Elementi di cultura aziendale, professionale, giuridica e sociale

Università di Genova - a.a. 2024/2025

Lezione 1

La normativa europea in materia digitale

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

Mi presento

Manuela Bianchi

Avvocata, Data Protection Officer, Insegnante, Autrice

Data Lawyer
Data Protection Officer

Programma del corso

- La normativa europea in materia digitale
- Com’è fatta un’azienda
- Licenze software
- CTO, CISO, COO, AdS etc.
- Diversità e inclusione in azienda

Esami

Frequentanti (almeno 4 lezioni su 5)

Presentazione di un progetto di gruppo (minimo 3, max 5 persone) su un argomento precedentemente concordato nel mese di maggio

Non frequentanti

Test di 10 domande da svolgere in uno degli appelli delle sessioni regolari. Gli argomenti saranno tutti quelli trattati nel corso. Il materiale (slide) sarà messo a disposizione su Aulaweb al termine di ogni lezione

Oggi parliamo di:

- Regolamento europeo sul trattamento dei dati personali (GDPR)
- Artificial Intelligence Act
- Digital Services Act
- Digital Markets Act
- Data Governance Act
- Cookie

Che cos’è la privacy?

The right to be left alone

(Samuel Warren e Louis Brandeis, The right to privacy, Harvard Law Review, 1890)

Europa:

L’esperienza dei regimi totalitari tra le due guerre mondiali, quando venne meno la libertà di esprimere il proprio pensiero e di riunirsi, ha comportato la scrittura di costituzioni che tutelano la riservatezza della vita familiare, del domicilio e delle comunicazioni

Art. 15 Costituzione italiana:

La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili

Sentenza Corte costituzionale tedesca 209/1983:

Sancisce il diritto all'autodeterminazione informativa, definibile come il diritto del singolo a decidere in prima persona sulla cessione e l'uso dei dati che lo riguardano

Sentenza Corte costituzionale tedesca 209/1983:

È una decisione che rispecchia i tempi, aderendo alle esigenze della Information Society di cui il dato costituisce il carburante essenziale. I concetti di privacy e di data protection iniziano a confluire, sebbene non siano sinonimi e tutelino diritti differenti

Art. 7 CEDU

Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni (privacy)

Art. 8 CEDU

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

(Data protection)

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
- garantisce il libero flusso dei dati personali all'interno della UE
- 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 garantiti dalla Carta Europea dei diritti dell'Uomo (artt. 7 e 8)

Elementi rilevanti del GDPR

- 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
- la protezione dei dati garantita dal GDPR viaggia al di fuori della UE, garantendo una maggiore tutela ai soggetti che si trovano all’interno dello SSE

Artificial Intelligence Act

(Regolamento Europeo n. 2024/1689, approvato dal Parlamento europeo il 13/3/2024 e dal Consiglio d'Europa il 21/5/2024, data di effettiva adozione)

(Entrato in vigore l'1/8/2024, pienamente applicabile dall'1/8/2026, tranne alcuni obblighi operativi dal 2/2/2025)

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, promuovendo lo sviluppo e l'adozione di una AI antropocentrica, affidabile e conforme ai valori europei
- predisporre una governance efficace che garantisca l'applicazione della normativa esistente in materia di diritti fondamentali e sicurezza ai sistemi di IA

Soggetti coinvolti

- Fornitori: responsabili dello sviluppo e della messa sul mercato dei sistemi di IA, indipendentemente dalla loro ubicazione geografica, devono garantirne la tracciabilità, la certificazione, la registrazione in database europei e la conformità agli standard di sicurezza

- Deployer: soggetti che utilizzano i sistemi di IA nell'UE, con obblighi di monitoraggio costante delle performance e di segnalazione di eventuali anomali o malfunzionamenti

- Importatori e Distributori: devono garantire la conformità dei sistemi di IA che introducono nel mercato europeo

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

- inaccettabile (IA vietata)
- alto rischio: per casi d'uso in settori specifici (es. sanità, lavoro, credito) vengono introdotti requisiti di conformità dei sistemi, inclusa la documentazione tecnica e il monitoraggio
- rischio minimo: obblighi di trasparenza (es. chatbot che deve dichiarare la sua natura non umana)

APPLICAZIONI DI IA PROIBITE

- tecniche subliminali e sfruttamento di vulnerabilità (es. servizio di streaming che inserisce messaggi subliminali nei video o nei film)

- social scoring (es. il sistema utilizzato in Cina che assegna punteggi sociali ai cittadini in base al loro comportamento, limitando l'accesso a servizi come la richiesta del passaporto o la frequenza di determinati istituti scolastici)

- giustizia predittiva (es. il software COMPAS, usato negli USA per valutare la probabilità di recidiva basandosi su fattori esterni come amicizie e quartiere di residenza, risultando discriminatorio verso le persone di colore)

APPLICAZIONI DI IA PROIBITE

- creazione di banche dati per riconoscimento facciale (es. Clearview, sanzionato dal Garante italiano e da altri Garanti europei, aveva creato una banca dati attraverso lo scraping di immagini dai social network e dalle telecamere a circuito chiuso)

- inferenza di emozioni (es. sistema di IA che analizza le espressioni del viso degli studenti durante gli esami): può essere usato in caso eccezionale per motivi sanitari e di sicurezza

APPLICAZIONI DI IA PROIBITE

- classificazioni biometriche (es. il sistema cinese IJOP - Integrated Joint Operation Platform, che identifica e traccia gli Uiguri basandosi sulle caratteristiche somatiche)

