fornitori di servizi ora offrono piattaforme di consenso informato eticamente solide e sicure che possono aiutarti a gestire, documentare e dimostrare le procedure per l'ottenimento del consenso.

VI. Raccolta di dati sui bambini

Tutte le ricerche che coinvolgono bambini e giovani sollevano questioni etiche significative, in quanto questi potrebbero essere meno consapevoli dei rischi e delle conseguenze della loro partecipazione. Ciò vale anche per quanto riguarda il trattamento dei loro dati personali.

Se il vostro progetto di ricerca prevede la raccolta di dati da parte di minori, dovete seguire ***la nota orientativa della Commissione Europea sul consenso informato***, in particolare le disposizioni sull'ottenimento del consenso di un genitore/rappresentante legale e, se del caso, del consenso del minore. Come la nota chiarisce, è imperativo che tutte le informazioni che si rivolgono a un bambino siano in un linguaggio adatto all'età e semplice, cosicché possano essere facilmente capite. È inoltre necessario applicare il principio di protezione dati fin dalla progettazione (privacy by design) per la ricerca di dati riguardanti i bambini e ridurre al minimo la raccolta e il trattamento dei loro dati per quanto possibile.

Il GDPR stabilisce speciali garanzie per i bambini in relazione ai "servizi della società dell'informazione", un ampio termine che include tutti i fornitori di servizi Internet, comprese le

[7] ad esempio, "Un dipartimento di ricerca universitario conduce un esperimento che analizza i cambiamenti di umore su 50 materie. Questi sono requirosso per registrare in un file elettronico i loro pensieri ogni ora, in un dato momento. Le 50 persone hanno dato il loro consenso per questo particolare progetto, e questo uso specifico dei dati da parte dell'università. Il dipartimento di ricerca scopre presto che elettronicamente registrazione di pensieri sarebbe molto utile per un altro progetto incentrato sulla salute mentale, sotto il coordinamento di un altro team. Anche se l'università, come controllore, avrebbe potuto utilizzare gli stessi dati per il lavoro di un altro team senza ulteriori passi perla legittimità del trattamento di tali dati, dato che gli scopi sono compatibili, l'università ha informato le materie e ha chiesto nuovo consenso, seguendo il suo codice etico della ricerca e il principio del trattamento equo" (*Manuale sulla protezione dei dati europei law: edizione 2018*, Fondamentale dell'UE Agenzia europea dei diritti dell'uomo, Consiglio d'Europa e supervisore europeo per la protezione dei dati (2018); http://fra.europa.eu/en/publication/2018/manuale-europeo-dati-protezione-legge).

piattaforme di social media.[8] Queste includono l'obbligo di consenso parentale ***verificato*** per quanto riguarda i servizi della società dell'informazione offerti direttamente ai bambini di età inferiore ai 16 anni. I singoli Stati membri possono prevedere l'abbassamento di tale soglia a 13 anni. Se state raccogliendo dati da minori che utilizzano le ICTs (ad es. da piattaforme o app di social media), dovete assicurarvi di osservare le garanzie del diritto nazionale e dell'UE e spiegare nella vostra proposta come otterrete e verificherete il consenso del genitore/rappresentante legale.

VII. Uso dei dati raccolti in precedenza ('uso secondario')

Come osservato in precedenza, alcune delle violazioni di più alto profilo delle norme etiche hanno riguardato l'uso di dati raccolti per uno scopo e poi utilizzati per altri processi di ricerca o targeting, senza la conoscenza o il consenso della persona interessata. Se si trattano dati personali nell'ambito della ricerca senza il consenso esplicito degli interessati, è necessario spiegare come si otterranno i dati, giustificare il loro utilizzo nel progetto e garantire che il trattamento è equo per l'interessato

Se la raccolta o l'utilizzo dei dati solleva questioni etiche specifiche (ad es. per quanto riguarda il consenso e la trasparenza, la vita privata e i diritti e le aspettative degli interessati), è necessario fornire una panoramica dettagliata delle operazioni di raccolta e trattamento dei dati pianificate e spiegare in che **modo le criticità etiche saranno attenuate.**

Se si utilizzano dati disponibili pubblicamente, è necessario fornire i dettagli della fonte o delle fonti e verificare che i dati siano accessibili apertamente e pubblicamente e possano essere utilizzati per scopi di ricerca. È inoltre necessario eseguire questa operazione qualora i dati che si intende utilizzare siano stati manifestamente resi pubblici dall'interessato (vedi Box 4).

