



UNIVERSITÀ  
POLITECNICA  
DELLE MARCHE

**DII**  
Dipartimento di Ingegneria  
dell'Informazione



**unIMC**

# Il trattamento dei dati personali in ambito giudiziario.

Rosario Calore

Dipartimento di Ingegneria dell'informazione

Università Politecnica delle Marche

Email: [rosario.calore@unimc.it](mailto:rosario.calore@unimc.it) telefono 0712204700

Venerdì 3 Ottobre 2025



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

# Obiettivi dell'elaborato

---

- Comprendere il quadro normativo
- Analizzare le tipologie di dati
- Approfondire principi e diritti
- Esaminare misure di sicurezza
- Riflettere sull'impatto della digitalizzazione



# Indice della Tesina

---

- Capitolo 1 – Quadro normativo di riferimento
- Capitolo 2 – Definizione e tipologie di dati giudiziari
- Capitolo 3 – Principi e condizioni di liceità del trattamento
- Capitolo 4 – Il trattamento nel processo giudiziario
- Capitolo 5 – Diritti dell'interessato e loro limitazioni
- Capitolo 6 – Misure di sicurezza e responsabilità
- Capitolo 7 – Casi pratici e giurisprudenza
- Capitolo 8 – Prospettive future e digitalizzazione
- Conclusioni
- Riferimenti bibliografici



# Capitolo 1 – Quadro normativo di riferimento



## 1.1 Il Regolamento Generale sulla Protezione dei Dati (GDPR)

Il Regolamento (UE) 2016/679, noto come GDPR, rappresenta il pilastro della normativa europea in materia di protezione dei dati personali. Esso stabilisce i principi generali del trattamento, tra cui: liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

# Capitolo 1 – Quadro normativo di riferimento



## 1.2 Il Codice Privacy (D. lgs. 196/2003)

Il Codice in materia di protezione dei dati personali, introdotto con il D.lgs. 196/2003 e aggiornato dal D.lgs. 101/2018, recepisce il GDPR nel sistema italiano. Esso contiene disposizioni specifiche per il trattamento dei dati giudiziari, in particolare l'art. 2-octies e l'art. 10 GDPR.

## 1.3 La Direttiva UE 2016/680

La Direttiva UE 2016/680 disciplina il trattamento dei dati personali da parte delle autorità competenti per finalità di prevenzione, indagine, accertamento e perseguimento di reati. In Italia, è stata recepita con il D.lgs. 51/2018.

# Capitolo 1 – Quadro normativo di riferimento



## 1.4 Il ruolo del Garante per la protezione dei dati personali

Il Garante Privacy è l'autorità indipendente che vigila sull'applicazione delle norme in materia di protezione dei dati. In ambito giudiziario, il Garante esprime pareri, definisce garanzie appropriate e emette provvedimenti e sanzioni.

## Capitolo 2 – Definizione e tipologie di dati giudiziari



### 2.1 Cosa sono i dati giudiziari

Secondo l'art. 10 del GDPR, i dati giudiziari sono dati personali relativi a condanne penali e reati o a connesse misure di sicurezza.

### 2.2 Tipologie di dati giudiziari

Condanne penali definitive, misure di sicurezza, carichi pendenti, qualità di indagato o imputato, misure di prevenzione.

## Capitolo 2 – Definizione e tipologie di dati giudiziari



### 2.3 Differenza tra dati comuni, sensibili e giudiziari

Dati comuni: identificativi;

Sensibili: salute, orientamento sessuale;

Giudiziari: condanne e reati.

### 2.4 Ambito di applicazione

Soggetti pubblici: D.lgs. 51/2018;

Soggetti privati: art. 10 GDPR e art. 2-octies Codice Privacy.

# Capitolo 3 – Principi e condizioni di liceità del trattamento



## 3.1 Principi generali del trattamento

Liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, conservazione, integrità e riservatezza.

## 3.2 Condizioni di liceità del trattamento

Art. 6 GDPR: consenso, contratto, obbligo legale, interesse pubblico. Art. 10 GDPR: autorizzazione da legge o controllo pubblico.

## 3.3 Il principio di necessità e proporzionalità

Trattamento solo se indispensabile e proporzionato.

## 3.4 Designazione del DPO

Obbligo di nomina del DPO per trattamenti su larga scala di dati giudiziari.

# Capitolo 4 – Il trattamento nel processo giudiziario



## **4.1 Acquisizione e uso dei dati nel processo**

Dati acquisiti tramite atti di indagine, documenti, testimonianze.

## **4.2 Ruolo del giudice e degli ausiliari**

Trattamento lecito per esercizio di pubblici poteri. Misure di sicurezza richieste.

## **4.3 Accesso al fascicolo da parte delle parti e dei terzi**

Parti: diritto di accesso. Terzi: accesso limitato. Bilanciamento tra trasparenza e riservatezza.

