FIghting Cybercrime with OSINT (FICO)

Linee guida per il trattamento dei dati personali nell'ambito della ricerca FICO

Legenda: **in blu sono evidenziate informa sintetica** le indicazioni sulle modalità di trattamento dei dati personali

Sommario

Il presente documento mira a fornire indicazioni sugli obblighi relativi alla protezione dei dati personali con specifico riferimento al trattamento dei dati raccolti ed utilizzati nell'ambito del progetto di ricerca scientifica FIghting Cybercrime with OSINT (FICO).
Esso, pertanto, si riferisce esclusivamente all'attività di ricerca FICO e alla relativa fase di raccolta dei dati da parte dei ricercatori del progetto, dei responsabili e delle persone autorizzate al trattamento dei dati personali. **In grassetto azzurro sono evidenziate le indicazioni sintetiche da seguire.**

Si è ritenuto utile, per una più agevole fruizione del documento, includere una breve appendice definitoria relativa alle principali qualificazioni giuridiche impiegate, corredata anche dai riferimenti normativi consultati.

Il WP4 rinnova la propria disponibilità ad attività di *counselling* concernenti il trattamento dei dati personali all'interno del progetto.

Le linee guida sono state redatte dal prof. Ponti (benedetto.ponti@unipg.it) insieme alla dott.ssa Trozzi (simonetta.trozzi@unipg.it) e sottoposte a valutazione con la prof. Stefanelli (stefania.stefanelli@unipg.it)

Presupposti di liceità del trattamento

1. Caratteristiche del progetto di ricerca FICO

FICO aspira a sviluppare metodi per contrastare specifici cybercrime (cyberterrorismo, corruzione e reati della sfera personale quali la pedopornografia) progettando un sistema software di Open Source Intelligence (OSINT) corredato anche di sonde/sensori in ambiente edge (SIEM).

Il trattamento riguarda dati raccolti in rete, in via prevalentemente automatizzata, con sistemi di OSINT. Anche le attività di Human Intelligence (HUMINT) si svolgeranno in via prevalentemente automatizzata. Pertanto, fonti di studio, catturate dal sistema OSINT, saranno sia i dati raccolti da siti e ambienti web aperti alla consultazione pubblica (ivi compresi i *social network*), sia i dati tratti da specifici *data lake* già disponibili.

2. Obblighi dei ricercatori concernenti il trattamento dei dati personali durante lo svolgimento dell'attività di ricerca

2.1 Base giuridica di liceità del trattamento dei dati

Il Regolamento EU 2016/676 (Regolamento europeo sulla protezione dei dati delle persone fisiche e sulla libera circolazione dei dati, d'ora in poi GDPR) prevede una serie di condizioni denominate "basi giuridiche" al cui ricorrere è possibile ritenere integrato il presupposto di liceità del trattamento di dati personali. Costituisce attività di trattamento anche la raccolta dei dati (V. appendice definitoria, voce trattamento). Si noti, il presupposto di liceità è condizione necessaria per poter procedere al trattamento dei dati personali, ma non è anche sufficiente (nel senso che, accertata l'esistenza di una base giuridica/presupposto per il trattamento, poi occorre anche rispettare i principi e altre regole del GDPR, in relazione alla tipologia di trattamento effettuata).
Nel caso specifico del trattamento di dati personali nell'ambito della ricerca FICO la base giuridica di legittimità va ravvisata nell'esecuzione di un compito di interesse pubblico quale è l'esercizio dell'attività di ricerca scientifica da parte di un soggetto pubblico [l'università, nel caso di specie L'Università degli studi di Perugia] il cui compito istituzionale, affidatole dalla legge [legge 240/2010], è lo svolgimento (anche) dell'attività di ricerca. In particolare, la base giuridica che legittima il trattamento dei dati personali nell'ambito della ricerca FICO è da identificarsi nella fattispecie per cui "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" (art. 6, par. 1, lett. e GDPR); il compito di interesse pubblico (ai sensi dell'art. 2-*ter* d.lgs. 196/2003, d'ora in poi Codice privacy) è definito e specificato con atto amministrativo generale dell'Ateneo, identificato nel "Piano di Ateneo di azioni collaborative e trasversali in materia di Ricerca e Terza Missione"