[Box 4] Utilizzo dei dati 'open source'

Il fatto che alcuni dati siano disponibili pubblicamente non significa che non vi siano limiti al loro utilizzo.

Al contrario, **se si prendono dati personali "open source" relativi a persone identificabili e si creano nuovi record o file/profili, si trattano dati personali connessi ad esse ed è necessario avere una base** legale/legittima per farlo.

È necessario garantire che il trattamento dei dati sia equo nei confronti dell'interessato e che i suoi diritti fondamentali siano rispettati.

Se il vostro progetto di ricerca utilizza **dati provenienti da reti di social media** e non intendete chiedere il consenso esplicito degli interessati all'uso dei loro dati, è necessario valutare se tali persone effettivamente intendevano rendere pubbliche le loro informazioni (ad es. alla luce delle impostazioni sulla privacy o dell'audience limitata a cui i dati sono stati resi disponibili).

Non è sufficiente che i dati siano accessibili; devono essere stati resi pubblici nella misura in cui gli interessati non hanno alcuna **ragionevole aspettativa di privacy**. **È inoltre necessario assicurarsi che l'utilizzo previsto dei dati sia conforme a tutti i termini e le condizioni pubblicati dal Titolare del trattamento**.
Se avete dubbi su cosa potete o non potete fare con questo tipo di dati, dovreste chiedere consiglio al vostro responsabile della protezione dei dati o a un esperto adeguatamente qualificato e includere il loro parere nella vostra proposta.

[8] Si veda anche la direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015 che stabilisce una procedura per la fornitura di informazioni nel campo delle normative tecniche e delle norme sui servizi della società dell'informazione(OJ L 241, 17.9.2015, pa. 1).

Se si intende utilizzare i dati personali raccolti da un precedente progetto di ricerca, è necessario fornire dettagli relativi alla raccolta iniziale dei dati, alla metodologia e alla procedura di consenso informato. È inoltre necessario verificare di disporre dell'autorizzazione del proprietario/gestore dei set di dati per il loro utilizzo nel progetto.

Quando l'uso pianificato dei dati si basa sugli "interessi legittimi" del Titolare del trattamento, la natura e lo scopo del set di dati devono essere descritti in dettaglio, unitamente alle garanzie (ad esempio tecniche di anonimizzazione o pseudonimizzazione) che ne giustificano l'uso nel progetto.[9]

Se il trattamento dei dati previsto si basa sulla legislazione nazionale o su normative internazionali che autorizzano la ricerca, o su un interesse pubblico dimostrabile (ad esempio la salute pubblica, la protezione sociale) che consente di utilizzare un particolare set di dati, la proposta deve fare riferimento al diritto o alla politica dello Stato membro o dell'Unione.

In linea di principio, se si utilizzano dati personali forniti da terzi e gli interessati non hanno espressamente acconsentito al loro utilizzo in progetti di ricerca, è necessario, in conformità con il GDPR, informarli che avete acquisito i dati e per ciò che saranno utilizzati (art.14 GDPR). È inoltre necessario fornire loro le stesse informazioni di base sul trattamento dei dati e sui diritti degli interessati che siete obbligati a fornire alle persone di cui state raccogliendo i dati direttamente (vedi sezione V). Questi requisiti non si applicano solo quando questo non è possibile o comporterebbe uno sforzo sproporzionato per contattare gli interessati. Tuttavia in questi casi è necessario implementare adeguate misure di salvaguardia, comprese le misure tecniche e organizzative per garantire il rispetto del principio della minimizzazione dei dati (cfr. Box 3) e proteggere i diritti fondamentali dei soggetti. Fondamentalmente, il GDPR richiede che la pseudonimizzazione o le tecniche di anonimizzazione (vedi sopra) siano applicate ovunque possibile (articolo 89 GDPR).

VIII. Valutazione d'impatto sulla protezione dei dati

L'approccio basato sul rischio per il trattamento dei dati su cui si basa il GDPR può aiutare i ricercatori a identificare i requisiti necessari per il trattamento di dati complessi, sensibili o su larga scala e affrontare le questioni etiche che derivano dai loro metodi e obiettivi di ricerca.

La valutazione d'impatto (DPIA) è un processo progettato per valutare l'impatto sulla protezione dei dati di un progetto, politica, programma, prodotto o servizio e, in consultazione con le parti interessate, per garantire che vengano intraprese azioni correttive per correggere, evitare o ridurre al minimo i potenziali impatti negativi sugli interessati.

