

Elementi di cultura aziendale, professionale, giuridica e
sociale

Università di Genova - a.a. 2023/2024

La normativa europea in materia digitale

Avv. Manuela Bianchi - manuela.bianchi@bmsfarm.it

Mi presento

Manuela Bianchi

Avvocata, Data Protection Officer, Insegnante, Autrice

Programma del corso

- La normativa europea in materia digitale: GDPR, AI Act, DSA, DMA, cookie)
- Com'è fatta un'azienda
- Licenze software
- Certificazioni aziendali e professionali
- Diversità e inclusione in azienda

Regolamento europeo sulla protezione dei dati (GDPR) UE n. 679/2016

- entrato in vigore il 25 maggio 2018
- direttamente applicabile negli ordinamenti giuridici degli Stati membri
- rinforza la protezione dei diritti dei soggetti interessati con riferimento al trattamento dei dati personali, dando risalto al principio in base al quale la protezione dei dati è uno dei diritti fondamentali della UE
- garantisce il libero flusso dei dati personali all'interno della UE

Nuove opportunità per le società e per il business (1/2)

- condizioni di parità per tutte le società che operano nel mercato europeo
- i principi di “privacy by design” e “privacy by default” creano incentivi per la ricerca di soluzioni informatiche innovative per la protezione dei dati fin dall’inizio della progettazione
- diritti individuali rafforzati
- maggiore controllo da parte delle persone fisiche sui propri dati
- maggiore protezione contro la violazione dei dati

Nuove opportunità per le società e per il business (2/2)

- maggiore flessibilità per titolari e responsabili che trattano dati grazie a disposizioni più chiare in materia di responsabilità
- la protezione dei dati garantita dal GDPR viaggia al di fuori della UE, garantendo una maggiore tutela

AI ACT

(approvato dal Parlamento europeo il 13 marzo 2024)

OBIETTIVI

- sviluppare un quadro normativo uniforme che favorisca il buon funzionamento del mercato unico digitale e lo sviluppo di tecnologie e prodotti basati sull'intelligenza artificiale
- garantire la sicurezza e la conformità dei sistemi di IA immessi sul mercato con la normativa europea in materia di diritti fondamentali
- predisporre una governance efficace che garantisca l'applicazione della normativa esistente in materia di diritti fondamentali e sicurezza ai sistemi di IA

APPROCCIO BASATO SUL RISCHIO per la salute e la sicurezza e per i diritti fondamentali delle persone fisiche

- inaccettabile
- alto rischio
- rischio minimo

APPLICAZIONI DI IA PROIBITE sono quelle coi seguenti scopi:

- manipolare le persone, in modo da arrecare danni fisici e psicologici
- sfruttare la vulnerabilità delle persone
- classificare le persone e assegnarle a categorie sulla base di caratteristiche sensibili
- social scoring
- identificazione biometrica remota, possibile solo se in tempo reale e solo se mirata: (i) alla ricerca di potenziali vittime di un reato; (ii) alla prevenzione di una minaccia specifica, sostanziale o imminente per la vita o l'incolumità delle persone o di un attacco terroristico; (iii) identificare e perseguire l'autore di un reato per cui è previsto il mandato d'arresto europeo

DIGITAL SERVICE ACT

(Regolamento UE sui servizi digitali)

(Regolamento UE 2022/2065)

- entrato in vigore il 17 febbraio 2024, sebbene vincolante dal 25 agosto 2023 per i “gatekeepers” (ovvero le LoPs - Large Online Platforms: Google con 4 servizi, YouTube, Meta, Bing, X, Pinterest, Snapchat, Amazon, LinkedIn, Booking, Wikipedia, AppStore di Apple, TikTok, Alibaba Express, Zalando)
- si applica a intermediari e piattaforme online come marketplace, social network, piattaforme per la condivisione di contenuti, app store e piattaforme online per viaggi e alloggi
- obiettivo: prevenire le attività illegali e dannose online e la diffusione di notizie false, garantire la sicurezza degli utenti e proteggere i diritti fondamentali stabilendo norme chiare e proporzionate per le attività online