(adottato nel luglio del 2021), poi attuato con l'"Avviso per il finanziamento di Progetti di Ricerca di Ateneo - Anno 2021" e la connessa, conseguente selezione del progetto FICO.
Pertanto, il trattamento dei dati personali nell'ambito delle attività di ricerca del progetto FICO è lecito se ed in quanto necessario per lo svolgimento dell'attività di ricerca, così come individuata nel progetto. L'attività di raccolta di dati personali e ogni ulteriore trattamento degli stessi, dunque, non necessitano, per essere legittimi, del consenso dell'interessato, ossia la persona fisica alla quale si riferisce il dato raccolto.

2.2 Principi e modalità di trattamento: quali dati bisogna trattare e come bisogna trattarli?

Il GDPR (Considerando 159) prevede che anche per il trattamento a fini di ricerca scientifica è necessario rispettare i generali principi, tra i quali quelli previsti all'art. 5 GDPR, seppure con alcune deroghe specifiche previste per l'attività di ricerca scientifica (art. 89).
A tal proposito, e coerentemente con il principio di finalità del trattamento dei dati personali, è previsto un generale divieto in base al quale i dati personali trattati a fini di ricerca non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti finalizzati a scopi diversi e ulteriori rispetto a quello della ricerca scientifica (art. 105 Codice privacy). Pertanto, **i dati raccolti ed utilizzati per le finalità di ricerca del progetto FICO possono essere trattati solo ed esclusivamente per le attività di ricerca del progetto.**

Quali dati personali è possibile trattare?

Ai fini della ricerca FICO è possibile trattare tutti i dati personali, siano essi dati comuni, particolari o giudiziari. A tal proposito, occorre sottolineare che l'art. 5 par. 1, lett. b del GDPR prevede una deroga al generale principio della limitazione della finalità del trattamento dei dati personali. In base a questo principio i dati possono essere trattati per finalità ulteriori rispetto alle finalità che ne hanno giustificato l'iniziale trattamento, solo se tale ulteriore finalità risulta compatibile con quella iniziale. Nel caso della ricerca FICO, si utilizzano dati personali tratti essenzialmente da due tipologie di fonti. Con riferimento alle fonti OSINT, la finalità iniziale del trattamento è quella connessa alla disponibilità dei dati sulle fonti aperte. Con riferimento ai *data lake*, la finalità iniziale è quella che ha sorretto/giustificato la raccolta dei dati.
Tuttavia, questa verifica di compatibilità nel nostro caso non è necessaria. **Infatti, nel caso del trattamento dei dati personali a fini di ricerca scientifica è proprio il GDPR a stabilire che la compatibilità di tale finalità con la finalità iniziale di raccolta si presume, e dunque non va provata**.
Pertanto, **il ricercatore che intenda trattare dati personali a fini di ricerca scientifica, non deve**

verificare e dimostrare che tale finalità è compatibile con quella iniziale (tale compatibilità è presunta dalla legge).

Inoltre, **nel caso di trattamento per scopi di ricerca scientifica, è prevista una deroga al generale divieto di trattare categorie particolari di dati personali** (art. 9, par. 2 lett. g) e j) GDPR e art. 2-*sexies* Codice privacy).
Infatti, il divieto di trattamento delle categorie di dati particolari di cui all'art. 9 non si applica se:

- il trattamento è necessario per motivi di **interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2 lett. g) GDPR)
- il trattamento è 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.

Ai sensi della disciplina nazionale di attuazione, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri **per fini di ricerca scientifica** (art. 2-sexies Codice privacy)

Per quanto concerne **i dati particolari e giudiziari relativi a condanne penali e reati o a connesse misure di sicurezza (art. 10 GDPR) il trattamento a fini di ricerca scientifica deve di regola avvenire in forma anonima**. È opportuno attenersi a tali indicazioni salvo che l'anonimato renda impossibile l'attività di ricerca (art. 7 delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica).

