UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Analisi comparativa dei regolamenti internazionali sul trattamento dei dati personali

Massimiliano Alfieri

Dipartimento di Ingegneria dell'Informazione - DII

www.linkedin.com/in/massimiliano-alfieri-ing
massimiliano1alfieri@gmail.com

Giovedì 2 Ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Sommario

Il trattamento dei dati personali è disciplinato da normative che variano in funzione dei contesti giuridici nazionali e sovranazionali.

Questa analisi comparativa esamina le *similitudini* e le *differenze* tra i vari quadri normativi, prendendo in considerazione i principali regolamenti internazionali sul trattamento dei dati personali:

- *Regolamento Generale sulla Protezione dei Dati* (**GDPR**), Unione Europea;
- *California Consumer Privacy Act* (**CCPA**), California;
- *Legge sulla Protezione dei Dati Personali* (**LGPD**), Brasile;
- *Personal Information Protection Law* (**PIPL**), Cina.

Argomenti

- **1 Introduzione**
  - Differenze tra *Regolamento* e *Direttiva nell'ambito UE*
  - *Garante* per la protezione dei dati personali
- **2 Regolamento Europeo**
  - Caratteristiche principali
  - Struttura e contenuti
  - *Data Protection Officer* (DPO)
- **3 Regolamenti extra-UE**
  Caratteristiche principali
- **4 Confronto tra i regolamenti**
  Tabella comparativa
- **5 Giurisprudenza**
  Caso *Foodinho S.r.l.*
- **6 Conclusioni**

Introduzione

Differenze tra *Regolamento* e *Direttiva nell'ambito UE*

Regolamento e *direttiva* sono due tipi di atti legislativi dell'Unione Europea che hanno scopi e caratteristiche diverse.

- **regolamento:**
  - è vincolante e si applica direttamente negli Stati membri dopo la sua entrata in vigore;
  - è obbligatorio in tutti i suoi elementi e non lascia spazio a scelte o interpretazioni alle autorità nazionali.
- **direttiva:**
  - stabilisce un obiettivo che tutti i paesi dell'UE devono conseguire;
  - non è direttamente applicabile negli Stati membri, ma deve essere recepita nel diritto nazionale prima di essere applicabile;
  - vincola gli Stati membri a raggiungere un determinato risultato, lasciando alle autorità nazionali la scelta della forma e dei mezzi per raggiungere tale scopo.

Garante per la protezione dei dati personali

È un'**autorità amministrativa indipendente italiana**, istituita dalla legge n. 675 del 1996.

I Compiti del Garante sono definiti dal:

- Regolamento (UE) 2016/679;
- codice in materia di protezione dei dati personali (D. Lgs. 30/06/2003, n.196), adeguato alle disposizioni del GDPR tramite il D. Lgs. 10/08/2018, n. 101;
- altri atti normativi italiani e internazionali.

Il Garante si occupa, tra l'altro, di:

- controllare la conformità del trattamento dei dati personali al GDPR e alla normativa nazionale;
- esaminare reclami e sanzionare le violazioni con ammonimenti, limitazioni o cancellazioni dei dati;
- collaborare con autorità nazionali e internazionali per l'attuazione del Regolamento;
- segnalare al Parlamento e ad altri organismi la necessità di nuove normative;
- partecipare alle attività UE e internazionali su privacy e protezione dei dati;
- informare e sensibilizzare i cittadini, con particolare attenzione ai minori;
- imporre sanzioni pecuniarie e condurre consultazioni pubbliche per migliorare la regolamentazione.

Regolamento Europeo

Regolamento Generale sulla Protezione dei Dati (GDPR), UE

In vigore dal 25/05/2018

Caratteristiche principali:

- **ambito di applicazione:**
  si applica a tutte le aziende che trattano dati personali di cittadini UE, indipendentemente dalla loro sede;
- **base giuridica per il trattamento:**
  richiede una base legale per il trattamento, come il consenso esplicito o obblighi contrattuali;
- **diritti degli interessati:**
  diritto all'accesso, alla rettifica, alla cancellazione (*diritto all'oblio*), alla portabilità dei dati, alla limitazione del trattamento e all'opposizione;
- **sanzioni:**
  le aziende devono dimostrare la conformità e possono essere multate fino al 4% del fatturato globale o 20 milioni di euro;
- **notifica delle violazioni:**
  obbligo di segnalare violazioni di dati alle autorità entro 72 ore.