- promuove l'innovazione, la crescita e la competitività e facilita l'espansione delle piattaforme più piccole, delle pmi e delle start-up
- sanzioni: multe fino al 6% del fatturato annuale e fino al 5% dei ricavi medi quotidiani per ogni giorno di ritardo nell'applicazione delle contromisure richieste

DIGITAL MARKETS ACT

(Regolamento UE sui mercati digitali)

(Regolamento UE 2022/2065)

- entrato in vigore il 17 febbraio 2024, insieme al DSA
- “un testo innovativo e tanto atteso per garantire una concorrenza leale nei mercati digitali” (presidenza francese del Consiglio europeo)
- attualmente, la posizione di poche grandi piattaforme nel mercato digitale provoca: (i) debole contendibilità dei mercati delle piattaforme, (ii) debile concorrenza, (iii) pratiche commerciali sleali che arrecano danno agli utenti

I gatekeeper del mercato digitale sono i **fornitori di servizi di piattaforma di base**: social network, browser, motori di ricerca, servizi di messaggistica o social media

I gatekeeper del mercato digitale sono i **fornitori di servizi di piattaforma di base**: social network, browser, motori di ricerca, servizi di messaggistica o social media, con le seguenti caratteristiche:

- oltre 45 milioni di utenti finali attivi al mese
- un fatturato di oltre 7,5 mld di € negli ultimi tre esercizi finanziari

Obiettivi:

- garantire l'**assenza di barriere di ingresso** (contestability) di tutti i servizi online,
- **combattere gli abusi di mercato** delle grandi piattaforme digitali,
- **stimolare l'innovazione e la concorrenza** dei mercati digitali,
- sopperire al vuoto normativo che mette a **repentaglio i dati** degli utenti e la loro privacy,
- creare uno **spazio economico più equo** per le imprese europee,
- favorire la **suddivisione di valori e utili** tra le imprese che operano nell'economia digitale,
- avviare **presupposti competitivi ed equi** per chi opera nei settori informatico e tecnologico,
- offrire **maggior possibilità di scelta** ai cittadini europei

Per superare questi limiti e agevolare la concorrenza, il Digital Markets Act introduce l'utilizzo di:

- **blacklist**, con divieti e restrizioni per evitare pratiche sleali;
- **whitelist**, con nuovi obblighi per le aziende;
- **case by case assessment**, ovvero valutazioni da applicare caso per caso alle grandi piattaforme

Tra le pratiche sanzionabili, incluse nella blacklist:

- **il leveraging**, cioè lo sfruttamento della propria posizione dominante per monopolizzare nuovi mercati, attraverso l'imposizione di commissioni elevate o la limitazione forzata dell'accesso a servizi e prodotti online;
- **il self preferencing**, cioè il favorire arbitrariamente i propri prodotti sulla piattaforma a discapito di quelli proposti da altre società;
- **il rifiuto di accesso ai dati dell'utenza a terze parti terze**, previa autorizzazione dell'utente stesso;
- **l'obbligo di termini e condizioni che bloccano l'accesso a determinate funzionalità**;

- **le pratiche di vincolo (tying) e aggregazione (bundling)**, come la vendita o l'offerta congiunta e ingiustificata di beni/servizi diversi;
- **l'imposizione di termini e condizioni poco chiare**, come raccolta ingiustificata dei dati degli utenti finali;
- **la limitazione o il rifiuto della portabilità dei dati o del riutilizzo dei dati**, per scoraggiare o impedire all'utente l'abbandono della piattaforma;
- **il rifiuto immotivato di soluzioni di interoperabilità** per rendere più difficile cambiare piattaforma;
- **la combinazione di dati personali dell'utente**, ricavati dai servizi di piattaforma, con altri dati personali ricavati da altri servizi, anche di terze parti, senza espressa autorizzazione dell'utente stesso