Come bisogna trattare i dati personali?

A) Misure di sicurezza

Gli adempimenti relativi alle modalità di trattamento derivano dal rispetto del principio di minimizzazione dei dati, mediante il quale si persegue la finalità di ridurre il più possibile i rischi per i diritti e le libertà dell'interessato che possono derivare dal trattamento. In base a tale principio ogni ricercatore dovrà trattare solo i dati personali di cui ha realmente bisogno perché indispensabili in concreto al perseguimento degli scopi della ricerca.
Al fine di garantire il rispetto di tale principio, ogni ricercatore dovrà pertanto adottare concretamente **garanzie tecniche e organizzative, denominate misure di sicurezza** (art. 89 e art. 32 GDPR) e di seguito elencate.

Si richiede che egli adotti tali misure qualsiasi sia il dato raccolto nell'ambito dell'attività di ricerca (dati comuni, particolari e giudiziari), e ciò sia per i dati personali raccolti tramite da fonti aperte (OSINT) che per i dati già presenti in *data lake*.

All'articolo 32 GDPR sono indicate a titolo esemplificativo già alcune misure, riportate anche nel sito web d'Ateneo nella sezione dedicata *La ricerca scientifica e a la data protection*. Analogamente, la Circolare AgID n. 2 del 18/04/2017 sulle misure minime di sicurezza ICT per le pubbliche amministrazioni, suggerisce alcune prescrizioni da adottare nel trattamento dei dati personali in base al livello di rischio individuato per ogni singolo trattamento.

A.1) Tecniche di pseudonimizzazione e anonimizzazione

Tra le misure di sicurezza previste vanno adottate, in primo luogo, quelle finalizzate a non rendere direttamente riconducibili i dati raccolti agli interessati, permettendo di identificare questi ultimi solo in caso di necessità.

A tal proposito bisogna **distinguere** tra **dato pseudonomizzato** e **dato anonimo**. Infatti, mentre i dati personali pseudononimizzati sono da considerarsi ancora dati personali, e quindi soggetti al GDPR, i dati anonimi (cioè, i dati che risultano da un processo di anonimizzazione applicato a dati personali) non sono considerati dati personali, e quindi non sono soggetti alle regole del GDPR (Considerando 26).

- La pseudonimizzazione è una elaborazione consistente nella sostituzione di un attributo di identificazione univoco legato ad una collezione di dati con uno pseudonimo, tale che il collegamento con l'interessato non sia più immediatamente possibile senza l'uso di informazioni aggiuntive, tenute separate e messe in sicurezza con misure tecniche ed organizzative adeguate.
- L'anonimizzazione è invece il risultato di tecniche che vengono applicate ai dati personali al fine di rendere la re-identificazione ragionevolmente impossibile. La re-identificazione si verifica nel caso in cui, partendo da dati erroneamente ritenuti anonimi, si riesca a recuperare informazioni identificative degli interessati, sia direttamente, sia tramite metodi di correlazione e deduzione.

Pertanto, la pseudonimizzazione non consiste in una tecnica per mezzo della quale il dato diventa anonimo, ma si sostanzia in una misura di sicurezza. Il dato pseudonimizzato a differenza di quello anonimo rimane un dato personale e come tale deve essere trattato in conformità alla normativa sulla protezione dei dati.

A tal fine il singolo ricercatore dovrà concretamente:

- per quanto concerne i dati personali c.d. comuni prediligere il trattamento tramite pseudonimizzazione purchè le finalità di ricerca possano essere conseguite in tal modo.

Qualora le finalità di ricerca possano essere perseguite tramite dati resi anonimi allora egli sceglierà l'anonimizzazione (art. 89 GDPR). La necessità di anonimizzare o pseudoanonimizzare va stimata in relazione alla quantità dei dati personali raccolti, alla portata del trattamento, ai tempi di conservazione e all'accessibilità, nonché alla conoscibilità derivante da obblighi di legge.