Ai sensi del GDPR, una DPIA è obbligatoria per le operazioni di trattamento che potrebbero "comportare un rischio elevato per i diritti e le libertà delle persone fisiche" (art.35). Queste includono in particolare:

- un'analisi "sistematica e globale" dei dati personali nel contesto di un trattamento automatizzato, compresa la profilazione, qualora ciò abbia un effetto significativo sull'interessato;

[9] Secondo il GDPR, "gli interessi legittimi di un titolare del trattamento, compresi quelli di un titolare del trattamento al quale i dati personali possono essere comunicati, o di un terzo, possono fornire una base giuridica per il trattamento, purché non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenendo conto delle ragionevoli aspettative degli interessati in base al loro rapporto con il titolare del trattamento". Si veda anche il considerando 47 e l'articolo 89 del GDPR.

- il trattamento su larga scala di "categorie particolari" di dati personali o di dati personali relativi a condanne e reati penali; o
- la sorveglianza sistematica su larga scala di un'area accessibile al pubblico.

Il Gruppo di lavoro Articolo 29 dell'UE (WP29) ha elaborato un lungo elenco di scenari in cui è probabile che sia necessario condurre un DPIA (si veda il Box 5). Il Comitato europeo per la protezione dei dati e le autorità nazionali di controllo per la protezione dei dati dovrebbero chiarire ulteriormente le operazioni di trattamento per le quali le valutazioni d'impatto sono obbligatorie. È vostra responsabilità verificare se siete tenuti a condurre una DPIA in conformità alle norme UE o degli Stati membri.

Se gli obiettivi e i metodi di ricerca richiedono la conduzione di una DPIA in conformità con il GDPR, allora la previsione di questa valutazione deve essere fatta nella vostra proposta. Ciò include i dettagli su come, quando e da chi verrà effettuata tale operazione.

Fondamentalmente, se la DPIA indica che il trattamento previsto comporta un elevato rischio per i diritti e le libertà delle persone in assenza di misure adottate dal Titolare del trattamento per mitigare il rischio, è necessario chiedere il parere dell'autorità di vigilanza sulla protezione dei dati per sapere se il trattamento è ammissibile (art.36 GDPR). Ciò può a sua volta avere un impatto significativo sulla fattibilità della vostra proposta di ricerca e deve pertanto essere affrontato nella vostra valutazione dei rischi.

Se non siete sicuri di essere tenuti a condurre una DPIA, dovreste chiedere il parere del vostro responsabile della protezione dei dati o di un esperto adeguatamente qualificato e includere il loro parere nella proposta. Anche se non è richiesto di condurre una DPIA in conformità con il GDPR, è buona prassi condurre tale valutazione al fine di accertare e ridurre al minimo i rischi ovunque il trattamento dei dati previsto sia complesso, su larga scala o sensibile.

Indipendentemente dal fatto che una DPIA sia richiesta o condotta, se il trattamento dei dati previsto solleva preoccupazioni relative all'etica, è necessario fornire una valutazione approfondita di tali rischi nella proposta. Come minimo, questo dovrebbe includere il rischio di condotte non etiche o danni al benessere o agli interessi dei partecipanti alla ricerca sia a livello individuale (ad esempio, partecipanti alla ricerca, loro associati o altri terzi)) che a livello di gruppo (ad esempio, il potenziale di impatti negativi sulla comunità cui si riferiscono i dati).

Nel valutare le questioni etiche derivanti dalla ricerca, è necessario considerare il rischio di discriminazione, stigmatizzazione, violazioni dei dati (ad es. esporre l'identità o dati sensibili delle persone o danneggiare la loro reputazione attraverso una violazione della riservatezza) le minacce alla sicurezza dei partecipanti e il potenziale uso improprio della metodologia o dei risultati della ricerca.

[Box 5] Scenari in cui è necessario condurre una valutazione dell'impatto sulla protezione dei dati

Il Gruppo Art. 29 ritiene che **le operazioni di trattamento che sollevano molteplici problemi in materia di protezione dei dati siano più suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone interessate e richiedano pertanto una DPIA**, indipendentemente dalle misure che il titolare del trattamento intende adottare.

