ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Informatica e diritto
A.A. 2023/2024

La protezione dei dati personali

Prof. Andrea Amidei

Dipartimento di Informatica – Scienza e Ingegneria

Elezioni politiche

Il Garante per la privacy chiede chiarimenti sulle attività di Facebook in vista del voto

La società: "Gli strumenti elettorali lanciati in Italia sono stati espressamente progettati per rispettare la privacy degli utenti e conformarsi al Gdpr"

ANSA.it › Tecnologia › Internet & Social › **Meta-Facebook aggiorna l'informativa privacy, 'più chiara'**

Meta-Facebook aggiorna l'informativa privacy, 'più chiara'

In vigore dal 26 luglio, da oggi avvisi agli utenti. Esperto, le normative europee funzionano

TECH

TikTok could face a $29 million fine in the UK for failing to protect kids' privacy

PUBLISHED MON, SEP 26 2022•8:05 AM EDT | UPDATED 6 HOURS AGO

IL PARERE

Sanità digitale, no del Garante Privacy alla nuova banca dati del Fascicolo elettronico

Dati: privacy vs. data protection

«I dati ridefiniranno il nostro modo di produrre, consumare e vivere» (Commissione Europea, 2020)

Sviluppo ed impiego delle tecnologie informatiche → perdita di controllabilità del dato da parte dell'interessato → esigenza di regolare il fenomeno

→ Diritto dell'interessato a **controllare, conoscere e limitare la circolazione dei propri dati**

→ Privacy ≠ data protection

→ Tutela dei soli dati personali

Cos'è un dato?

Un dato personale è:

- un elemento rappresentativo di una informazione
- riferito ad una determinata persona (fisica)
- e che consenta, direttamente o indirettamente, di individuare il soggetto al quale è riferito

Dato ≠ **informazione**

Dati personali vs. **Big data**

Il dato come «merce di scambio»

Il **valore economico** del dato

WIRED

LUCA ZORLONI 30 agosto 2017 SECURITY

L'Antitrust scova regole "vessatorie" nel contratto di Pokémon Go

Dalla responsabilità sul servizio alle norme per le controversie tra giocatori e azienda, c'è uno squilibrio tra i diritti di Niantic e quelli degli utenti

Il dato come «merce di scambio»

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

PS11147-PS11150 - Sanzioni per 20 milioni a Google e ad Apple per uso dei dati degli utenti a fini commerciali

L'Autorità ha accertato due violazioni del Codice del Consumo, una per carenze informative e un'altra per pratiche aggressive riguardo all'acquisizione e all'utilizzo dei dati dei consumatori

L'Autorità Garante della Concorrenza e del Mercato ha chiuso due istruttorie nei confronti di Google Ireland Ltd. e di Apple Distribution International Ltd., sanzionando entrambe per 10 milioni di euro ossia per il massimo edittale secondo la normativa vigente. L'Antitrust ha accertato per ogni società due violazioni del Codice del Consumo, una per carenze informative e un'altra per pratiche aggressive legate all'acquisizione e all'utilizzo dei dati dei consumatori a fini commerciali.

Google fonda la propria attività economica sull'offerta di un'ampia gamma di prodotti e di servizi connessi a Internet - che comprendono tecnologie per la pubblicità online, strumenti di ricerca, cloud computing, software e hardware - basata anche sulla profilazione degli utenti ed effettuata grazie ai loro dati. Apple raccoglie, profila e utilizza a fini commerciali i dati degli utenti attraverso l'utilizzo dei suoi dispositivi e dei suoi servizi. Quindi, pur senza procedere ad alcuna cessione di dati a terzi, Apple ne sfrutta direttamente il valore economico attraverso un'attività promozionale per aumentare la vendita dei propri prodotti e/o di quelli di terzi attraverso le proprie piattaforme commerciali App Store, iTunes Store e Apple Books.

In tali contesti, l'Autorità ha ritenuto che esiste un rapporto di consumo tra gli utenti e i due operatori, anche in assenza di esborso monetario, la cui controprestazione è rappresentata dai dati che essi cedono utilizzando i servizi di Google e di Apple.

- **Pre-flagging**
- E per i **dati non personali**? Nei rapporti tra imprese?

Il Regolamento Generale sulla Protezione dei Dati (GDPR)

Fonte **primaria** di disciplina della materia:

Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali, nonché alla libera circolazione di tali dati (GDPR)

+ normativa italiana di contorno

Gestione del rischio (risk management): parametrare obblighi e misure di sicurezza al rischio concreto connesso alla specifica attività

Il Regolamento Generale sulla Protezione dei Dati (GDPR)

Regola il rapporto tra:

- **Interessato** (data subject) = persona (fisica) a cui si riferiscono i dati
- **Titolare** del trattamento (data controller) = persona (fisica o giuridica) alla quale l'interessato cede i dati e che stabilisce come usarli, decide in ultima istanza come e perché usarli

«Trattamento» = qualunque operazione che abbia ad oggetto uno o più dati personali

→ raccolta, registrazione, organizzazione, uso, cancellazione, conservazione, estrazione, ecc.