Struttura e contenuti del GDPR

Tabella 1

CAPO	TITOLO	SEZIONI	ARTICOLI
I	Disposizioni generali	-	1 ÷ 4
II	Principi	-	5 ÷ 11
III	Diritti dell'interessato	5	12 ÷ 23
IV	Titolare del trattamento e responsabile del trattamento	5	24 ÷ 43
V	Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali	-	44 ÷ 50
VI	Autorità di controllo indipendenti	2	51 ÷ 59
VII	Cooperazione e coerenza	3	60 ÷ 76
VIII	Mezzi di ricorso, responsabilità e sanzioni	-	77 ÷ 84
IX	Disposizioni relative a specifiche situazioni di trattamento	-	85 ÷ 91
X	Atti delegati e atti di esecuzione	-	92 e 93
XI	Disposizioni finali	-	94 ÷ 99

Responsabile della Protezione dei Dati - Data Protection Officer (DPO)

Articoli del GDPR che riguardano il DPO:

- **Art. 37** Designazione del responsabile della protezione dei dati;
- **Art. 38** Posizione del responsabile della protezione dei dati;
- **Art. 39** Compiti del responsabile della protezione dei dati.

Ruolo del DPO:

- è responsabile della protezione dei dati personali all'interno dell'organizzazione;
- garantisce la conformità alle norme sulla protezione dei dati;
- identifica e valuta i rischi per la protezione dei dati;
- implementa misure per ridurre i rischi e proteggere i dati personali;
- collabora con le autorità competenti per risolvere eventuali controversie o violazioni dei dati.

Regolamenti extra-UE

Regolamenti extra-UE (1/3)

California Consumer Privacy Act (CCPA), California

In vigore dal 01/01/2020

Caratteristiche principali:

- **ambito di applicazione:**
  si applica alle aziende con un fatturato annuo superiore a 25 milioni di dollari, che trattano i dati di 50.000 o più consumatori o che generano almeno il 50% dei ricavi dalla vendita di dati;
- **base giuridica per il trattamento:**
  il consenso non è sempre richiesto, ma le aziende devono fornire trasparenza sulle pratiche di raccolta e vendita dei dati;
- **diritti degli interessati:**
  diritto di accesso, diritto alla cancellazione e diritto di *opt-out* dalla vendita dei dati;
- **sanzioni:**
  multe fino a 7.500 dollari per violazione intenzionale e 2.500 dollari per violazione non intenzionale;
- **notifica delle violazioni:**
  non obbligatoria per tutte le violazioni.

Regolamenti extra-UE (2/3)

Legge sulla Protezione dei Dati Personali (LGPD), Brasile

in vigore dal 18/09/2020

Caratteristiche principali:

- **ambito di applicazione:**
  si applica a tutte le aziende che trattano dati di cittadini brasiliani, indipendentemente dalla sede;
- **base giuridica per il trattamento:**
  richiede una base giuridica per il trattamento, simile al GDPR;
- **diritti degli interessati:**
  simili a quelli del GDPR, includendo accesso, rettifica, cancellazione e portabilità;
- **sanzioni:**
  multe fino al 2% del fatturato annuo in Brasile, con un massimo di 50 milioni di real brasiliani per violazione;
- **notifica delle violazioni:**
  obbligo di segnalazione, ma senza tempistiche rigide come nel GDPR

Regolamenti extra-UE (3/3)

Personal Information Protection Law (PIPL), Cina

in vigore dal 01/11/2021

Caratteristiche principali:

- **ambito di applicazione:**
  globale, sia territoriale che extraterritoriale (se tratta dati di cittadini cinesi);
- **base giuridica per il trattamento:**
  necessario per dati sensibili e trasferimenti internazionali;
- **diritti degli interessati:**
  accesso, correzione, cancellazione, restrizione del trattamento e ritiro del consenso;
- **sanzioni:**
  multe fino al 5% del fatturato per violazioni gravi;
- **notifica delle violazioni:**
  obbligatoria, tempestiva, ma senza limiti di tempo definiti.