Le linee guida del Gruppo Art. 29[10] forniscono i seguenti esempi:

Esempi di trattamento	Possibili criteri pertinenti	Una DPIA è probabilmente richiesta?
Un ospedale che tratta i dati genetici e sanitari dei suoi pazienti (sistema di informazione ospedaliera).	– Dati sensibili o dati di natura altamente personale – Dati relativi a soggetti di dati vulnerabili – Dati elaborati su larga scala	Sì
L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il Titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe.	– Monitoraggio sistematico. – utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative	Sì
Un'impresa che monitora sistematicamente le attività dei propri dipendenti, compreso il monitoraggio della stazione di lavoro dei dipendenti, l'attività su Internet, *ecc.*	– Monitoraggio sistematico – Dati relativi a soggetti di dati vulnerabili	Sì
La raccolta di dati sui social media pubblici per la generazione di profili.	– Trattamenti valutativi o di scoring – Dati elaborati su larga scala – Corrispondenza o combinazione di set di dati – Dati sensibili o dati di natura altamente personale	Sì
Un istituto che crea un credito a livello nazionale o una banca dati sulle frodi.	– Trattamenti valutativi o di scoring – Processo decisionale automatizzato con effetto significativo legale o simile – Impedisce al soggetto di dati di esercitare un diritto o di utilizzare un servizio o un contratto – Dati sensibili o dati di natura altamente personale	Sì
Memorizzazione a scopo di archiviazione di dati sensibili personali pseudonimizzati riguardanti soggetti vulnerabili di progetti di ricerca o sperimentazioni cliniche	– Dati sensibili – Dati relativi a soggetti di dati vulnerabili. – Impedisce ai soggetti di dati di esercitare un diritto o di utilizzare un servizio o un contratto	Sì

[10] Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, Article 29 Working Party

IX. Profilazione, monitoraggio, sorveglianza, processo decisionale automatizzato e big data

L'uso diffuso e il vasto potenziale di ricerca e sviluppo delle tecnologie dell'informazione e della comunicazione hanno creato una nuova serie di sfide etiche. Queste includono conseguenze potenzialmente negative o impreviste per i singoli interessati, comunità specifiche e la società in generale. Queste possono riguardare le implicazioni della combinazione e dell'analisi di diversi set di dati, il potenziale uso improprio delle applicazioni o il rischio di discriminazione istituzionalizzata.

Se il vostro progetto di ricerca coinvolge queste tecniche, è necessario fornire un'analisi dettagliata delle questioni etiche sollevate dalla vostra metodologia. Ciò dovrebbe comprendere:

- una panoramica di tutte le operazioni pianificate di raccolta ed elaborazione dei dati;
- l'identificazione e l'analisi delle questioni etiche sollevate; e
- una spiegazione di come queste questioni saranno affrontate per mitigarle nella pratica.

Se nella vostra ricerca sono coinvolti partecipanti umani, è necessario assicurarsi che siano in atto solide procedure di consenso informato. **La vostra ricerca coinvolge partecipanti umani se li reclutate direttamente, o se le vostre attività di ricerca consistono nel coinvolgere attivamente, influenzare, manipolare o dirigere le persone in qualsiasi modo.**

Se il vostro progetto prevede l'elaborazione su larga scala di dati personali utilizzando tecniche quali il data-mining, il web crawling o l'analisi di social network, dovreste affrontare sia le implicazioni etiche dei metodi di ricerca che la compatibilità del trattamento dei dati con il GDPR

Se il vostro progetto prevede l'elaborazione automatizzata o la profilazione dei dati personali (si veda Box 6), la proposta dovrebbe affrontare le implicazioni etiche degli obiettivi, dei metodi e dei risultati attesi. Si dovrebbe anche considerare l'impatto legale, sociale ed etico di qualsiasi analisi dei big data, [11] in particolare il suo potenziale impatto sulla parità di trattamento e di non discriminazione. [12]

Se il progetto comporta lo sviluppo o l'utilizzo di tecnologie che possono essere utilizzate per la sorveglianza o la tracciabilità delle persone, può rientrare nell'ambito di applicazione del Regolamento CE sul duplice uso (428/2009) o essere vulnerabile ad abusi. In tali casi, è necessario consultare la nota orientativa della Commissione Europea - **Ricerca su prodotti a duplice uso** e/o la nota orientativa della Commissione Europea - **Potenziale uso improprio della ricerca**

Se il vostro progetto comporta un monitoraggio intensivo o il tracciamento dei partecipanti alla ricerca, ad esempio per quanto riguarda i loro movimenti, comportamenti, attività o emozioni, la vostra proposta deve spiegare quali misure saranno adottate per proteggere sia i loro dati personali che i diritti fondamentali.

Se l'obiettivo del progetto è sviluppare tecnologie o tecniche di sorveglianza ai fini dell'applicazione della legge, la proposta dovrebbe spiegare perché la sorveglianza può essere ritenuta necessaria e proporzionata in una società democratica, conformemente ai valori, ai principi e alle leggi dell'UE.