- per quanto concerne i dati particolari (art. 9) il trattamento deve avvenire preferibilmente in forma anonima. È opportuno attenersi a tali indicazioni salvo che l'anonimato renda impossibile il conseguimento degli obiettivi dell'attività di ricerca.

In sintesi: **nel caso in cui l'attività di ricerca possa essere svolta mediante il trattamento di dati anonimi, questa soluzione è da preferire**, anche considerata la difficoltà pratica di distinguere (in sede di raccolta, soprattutto se la raccolta avviene in modo automatizzato) i dati personali comuni da quelli particolari e dal quelli relativi a condanne penali e reati o a connesse misure di sicurezza. **Nel caso in cui le finalità e gli scopi dell'attività di ricerca non possano essere conseguiti mediante il trattamento di dati anonimi, allora la soluzione preferibile da applicare** (in virtù del principio di minimizzazione) **è quella di utilizzare dati pseudonimizzati**.
Per compiere questa valutazione (*ho bisogno di trattare dati di soggetti identificabili oppure no?*), occorre che il ricercatore si interroghi sulla tipologia di trattamento in relazione alle finalità della ricerca: *a che tipo di applicazioni potenziali sto lavorando? a cosa devono servire? che caratteristiche devono avere per risultare utili ed in linea con le finalità della ricerca?*). Se, ad esempio, per effettuare la ricerca ho necessità di mantenere l'identificabilità dell'interessato, perché ad esempio sto elaborando un indicatore che combina elementi informativi provenienti da fonti diverse ma relativi al medesimo soggetto, allora l'uso di dati anonimi mi impedirebbe di conseguire questo risultato. Se, invece, ai fini dello sviluppo di una soluzione o di un modello di analisi, l'identificabilità dell'interessato non è necessaria, allora sarà preferibile operare su dati anonimi (e, se quando li raccolgo non sono anonimi, li dovrò anonimizzare prima di trattarli ulteriormente ai fini della ricerca).

Infine, sarà possibile utilizzare dati personali non pseudononimizzati solo quando il loro utilizzo è strettamente indispensabile per il conseguimento dei fini di ricerca (ma, come si capisce, è difficile dimostrare questa condizione).

A.2) Altre misure di sicurezza

Infine, i ricercatori FICO dovranno sempre garantire, in qualsiasi fase della ricerca ossia non solo nella fase della raccolta e memorizzazione o archiviazione dei dati, ma anche nella fase successiva di elaborazione delle medesime informazioni, nonché nella fase di trasmissione dei dati, **la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei**

sistemi e dei servizi di trattamento. Ciò in base al livello di rischio che il singolo ricercatore ravvisa in rapporto al trattamento dei dati personali che sta effettuando.

Tra le misure di sicurezza in oggetto si individuano a titolo esemplificativo la cifratura per i dispositivi portatili, l'installazione di firewall e antivirus locali, la predisposizione di profili di autenticazione e di autorizzazione, gli accessi limitati, i backup periodici.

In particolare, le linee guida di Ateneo prevedono che si dovrà avere riguardo a:

a) idonei accorgimenti per garantire la protezione dei dati dello studio dai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione parziale o integrale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure che rendano inintelligibili i dati ai soggetti non legittimati) nelle operazioni di registrazione e archiviazione dei dati;
b) canali di trasmissione protetti, tenendo conto dello stato dell'arte della tecnologia, nei casi in cui si renda necessaria la comunicazione dei dati raccolti nell'ambito dello studio a una banca dati centralizzata dove sono memorizzati e archiviati oppure ad un promotore o a soggetti esterni di cui lo stesso promotore si avvale per la conduzione dello studio. Laddove detta trasmissione sia effettuata mediante supporto di memorizzazione elettronico è designato uno specifico incaricato della ricezione presso il promotore ed è utilizzato, per la condivisione della chiave di cifratura dei dati, un canale di trasmissione differente da quello utilizzato per la trasmissione del contenuto;
c) con specifico riferimento alle operazioni di elaborazione dei dati dello studio, memorizzati in una banca dati centralizzata, è necessario adottare:
1. idonei sistemi di autenticazione e di autorizzazione per il personale preposto al trattamento in funzione dei ruoli ricoperti e delle esigenze di accesso e trattamento, avendo cura di utilizzare credenziali di validità limitata alla durata dello studio e di disattivarle al termine dello stesso;
2. procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti designati al trattamento;
3. sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Ciascun ricercatore dovrà infine segnalare tempestivamente al titolare del trattamento eventuali violazioni di dati personali (c.d. data breach) intervenute nell'ambito della ricerca.