Il Regolamento Generale sulla Protezione dei Dati (GDPR)

Ambito applicativo:

- tutela esclusivamente le **persone fisiche**
- si applica a **tutti i tipi di trattamenti** (elettronici, cartacei, manuali)
- si applica a tutti i trattamenti effettuati **da chiunque abbia sede nel territorio dell'UE**
- si applica tutti i trattamenti svolti **all'estero** in relazione a beni o servizi offerti a soggetti **che si trovano nell'UE**
- **non** si applica a trattamenti soltanto **«domestici»** o **«personali»** effettuati **da persone fisiche**

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Alcuni esempi pratici…

- Società che raccoglie i numeri di telefono dei dipendenti per organizzare una festa di pensionamento per un collega
- Società con sede negli Stati Uniti che elabora dati di aziende clienti con sede in Francia
- Sito di e-commerce gestito da società con sede in Cina; le attività di trattamento sono svolte solo in Cina; la società apre un ufficio a Berlino per gestire marketing
- Società farmaceutica con sede a Stoccolma colloca il trattamento di tutti i propri dati in Cina

I protagonisti della data protection

- **Interessato** (data subject)

→ persona fisica

- **Titolare del trattamento** (data controller)

→ persona fisica o giuridica (se giuridica, è l'ente)

- **Responsabile del trattamento** (data processor)

→ persona fisica o giuridica (eventuale)

- **Soggetto autorizzato**

→ persona fisica

- **Data Protection Officer** (DPO) (se trattamenti particolarmente sensibili o complessi)

→ persona fisica

Data protection: i principi fondamentali

- **Liceità**: rispetto di tutte le norme dell'ordinamento
- **Trasparenza**: l'interessato deve sapere che i suoi dati sono oggetto di trattamento
- **Limitazione delle finalità**: i) le finalità del trattamento devono essere determinate e non generiche e ii) il trattamento deve essere limitato a quelle finalità
- **Minimizzazione dei dati**: i dati devono essere limitati a quanto necessario alle finalità del trattamento
- **Esattezza**: i dati devono essere esatti ed aggiornati
- **Limitazione della conservazione**: non deve eccedere il tempo necessario per le finalità

Alcuni esempi…

- Medico che utilizza gli indirizzi di ex pazienti per inviare lettere a sostegno di un candidato alle elezioni politiche
- Sito web di informazione giuridica che, ai fini dell'iscrizione ad un servizio di invio di newsletter via e-mail, richiede dati relativi al sesso dei destinatari
- Supermercato che al fine dell'iscrizione ad un «programma fedeltà» richiede dati relativi al reddito annuo dei consumatori
- Sito web su iscrizione che opera a livello mondiale e che offre l'informativa sui dati solo in inglese

Data protection: i principi fondamentali

Regola generale: serve il **consenso dell'interessato** (è la «base giuridica» principale del trattamento)

→ il consenso deve essere libero ed effettivo → informativa

→ forma libera (ma problema di prova…)

→ il consenso deve essere specifico per ogni finalità

- Quando non serve il consenso dell'interessato?

→ **obblighi legali** ed **esecuzione di un contratto con l'interessato**

- Dati **«particolari»**

Gli adempimenti per il titolare

→ **Informativa** all'interessato

→ **Misure di sicurezza** organizzative e tecniche

→ Nomina del **DPO** (eventuale)

→ **Registro delle attività di trattamento** (eventuale → i) se azienda > 250 dipendenti, o ii) se sussistono rischi elevati per diritti degli interessati, o iii) se si trattano dati particolari, o iv) se trattamenti non occasionali)

L'informativa

- Da fornire all'interessato prima dell'inizio del trattamento
- Per iscritto (regola generale), oralmente o con altri mezzi (ma come si **dimostra**…?)
- Trasparenza + comprensibilità + proporzionalità
- Contenuto obbligatorio → in particolare:
  - Modalità, scopo e durata di ogni trattamento
  - Dati titolare
  - Avviso su conseguenze mancato consenso
  - **Diritti dell'interessato**:
    - Portabilità
    - Rettifica
    - Cancellazione

L'informativa: alcuni casi pratici

Supermoney S.p.A. (Garante, 2018):

- sito di confronto offerte (mutui, gas, luce, polizze)
- popup con caselle di testo editabili per inserimento dati e casella di spunta con seguente formula:

  «*Ho letto l'informativa privacy e acconsento al trattamento dei dati*» (con link ad informativa)
- l'informativa chiariva le diverse finalità del trattamento: esecuzione del servizio + invio di comunicazioni promozionali proprie o di terzi + comunicazione di dati a terzi, anche extra-UE, per finalità di marketing

→ Perché il Garante ha sanzionato?