[11] Vedi anche *Linee guida sulla protezione delle persone per quanto riguarda il trattamento dei dati personali in un mondo di Big Data (Linee guida per i Big Data)*, Consiglio d'Europa (gennaio 2017).
[12] Articolo 21, Carta dei diritti fondamentali dell'UE

Come osservato in precedenza, questo tipo di ricerca può richiedere una DPIA in conformità con il GDPR o agli orientamenti supplementari emessi dalle autorità di vigilanza. Se le attività di ricerca pianificate comportano questioni etiche molteplici o particolarmente complesse che non possono essere risolte nella fase di proposta o successivamente tramite una DPIA, la proposta dovrebbe prevedere una valutazione dell'impatto etico più ampia, che dovrà essere a sua volta soggetta a revisione da parte del comitato etico della ricerca o di un altro organismo appropriato.

[Box 6] Trattamenti automatizzati e profilazione a

Il GDPR comprende garanzie specifiche relative al trattamento automatizzato o alla "profilazione" dei dati personali che hanno, o potrebbero avere, un significativo impatto giuridico o materiale sull'interessato (articolo 22 GDPR). **La profilazione e il suo impatto sono espressamente legati alla valutazione e al rendimento: più la profilazione è invasiva e tanto maggiore è l'effetto potenziale del risultato, tanto più è probabile che sollevi importanti questioni etiche e** di diritti fondamentali. Le salvaguardie del GDPR sono concepite per consentire agli interessati di:

- comprendere che sono soggetti a profilazione;
- conoscere la logica alla base del trattamento ed eventuali conseguenze previste da tale trattamento;
- opporsi o rinunciare al trattamento; e
- contestare o chiedere l'intervento umano in relazione alla decisione automatizzata raggiunta.

Come progetti di ricerca o sviluppo (piuttosto che applicazioni reali), le vostre attività potrebbero non avere un impatto significativo, giuridico o materiale, sulla persona interessata. Tuttavia, in conformità con i principi di protezione dei dati fin dalla progettazione (privacy by design) e della ricerca e innovazione responsabili è necessario prendere in considerazione il trattamento automatizzato e le garanzie sulla profilazione richieste dal GDPR nella fase di sviluppo del progetto. Se intendete o prevedete di utilizzare la vostra metodologia in modo più ampio (ad es. in un prodotto, in un'applicazione o in un contesto di ricerca), dovete sviluppare le garanzie necessarie.
Le garanzie sulla profilazione comprendono l'uso di metodi matematici e statistici comprovati e affidabili, metodi per garantire che i dati siano il più accurati possibile e lo sviluppo di modelli e tecniche per ridurre al minimo il rischio di errore o di effetti discriminatori. **La trasparenza e la responsabilità nei confronti dei partecipanti** alla ricerca sono particolarmente importanti e il GDPR richiede **anche di fornire interessati informazioni sul trattamento automatizzato, la profilazione e la valutazione e la possibilità di ricorso per le persone interessate per ottenere una spiegazione e contestare la decisione raggiunta**.

X. Sicurezza dei dati

Ogni qualvolta e in qualsiasi modo raccogliate dati personali, avete obblighi sia etici che legali per garantire che le informazioni dei partecipanti siano adeguatamente protette. Ciò è fondamentale per salvaguardare i loro diritti e le loro libertà e ridurre al minimo i rischi etici connessi al trattamento dei dati.

Il GDPR impone a tutti i titolari del trattamento e ai responsabili del trattamento di attuare misure tecniche e organizzative idonee a garantire un livello di sicurezza dei dati commisurato ai rischi cui sono esposti gli interessati in caso di accesso non autorizzato, o divulgazione, cancellazione accidentale o distruzione dei propri dati (art.32 GDPR).

La vostra proposta dovrebbe fornire dettagli sulle misure tecniche e organizzative che saranno attuate per proteggere i dati personali trattati nel corso della vostra ricerca, ad es. con riferimento alle politiche di protezione dei dati e di sicurezza delle informazioni dell'istituto ospitante e dei partner di ricerca. Tali misure possono includere la pseudonimizzazione e la cifratura dei dati

personali, nonché politiche e procedure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi di trattamento.

Qualora sia previsto un trattamento a più alto rischio (ad es. per categorie particolari di dati o trattamenti su larga scala), è necessario spiegare chiaramente come si garantirà un maggiore livello di sicurezza dei dati. In questi scenari è importante scegliere metodi di ricerca e strumenti di elaborazione dati appropriati (vedi Box 7).