B) Conservazione dei dati e comunicazione dei dati a *partner* di ricerca

In deroga (art. 5, par. 1, lett. e GDPR e art. 99 codice privacy) al principio per cui i dati personali devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità, nel caso della ricerca scientifica **i dati raccolti possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente per i medesimi fini di ricerca scientifica**.

È inoltre previsto che a fini di ricerca scientifica possono essere conservati o ceduti ad altro titolare i dati personali dei quali è cessato il trattamento, nel rispetto delle misure tecniche e organizzative più adeguate per assicurare sia il rispetto del principio di minimizzazione (pseudonimizzazione o anonimizzazione) sia la sicurezza del trattamento (ad es. cifratura per i dispositivi portatili, installazione di firewall e antivirus locali, predisposizione di profili di autenticazione e di autorizzazione, accessi limitati, backup periodici). Difatti anche la comunicazione di dati personali ad un *partner* di progetto rientra tra le operazioni di trattamento. Pertanto, nell'ambito dell'attività di ricerca congiunta con altri partners di ricerca (università, enti di ricerca ecc..) è sempre da preferire che la comunicazione di dati avvenga in forma anonima.

C) Altri adempimenti

- **Registro delle attività**

Il GDPR (art. 30) richiede che ogni attività di trattamento di dati personali debba essere inserita nel Registro delle attività di trattamento. Anche le attività di trattamento di dati personali svolte nell'ambito dei progetti di ricerca devono essere inserite nel Registro. Per consentirne l'inserimento, la scheda del progetto deve essere inviata a rpd@unipg.it da parte del Responsabile scientifico del progetto. Devono essere comunicati anche i Responsabili del trattamento designati e tutti soggetti coinvolti nel trattamento dei dati personali – ricercatori, responsabili e persone autorizzate al trattamento – devono sottoscrivere una dichiarazione d'impegno a conformarsi alle Regole deontologiche approvate dal Garante privacy (art. 3 Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica).

- **Informazioni da fornire all'interessato. Avviso sul sito FICO**

Qualora, come nell'ambito del progetto FICO, i dati personali non siano stati ottenuti dall'interessato l'art. 14 del GDPR prevede che venga ad esso rilasciata un'informativa. Tuttavia, nel caso del progetto FICO, fornire a ciascun interessato l'informativa implicherebbe uno sforzo sproporzionato in termini di risorse e di mezzi necessari (art. 14, par. 5, lett. b) GDPR; art. 105, co. 4 Codice privacy; art. 6 delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica). **Pertanto, conformemente alle previsioni normative richiamate, verranno adottate idonee forme di pubblicità consistenti nell'inserimento sul sito del progetto di ricerca FICO di una informativa accessibile a chiunque** [l'informativa è prodotta in allegato].

- **Valutazione del rischio e valutazione dell'impatto sul trattamento dei dati personali DPIA per le categorie particolari di dati personali**

Nel provvedimento del Garante contenente l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati è espressamente contemplato il

trattamento di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
L'art. 16, co. 2 lett. b) del Regolamento sul trattamento dei dati personali d'Ateneo D.R. n. 1518/2020 prevede che qualora sia effettuato su larga scala il trattamento di categorie particolari di dati particolari è necessario procedere ad una valutazione del rischio. Se tale valutazione effettuata dal gruppo di ricerca, con il proprio responsabile, evidenzia un rischio medio/alto è necessario procedere a DPIA (artt. 35 e 36 GDPR) prima di procedere al trattamento.