I gatekeeper non potranno, per esempio:

- promuovere eccessivamente i propri prodotti
- imporre il proprio metodo di pagamento come unica possibilità
- riutilizzare i dati personali raccolti per un servizio ai fini di un altro servizio
- imporre condizioni inique e limitazioni agli utenti commerciali
- preinstallare determinate applicazioni software

I gatekeeper non potranno, per esempio:

- promuovere eccessivamente i propri prodotti
- imporre il proprio metodo di pagamento come unica possibilità
- riutilizzare i dati personali raccolti per un servizio ai fini di un altro servizio
- imporre condizioni inique e limitazioni agli utenti commerciali
- preinstallare determinate applicazioni software

Sanzioni:

- fino al 10% del fatturato e fino al 20% in caso di recidiva
- per violazioni di minore importanza (es. non collaborare durante i procedimenti istruttori e di indagine): ammenda fino all'1% del fatturato

promuovere eccessivamente i propri prodotti

- in caso di violazione sistematica delle norme: sanzioni straordinarie, fino all'obbligo di cedere parte del capitale o delle proprietà aziendali

COOKIE

Linee guida sull'utilizzo di cookie e di altri strumenti di tracciamento



GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI



Cosa sono i cookie, a cosa servono e perché riguardano la nostra privacy?

I **cookie** sono piccoli file di testo che i siti visitati dagli utenti inviano ai dispositivi usati per la consultazione (computer, smartphone, tablet, smart TV, ecc.) per essere memorizzati e poi ritrasmessi agli stessi siti in occasione della visita successiva.

I cookie **semplificano e velocizzano gli accessi** ai siti web da parte degli utenti, in quanto memorizzano alcune informazioni relative agli stessi che non debbono più essere reperite ed elaborate dai dispositivi dopo il primo accesso. I cookie inoltre **semplificano la fruizione** di alcuni servizi web: infatti, possono ad esempio essere impiegati per tenere traccia degli articoli in un carrello degli acquisti online o delle informazioni utilizzate per la compilazione di un modulo informatico.

Tuttavia, i cookie sono molto utili anche ai soggetti che gestiscono i siti web, perché **consentono la raccolta e il trattamento di vari dati personali** (es: indirizzo IP, nome utente, identificativo univoco o indirizzo e-mail) e **dati non personali** (come le impostazioni della lingua o informazioni sul tipo di dispositivo che una persona sta utilizzando per navigare nel sito): informazioni che possono essere utilizzate a fini di marketing e di profilazione, e condivise eventualmente anche con terze parti.

Le nuove Linee guida del Garante



Lo scorso giugno il Garante ha approvato nuove Linee guida in materia di Cookie e altri strumenti di tracciamento tenendo conto:

- 1) del **quadro giuridico di riferimento**, soprattutto a seguito dell'introduzione del Regolamento 2016/679 (GDPR);
- 2) della **rapida e continua innovazione tecnica e tecnologica** delle reti e degli strumenti;
- 3) dell'**evoluzione del comportamento degli utenti**, che utilizzano sempre più spesso servizi (web, social media, app, ecc.) e strumenti plurimi (computer, tablet, smartphone, smart TV, ecc.), con il conseguente moltiplicarsi delle possibilità di raccolta e incrocio dei dati ad essi riferiti.

Gli **elementi chiave delle nuove Linee guida** sono:

- Promozione dell'accountability;
- Offerta agli utenti di informative trasparenti e chiare;
- Rafforzamento del meccanismo del consenso;
- Rispetto dei principi di privacy by design e by default.

Le nuove Linee guida, inoltre, estendono il loro ambito di applicazione oltre che ai cookie anche ad **altri strumenti di tracciamento**, come ad esempio il **fingerprinting**.

**Le indicazioni contenute
nelle linee guida
diventano operative dal
9 GENNAIO 2022**