Questo è fondamentale quando la vostra ricerca coinvolge soggetti di ricerca che sono vulnerabili o possono essere resi vulnerabili a causa della loro partecipazione al vostro progetto. Questo può essere il caso, ad esempio se si raccolgono dati su questioni politiche sensibili o si comunica con persone in paesi con governi repressivi. Quasi tutte le comunicazioni sono vulnerabili alla sorveglianza e all'intercettazione, ma alcuni canali sono più sensibili di altri. Laddove si ritenga che vi sia un rischio elevato per i ricercatori e i partecipanti alla ricerca, è necessario assicurarsi che le comunicazioni siano al sicuro da accessi non autorizzati.

[Box 7] Sicurezza dei dati: 10 cosa fare e cosa non fare

Fare

- ✓ utilizzare strumenti conformi al GDPR per raccogliere, elaborare e archiviare i dati personali dei soggetti di ricerca;
- ✓ prendere sul serio la sicurezza delle comunicazioni, elaborare e implementare protocolli dedicati per il vostro progetto, se necessario;
- ✓ verificare i termini e le condizioni di tutti i fornitori di servizi che utilizzate (software, applicazioni, archiviazione, ecc.) per elaborare i dati personali all'interno del tuo progetto, al fine di identificare e mitigare i rischi per le persone interessate;
- ✓ crittografare i dati di ricerca e/o i dispositivi su cui sono memorizzati e garantire che le chiavi/password siano adeguatamente protette; e
- ✓ e consultare il proprio responsabile della protezione dei dati o un esperto adeguatamente qualificato per ottenere consulenza su come raggiungere un livello di sicurezza dei dati commisurato ai rischi per gli interessati;
- ✓

Non fare

- ✗ raccogliere dati su un dispositivo personale come uno smartphone senza garantirne una protezione adeguata (ad es. considerare le implicazioni dei backup automatici sul cloud e le caratteristiche di sicurezza del dispositivo);
- ✗ utilizzare servizi gratuiti che possono utilizzare i dati dei partecipanti per i propri scopi al posto del pagamento, o raccogliere dati o comunicare con i partecipanti alla ricerca tramite piattaforme di social media senza prima valutare le implicazioni sulla protezione dei dati;
- ✗ utilizzare e-mail non cifrate, SMS o piattaforme 'voice over IP' non sicure per comunicare con i partecipanti vulnerabili o coloro che possono essere soggetti a sorveglianza statale;;
- ✗ esporre i dati personali all'accesso o all'uso non autorizzato quando vi si accede da remoto (ad esempio utilizzando connessioni wifi non sicure) o viaggiando in paesi in cui i dispositivi possono essere ispezionati o sequestrati;
- ✗ presupporre che i vostri partner di ricerca, collaboratori o fornitori di servizi dispongano di adeguate politiche in materia di sicurezza delle informazioni e protezione dei dati senza verificare che ciò avvenga.

XI. Trasferimento di dati personali a paesi terzi

L'invio dei dati personali dei partecipanti a partner, collaboratori o fornitori di servizi al di fuori dell'UE solleva questioni etiche e giuridiche che possono essere difficili da affrontare nella pratica. I ricercatori con sede al di fuori dell'UE possono essere soggetti a diverse norme etiche e il loro trattamento dei dati potrebbe non essere conforme agli standard dell'UE.

Pochi paesi extra UE hanno ricevuto dalla Commissione europea una decisione di adeguatezza che indica che essi dispongono di un quadro di protezione dei dati che offre un livello di protezione equivalente a quello previsto dal diritto UE. [13] Ciò significa che i dati dei soggetti di ricerca possono non essere adeguatamente protetti o essere utilizzati in modo tale da compromettere i loro diritti fondamentali. L'UE ha bisogno che i suoi standard etici si applichino a tutte le ricerche che finanzia, a prescindere dal paese in cui si svolgono. Il trasferimento di dati personali da paesi non appartenenti all'UE è soggetto a severi requisiti di protezione dei dati ai sensi del capitolo V del GDPR.

Non è necessario "inviare" i dati a un paese non membro dell'UE per l'applicazione di queste disposizioni; se uno dei vostri partner o fornitori di servizi si trova al di fuori dell'UE ed è in grado di accedere ai dati personali da voi raccolti, ciò equivale a un trasferimento di dati nel contesto del GDPR. È necessario fornire nella proposta i dettagli di tutti i trasferimenti di dati previsti verso paesi terzi. È inoltre necessario garantire che i destinatari dei dati garantiscano lo stesso livello di protezione dei dati richiesto dal diritto dell'UE.