3. Appendice. Definizioni utili e riferimenti normativi

App.3.1 Definizioni utili

I dati si distinguono in:
- **dati personali** (art. 4 del GDPR cd. comuni): informazione che identifica o rende identificabile una persona fisica. Si tratta di nome e cognome, indirizzi di residenza, e-mail, numero di telefono, indirizzo IP, stile di vita, relazioni interpersonali, situazione economica etc. Vi rientrano anche fotografie, registrazioni audio e video. Nell'ambito della ricerca scientifica i dati personali possono essere **dati identificativi** in ragione dell'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare o da altri per identificare l'interessati, anche in base alle conoscenze acquisite in relazione al progresso tecnico (art. 104, co. 1 Codice privacy, art. 4 Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica).
- **dati particolari** (art. 9 del GDPR) che includono origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici. Per dati genetici si intendono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione. Tra i dati particolari vi sono anche i dati biometrici ossia dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici. Infine, nella categoria rientrano anche i dati relativi alla salute: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
- **dati giudiziari** (art. 10 del GDPR)**:** dati che possono rilevare l'esistenza di determinati provvedimenti giudiziari soggetti all'iscrizione del casellario giudiziale (es. provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) e la qualità di imputato, di indagato o di informazioni connesse a misure di sicurezza.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati effettuate su dati personali (ad es. raccolta, registrazione, conservazione, estrazione, consultazione, uso, diffusione, comunicazione o trasmissione, cancellazione, distruzione).

Interessato: la persona identificata o identificabile attraverso i dati o le informazioni, ossia la persona cui si riferiscono i dati trattati.

Titolare: la persona fisica o giuridica, l'autorità pubblica o altro organismo che assume le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali. In questo contesto è l'Università di Perugia. Il singolo ricercatore risulta titolare solo nei casi di ricerche che svolge personalmente, fuori da un gruppo di ricerca o di un progetto universitario.

Responsabile del trattamento: la persona fisica, giuridica, PA o ente che elabora i dati personali per conto del titolare del trattamento.

Pseudonimizzazione: procedimento che rende possibile l'attribuzione di determinate qualità a un interessato specifico solo attraverso l'utilizzo di informazioni aggiuntive, tipicamente l'impiego di chiavi crittografiche. Proprio perché tale attribuzione resta possibile, i dati pseudonimizzati devono essere trattati come informazioni relative a una persona fisica identificabile, seppure in via indiretta.

Anonimizzazione: procedimento che ha lo scopo di impedire l'identificazione dell'interessato a partire dai dati personali trattati. I dati resi anonimi, ossia che non consentono più di risalire all'interessato cui si riferiscono, non rientrano nell'ambito di applicazione della legislazione in materia di protezione dei dati. La normativa va comunque applicata dalla raccolta dei dati personali alla loro effettiva e definitiva anonimizzazione.

App. 3.2 Riferimenti normativi

- Regolamento Generale sulla Protezione dei Dati, n. 679 del 2016 o "GDPR – General Data Protection Regulation (GDPR)
- D.lgs. n. 196/2003 (riformato dal d.lgs. 101/2018) c.d. "Codice privacy"
- 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, n. 101 - 19 dicembre 2018 e art. 102, 106 d.lgs. n. 196/2003. Provvedimento del Garante del 19.12.2018 pubblicato in G.U. n. 12 del 15 gennaio 2019
- Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101. All. 1.5. Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016)
- Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, Regolamento (UE) n. 2016/679- 11 ottobre 2018. Provvedimento del Garante del 11.10.2018 pubblicato in G.U. n. 269 del 19 novembre 2018.
- Regolamento sui dati personali dell'Università degli Studi di Perugia, D.R. n. 1518/2020 (Regolamento d'Ateneo), in particolare art. 24.
- Guida pratica dell'Università degli Studi di Perugia, *La ricerca scientifica e la data protection. Applicare la normativa sulla protezione dei dati personali nei progetti di ricerca*, Versione 1.1, marzo 2021.