## **4.4 Conservazione e pubblicazione degli atti**

Conservazione congrua. Pubblicazione con anonimizzazione e rispetto delle linee guida del Garante.

# Capitolo 5 – Diritti dell'interessato e loro limitazioni



## 5.1 I diritti riconosciuti dal GDPR

Accesso, rettifica, cancellazione, limitazione, portabilità, opposizione, decisioni automatizzate.

## 5.2 Limitazioni per motivi di giustizia

Art. 23 GDPR e art. 2-duodecies Codice Privacy: deroghe per salvaguardare la giustizia.

## 5.3 Bilanciamento tra privacy e diritto alla difesa

Giurisprudenza: prevalenza del diritto alla difesa.

## 5.4 Garanzie e trasparenza

Trasparenza, sicurezza, proporzionalità, comunicazione motivata.

# Capitolo 6 – Misure di sicurezza e responsabilità



## **6.1 Principio di responsabilizzazione**

Privacy by design e by default. Documentazione e valutazione dei rischi.

## **6.2 Misure tecniche e organizzative**

Cifratura, controllo accessi, backup, formazione.

## **6.3 Valutazione d'impatto (DPIA)**

Obbligatoria per trattamenti ad alto rischio. Consultazione del Garante.

## **6.4 Obblighi del titolare e del responsabile**

Designazione DPO, registro trattamenti, notifica violazioni, sanzioni.

# Capitolo 7 – Casi pratici e giurisprudenza



## **7.1 Provvedimenti del Garante Privacy**

Pareri su protocolli, garanzie appropriate, consenso non valido.

## **7.2 Sentenze della Cassazione**

Sentenza n. 3702/2022: anonimizzazione. Sentenza n. 35548/2020: compressione della riservatezza.

## **7.3 Esempi di violazioni e sanzioni**

Art. 167 Codice Privacy: reclusione. GDPR: sanzioni pecuniarie

# Capitolo 8 – Prospettive future e digitalizzazione



## 8.1 La giustizia telematica

Processo Civile Telematico, digitalizzazione del processo penale.

I due principali sistemi digitali utilizzati in Italia per la gestione dei procedimenti civili e penali sono:

## 8.2 Processo Civile Telematico (PCT)

Il sistema informatico dedicato alla digitalizzazione del processo civile.

Consente il deposito telematico degli atti, la consultazione dei fascicoli, le notifiche elettroniche e la gestione documentale.

È operativo in gran parte degli uffici giudiziari e ha semplificato notevolmente le attività di avvocati, magistrati e cancellieri.

## Capitolo 8 – Prospettive future e digitalizzazione



### 8.3 Processo Penale Telematico (PPT)

È il corrispettivo del PCT per il processo penale.

Utilizza l'Applicativo per il Processo Penale, noto come APP, sviluppato dal Ministero della Giustizia.

Include funzionalità come il deposito telematico degli atti, la consultazione dei fascicoli digitali e le notifiche elettroniche.

È ancora in fase di evoluzione, con l'obiettivo di estendere la digitalizzazione a tutti gli uffici, compresi quelli del Giudice di Pace e del Tribunale di Sorveglianza.

Entro il 2028 è previsto il lancio di un'unica piattaforma per tutti i procedimenti (civili, penali, amministrativi, tributari e contabili), con interoperabilità completa tra i sistemi del Ministero della Giustizia e quelli di altri enti che sarà gestita dal PSN.

## Capitolo 8 – Prospettive future e digitalizzazione



### 8.4 Polo Strategico Nazionale

Il PSN è un'infrastruttura cloud ad alta affidabilità per ospitare dati e servizi critici della Pubblica Amministrazione italiana. Gestito da Polo Strategico Nazionale S.p.A., partecipata da TIM, Leonardo, CDP Equity e Sogei.

Gli obiettivi del PSN consistono nel garantire la sovranità dei dati nazionali, migliorare la sicurezza informatica, supportare la digitalizzazione della PA, offrire infrastrutture moderne e sostenibili.

## Conclusioni



Il trattamento dei dati personali in ambito giudiziario richiede un equilibrio tra esigenze di giustizia e tutela dei diritti. La normativa europea e italiana offrono un quadro rigoroso, ma la digitalizzazione impone nuove sfide.

È essenziale promuovere una cultura della protezione dei dati per garantire una giustizia equa e rispettosa della dignità umana.

## Riferimenti bibliografici



1. Regolamento (UE) 2016/679 (GDPR)
2. Decreto Legislativo 30 giugno 2003, n. 196 (Codice Privacy)
3. Decreto Legislativo 18 maggio 2018, n. 51
4. Garante Privacy, Linee guida 2010
5. Bruno Saetta, ProtezioneDatiPersonali.it, 2022
6. Agenda Digitale, Marina Rita Carbone, 2021
7. Cassazione Civile, Sentenza n. 35548/2020
8. Cassazione Penale, Sentenza n. 3702/2022