Affinché i trasferimenti di dati verso paesi terzi possano essere legittimi, essi devono essere basati su uno delle seguenti condizioni:

- il consenso esplicito dell'interessato (che ne impone che sia informato prima di tali trasferimenti);
- una "decisione di adeguatezza" da parte della Commissione europea nei confronti del paese in questione;
- un accordo di trasferimento dei dati contenente clausole contrattuali standard approvate dalla Commissione Europea che diano effetto alla normativa UE sulla protezione dei dati; o
- norme aziendali vincolanti obbligatorie sia per il mittente che per il destinatario e approvate da un'autorità nazionale di vigilanza.

Questi requisiti si applicano a tutti i trasferimenti di dati personali, indipendentemente dalla sensibilità dei dati.

Dal punto di vista dell'etica della ricerca, il trasferimento dei dati dei partecipanti alla ricerca verso paesi terzi dovrebbe in linea di principio basarsi sempre sul loro consenso informato, che deve essere richiesto e ottenuto conformemente agli orientamenti di cui sopra.

Se la vostra proposta di ricerca prevede il trasferimento dei dati dei partecipanti a paesi non UE senza l'esplicito consenso degli interessati, la vostra proposta deve chiarire la base giuridica per tale trasferimento. In tali casi, è necessario consultare il responsabile della protezione dei dati dell'istituzione ospitante in merito alla legalità del trasferimento dei dati e includere il suo parere

[13] L'elenco dei paesi coperti da una decisione di adeguatezza della Commissione è disponibile al seguente link: https://ec.europa.eu/info/law/law-argomento/dati-protezione/dati-Trasferimenti-Fuori-eu/adeguatezzaProtezione-Personale-Dati-non-avuto-countries_en

nella proposta. Se l'istituto ospitante non dispone di un responsabile della protezione dei dati, è necessario rivolgersi a un esperto adeguatamente qualificato.

XII. Raccolta di dati personali al di fuori dell'Unione europea

La raccolta di dati personali da soggetti di ricerca in paesi terzi solleva questioni etiche simili, ma queste possono essere amplificate dalla necessità di garantire che i partecipanti siano:

- del tutto a proprio agio nell'essere parte di un progetto di ricerca condotto da ricercatori esterni al proprio paese;
- consapevoli di ciò che accadrà ai loro dati; e
- non soggetti ad alcuna pressione indebita a partecipare.

Come osservato in precedenza, i requisiti etici dell'UE si applicano a tutta la ricerca finanziata dall'UE, a prescindere dal luogo in cui si svolge. Analogamente, il GDPR si applica a tutte le operazioni di trattamento dei dati effettuate da titolari del trattamento con sede nell'UE, indipendentemente dal luogo in cui avviene il trattamento. Ciò significa che, anche se si raccolgono dati personali al di fuori dell'UE, si deve comunque garantire ed essere in grado di dimostrare il rispetto del diritto dell'UE.

È necessario rispettare anche le leggi del paese in si sta conducendo la ricerca, comprese le leggi nazionali sulla protezione dei dati. Ad esempio, potrebbe vigere l'obbligo di notificare o chiedere l'autorizzazione per la ricerca alle autorità nazionali o alle autorità di regolamentazione della protezione dei dati. Possono essere richieste ulteriori autorizzazioni per trasferire dati personali al di fuori del paese in cui si svolge la ricerca. Le disposizioni sulla "sovranità dei dati" possono anche vietare il trasferimento di determinati tipi di informazioni, quali dati sanitari o sui pazienti, al di fuori del paese

È vostra responsabilità determinare quali obblighi legali si applicano alla ricerca condotta al di fuori dell'UE e intraprendere qualsiasi azione necessaria per conformarvisi. Dovete anche essere in grado di dimostrare la conformità alla normativa, su richiesta. Anche in questo caso, se non siete sicuri di come gestire le questioni relative ai trasferimenti di dati internazionali, dovreste consultare il responsabile della protezione dei dati dell'istituto ospitante o un esperto adeguatamente qualificato e includere il loro parere nella tua proposta.