Confronto tra i regolamenti

Confronto tra i regolamenti

Tabella 2

Caratteristica	GDPR (UE)	CCPA (California)	LGPD (Brasile)	PIPL (Cina)
ambito di applicazione	globale (se tratta dati di cittadini UE)	solo grandi aziende con criteri specifici	globale (se tratta dati di cittadini brasiliani)	globale (se tratta dati di cittadini cinesi)
base giuridica per il trattamento	obbligatoria (es. consenso o contratto)	non sempre richiesta	obbligatoria (simile al GDPR)	necessaria per dati sensibili e trasferimenti internazionali
diritti degli interessati	ampi: accesso, rettifica, cancellazione, portabilità e opposizione	limitati: accesso, cancellazione e opt-out dalla vendita	simili al GDPR	accesso, correzione, cancellazione, restrizione del trattamento, ritiro del consenso
Sanzioni (max)	4% del fatturato globale o 20 milioni €	7.500 $ per violazione intenzionale	2% del fatturato in Brasile o 50 milioni R$	5% del fatturato annuo o 50 milioni di RMB
notifica violazioni	entro 72 ore	non sempre obbligatoria	obbligatoria, ma senza limiti di tempo definiti	obbligatoria e tempestiva, ma senza limiti di tempo definiti

Giurisprudenza

Giurisprudenza 1/2

Azienda coinvolta: Foodinho S.r.l.

Una società controllata da GlovoApp23 che opera nel settore *food delivery* e altri beni.
Utilizza una piattaforma digitale per la gestione degli ordini e il coordinamento dei rider.

- **Provvedimento del Garante, n.234 del 10/06/2021:**
  - **sanzione** amministrativa pecuniaria imposta: **2,6 milioni di euro**
  - **violazioni** riscontrate:
    - mancanza di trasparenza nell'uso dei dati dei rider;
    - trattamento automatizzato non conforme agli standard GDPR;
    - assenza di adeguate misure per garantire la non discriminazione algoritmica.

Giurisprudenza 2/2

- **Sentenza del Tribunale di Milano, n.35612 del 12/04/2022:**

Ha annullato integralmente la sanzione precedentemente esposta, ritenendola *fortemente sproporzionata* e *illegittima* rispetto ai parametri sanzionatori indicati nell'articolo 83 del GDPR.

art. 83 del GDPR: “Condizioni generali per infliggere sanzioni amministrative pecuniarie”

Accogliendo la tesi difensiva di Foodinho, assistita da **Hogan Lovells** (uno studio legale internazionale statunitense-britannico).

Conclusioni

Conclusioni

Confrontando i diversi regolamenti, si evidenzia che:

- **GDPR** è il più rigido e ha un'ampia portata extraterritoriale;
- **CCPA** è meno rigido rispetto al GDPR e permette maggiore flessibilità alle aziende;
- **LGPD** segue il modello GDPR, ma con alcune differenze in termini di attuazione;
- **PIPL** controllo severo da parte del governo e impone regole stringenti alle aziende straniere che trattano i dati di cittadini cinesi.

Inoltre:

- Le **aziende multinazionali**, per evitare sanzioni, devono adottare un approccio strategico e flessibile per conformarsi ai vari regolamenti sul trattamento dei dati nei diversi paesi. Per esempio, implementando *principi base di privacy* e creando un *sistema di gestione unico* che possa essere adattato alle diverse normative.
- Il **DPO** si distingue come una figura chiave nella governance della privacy a livello internazionale. Sebbene il suo ruolo vari tra le diverse giurisdizioni, la sua presenza risulta fondamentale per garantire trasparenza, responsabilità e tutela dei diritti degli interessati.