L'informativa: alcuni casi pratici

Vestas (Garante, 2019):

- sito prenotazioni online per un resort
- informativa: i dati verranno utilizzati «*per l'esecuzione degli obblighi derivanti dai contratti conclusi o dalla legge e per ricerche di mercato e direct marketing*»
- consenso unico per tutte le finalità
- difesa della società: anche se cliente dà consenso, in concreto il dato personale non viene utilizzato per finalità di marketing perché solo all'arrivo in hotel i dati vengono raccolti in modalità cartacea e viene chiesto un nuovo consenso

→ Il Garante ha sanzionato oppure no?

Le misure di sicurezza...

Il titolare deve porre in essere misure tecniche e organizzative adeguate al rischio → **risk management**:

1. individuazione rischi concreti e specifici connessi al trattamento e conseguenze per l'interessato;
2. ricognizione stato dell'arte della tecnica e dei costi;
3. individuazione misure specifiche e proporzionate utili a scongiurare specifici rischi di cui al punto 1.

→ **Data Protection Impact Assessment**

- Fase preliminare + ripetuto regolarmente nel tempo
- Obbligatorio se rischio elevato

… e la privacy by design (e by default)

Principio (e metodo) del «by design»

→ Il rispetto delle regole deve essere incorporato a partire dalla progettazione di ogni processo aziendale e di ogni applicazione informatica utilizzata (con «barriere» e «blocchi» da progettare e inserire sin dalla partenza)

+ Privacy «by default»: i processi aziendali e le applicazioni informatiche devono essere progettati per garantire (di default, per l'appunto) il rispetto dei principi fondamentali in materia di data protection

I trattamenti (interamente) automatizzati

Trattamenti **interamente automatizzati**: effettuati con supporti tecnologici senza alcun apporto umano

(esempio: profilazione)

(esempio: *credit scoring*)

Art. 22 GDPR → l'interessato ha diritto a non essere sottoposto a decisioni :

- basate unicamente su un trattamento di tipo automatizzato (ivi inclusa la profilazione)
- se la decisione incide in modo significativo sulla sua persona

I trattamenti (interamente) automatizzati

Quando sono leciti?

- Quando l'interessato ha dato espressamente il proprio **consenso** (a tale tipologia di trattamento)
- Quando lo prevede la legge
- Quando sono indispensabili ai fini dell'esecuzione di un contratto con l'interessato

→ Prevista possibilità di intervento umano

→ Prevista possibilità di contestare la decisione

→ **Diritto a <u>spiegazione</u> e <u>trasparenza</u>** (ma quale?)

Diritto alla spiegazione… ma quale?

Quanto (e come) deve essere comunicato all'interessato?

Recente caso della Corte di Cassazione (maggio 2021) su sistema automatizzato di calcolo per la definizione del rating reputazionale

«non può logicamente affermarsi che l'adesione a una piattaforma da parte dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione di dati personali, laddove non siano resi conoscibili lo ***schema esecutivo*** *in cui l'algoritmo si esprime e gli* ***elementi*** *all'uopo* ***considerati****»*

I data breach

Data breach = evento al quale consegue una violazione dei dati personali trattati, ivi inclusa (spesso) una violazione dei sistemi informatici del titolare

→ **Notifica a Garante per la Protezione dei Dati Personali +** (nei casi più gravi) **ai diretti interessati**

- Da effettuare entro 72 ore dalla scoperta del breach
- Non è sempre obbligatoria

→ obbligo parametrato al rischio effettivo, alla rilevanza dei dati «persi» ed alle potenziali conseguenze della perdita

Alcuni esempi…

- Un attacco ransomware causa la crittografia di tutti i dati contenuti nei sistemi e non esiste un backup
- Un supporto contenente un backup criptato con dati personali viene rubato
- Una interruzione di un'ora nel funzionamento del server impedisce agli interessati di accedere ai propri dati personali mediante il sito web
- Un errore nel codice del sistema che controlla l'accesso ad un sito web consente a tutti gli utenti loggati di accedere ai dati personali degli altri utenti
- Un cliente di una banca riceve per errore via mail l'estratto conto di un altro cliente

Le conseguenze di eventuali violazioni

- Responsabilità civile

→ **Risarcimento** del danno subito dall'interessato (deve esistere ed essere dimostrato un danno);

→ Il trattamento di dati personali (o almeno di alcuni tipi di dati personali) è «attività pericolosa»?

- Responsabilità amministrativa:

→ Il Garante per la Protezione dei Dati Personali può imporre **sanzioni** parametrate a i) gravità e ii) fatturato mondiale annuo

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Prof. Andrea Amidei
Informatica e Diritto

Dipartimento di Informatica - Scienza e Ingegneria

andrea.amidei3@unibo.it