[Box 8] Lista di controllo: trasferimenti di dati internazionali

Trasferimento di dati personali al di fuori dell'UE

- ✓ garantire che qualsiasi trasferimento internazionale di dati soddisfi almeno una delle condizioni pertinenti del capitolo V GDPR;
- ✓ verificare che i servizi di terze parti che si intende utilizzare (ad es. strumenti di sondaggio, analisi dei dati, archiviazione su cloud, ecc.) siano inseriti nel contesto di uno Stato membro dell'UE o legalmente rappresentati nell'UE in conformità al GDPR;
- ✓ adottare accordi giuridicamente vincolanti ed esecutivi con i partner prima dei trasferimenti di dati;
- ✓ vietare il successivo trasferimento di dati personali da parte dei membri del consorzio e di qualsiasi altro destinatario dei dati al di fuori del quadro di tali accordi; E
- ✓ attuare adeguate misure organizzative e tecniche per garantire che i dati personali siano trasferiti in modo sicuro.

Raccolta di dati personali in paesi Extra-UE

- ✓ garantire che le disposizioni in materia di trattamento, notifica, consenso e responsabilità siano conformi agli standard GDPR;
- ✓ identificare eventuali ulteriori requisiti in materia di protezione dei dati nelle leggi applicabili nel paese in cui i dati devono essere raccolti e spiegare nella proposta come si intende rispettarli;
- ✓ se del caso, garantire che i partecipanti alla ricerca comprendano e acconsentano all'esportazione dei dati personali che forniscono a uno Stato membro dell'UE o a un paese non UE;
- ✓ utilizzare tecniche di pseudonimizzazione o anonimizzazione per ridurre al minimo il rischio per le persone interessate;
- ✓ attuare adeguate misure organizzative e tecniche per garantire che i dati personali siano trasferiti in modo sicuro.

XIII. Cancellazione e archiviazione dei dati

È possibile conservare i dati personali raccolti solo per il tempo necessario per gli scopi per i quali sono stati raccolti o in conformità con le disposizioni di controllo, archiviazione o conservazione stabilite per il progetto. Questi devono essere spiegati ai partecipanti alla ricerca in conformità con le procedure di consenso informato.

I recenti casi di alto profilo relativi all'uso improprio dei dati personali derivano dalla mancata cancellazione dei dati personali da parte dei Titolari del trattamento e che avevano garantito che le terze parti a cui sono stati forniti i dati avevano fatto lo stesso in conformità con le condizioni concordate per il loro utilizzo.

Non appena i dati di ricerca non sono più necessari, o soggetti a un periodo di conservazione stabilito, è necessario eliminare in modo sicuro i dati nella loro interezza e assicurarsi che non possano essere recuperati. I dati conservati per i processi di audit dovrebbero essere conservati in modo sicuro e successivamente trattati solo per tali finalità.

Se i dati di ricerca sono conservati nel cloud o da un fornitore di servizi di terze parti, è necessario assicurarsi che i dati siano stati cancellati in modo sicuro insieme a eventuali backup. Se i dati sono stati condivisi con partner o trasferiti a terzi nel corso del progetto, è necessario assicurarsi che essi abbiano cancellato i dati, a meno che non abbiano una base legittima per conservarli.

XIV. Responsabili della protezione dei dati e altre fonti di aiuto

Se la vostra istituzione ha nominato un responsabile della protezione dei dati, si raccomanda di chiedere il suo parere in merito ai vostri obblighi in materia di protezione dei dati e a come adempierli. È necessario assicurarsi che i dati di contatto del responsabile della protezione dei dati siano messi a disposizione di tutti gli interessati coinvolti nella ricerca.

Se il vostro progetto solleva problemi complessi di protezione dei dati a causa della sensibilità dei dati, o la portata o la natura del trattamento in questione, si dovrebbe prendere in considerazione la nomina di uno specialista/consulente per la protezione dei dati per il vostro progetto o nel comitato etico di ricerca. Se l'istituto ospitante non dispone di un responsabile della protezione dei dati, è necessario consultare un esperto adeguatamente qualificato nella preparazione della proposta e/o, se necessario, nominare tale esperto per il progetto.

Se avete bisogno di aiuto e consulenza per affrontare le questioni etiche più ampie sollevate dal trattamento dei dati nel vostro progetto, è necessario contattare gli organi o i servizi istituzionali

pertinenti (ad es. ufficio di ricerca o comitato etico di ricerca) nella vostra università o istituzione, gli organismi nazionali competenti, i membri del consorzio o i colleghi della rete personale che possono avere competenze ed esperienza pertinenti.

Se non siete sicuri di eventuali aspetti etici nella ricerca, dovreste prendere in considerazione la nomina di un consulente etico o coinvolgere un mentore etico per fornire una consulenza, supervisionare le questioni etiche nella ricerca e assicurarvi che sia conforme eticamente.