- indentificazione biometrica in tempo reale, con eccezioni relative a casi specifici (es. utilizzo di sistemi di riconoscimento facciale in spazi pubblici da parte di forze dell'ordine per riconoscere le persone dai filmati delle telecamere, in tempo reale)

APPLICAZIONI DI IA AD ALTO RISCHIO (alcuni esempi)

- IA che monitora e controlla i sistemi di frenata degli ascensori
- IA che gestisce il controllo automatico della navigazione e la prevenzione delle collisioni
- IA che gestisce i sistemi di limitazione della velocità di un giocattolo elettrico cavalcabile dai bambini
- IA che controlla le valvole di sicurezza in caldaie industriali
- IA che gestisce i sistemi di frenata delle funivie
- IA che controlla i sistemi di spegnimento automatico in caso di perdite di gas
- IA che controlla i parametri vitali in un ventilatore polmonare
- IA che gestisce i sistemi di frenata automatica di emergenza delle auto
- IA che gestisce i listemi anti-bloccaggio freni nei veicoli
- IA per il controllo automatico del traffico aereo
- IA che analizza immagini mediche per rilevare patologie critiche

APPLICAZIONI DI IA AD ALTO RISCHIO (alcuni esempi)

- Identificazione/Categorizzazione biometrica (sistema di riconoscimento facciale negli aeroporti)
- Gestione infrastrutture critiche (sistema di controllo traffico autostradale, IA per gestione rete idrica urbana o rete elettrica nazionale)
- Istruzione e Formazione (sistema di valutazione automatica per ammissione università, sistemi di monitoraggio esami online, software per valutazione automatica dei test)
- Occupazione e Lavoro (ATS - Applicant Tracking System peer screening CV, IA per valutazione performance dei dipendenti, sistema per assegnazione turni basato sui comportamenti)

APPLICAZIONI DI IA AD ALTO RISCHIO (alcuni esempi)

- Accesso Servizi essenziali (IA per valutazione eligibilità sussidi sociali, sistema di credit scoring bancario, IA per triage ospedaliero, software per calcolo premi assicurativi)
- Attività di contrasto (IA per analisi affidabilità prove in tribunale, software per valutazione rischio recidiva)
- Migrazione e Frontiere (sistema screening visti, IA per analisi rischio confini, software per esame domande di asilo)
- Giustizie e Processi democratici (IA per ricerca precedenti legali e interpretazione normativa, sistema per analisi comportamento elettorale)

OBBLIGHI DEL FORNITORE DI IA AD ALTO RISCHIO

- Sistema di gestione dei rischi lungo l'intero ciclo di vita del sistema di IA: documentazione del sistema di gestione della qualità
- Qualità dei dataset di addestramento: apposizione dei riferimenti identificativi del fornitore
- Documentazione tecnica per dimostrare la conformità: conservazione per 10 anni
- Registrazione delle operazioni: sottoporre il sistema a valutazione interna/ esterna e redigere la dichiarazione di conformità
- Trasparenza by design: etichettatura CE
- Misure di supervisione umana: registrarsi e registrare i sistemi di IA ad alto rischio nella banca dati UE
- Accuratezza, robustezza e cybersecurity: monitoraggio del sistema post immissione e adozione misure correttive; rispetto dei requisiti di accessibilità

ALCUNE INDICAZIONI PER LE IMPRESE

- Investire in competenze specifiche e governance dei dati

- Prepararsi alla compliance attraverso un'adeguata organizzazione interna

- Valutare il ruolo strategico nella catena del valore dell'IA

DIGITAL SERVICE ACT
(Regolamento UE sui servizi digitali)
(Regolamento UE 2002/2065)

- 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, promuovendo una concorrenza equa tra le piattaforme online

- promuove l’innovazione, la crescita e la competitività e facilita l’espansione delle piattaforme più piccole, delle pmi (piccole e medie imprese) 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

Il DSA si applica ai **“servizi delle società dell’informazione”,** cioè a tutti gli intermediari che offrono servizi a distanza, per via elettronica/telematica, su richiesta, solitamente retribuita, di un destinatario, per esempio:

- mercati online;
- social network;
- piattaforme di condivisione dei contenuti;
- piattaforme di viaggio online e di alloggio;
- app store;
- servizi di intermediazione (es. provider Internet e register di domini);
- servizi di cloud e hosting web;
- piattaforme di economia collaborativa

OBIETTIVI:

- **proteggere i diritti dei consumatori** garantendo loro maggiore sicurezza;
- **contrastare** la diffusione di contenuti illegali, la manipolazione delle informazioni**, la disinformazione online;**
- offrire al consumatore e agli utenti commerciali di servizi digitali scelta più ampia e costi più contenuti;
- **istituire un quadro normativo chiaro**, efficace e di immediata applicazione nell'ambito della trasparenza e della responsabilità delle piattaforme online;
- **promuovere l'innovazione e la competitività nel mercato,** facilitando l'avvio di startup e lo sviluppo delle PMI,
- fornire accesso ai mercati europei per gli utenti commerciali di servizi digitali;
- favorire **un maggiore controllo democratico** e una migliore vigilanza sulle piattaforme;
- **potenziare tracciabilità e controlli sugli operatori** commerciali nei mercati online (anche attraverso controlli casuali per verificare l'eventuale ripubblicazione di contenuti illegali)

OBBLIGHI PER LE PIATTAFORME:

Gli obblighi del regolamento sono proporzionati al tipo di servizio offerto e al numero di fruitori.

Per questo, le piattaforme intermediarie di servizi vengono suddivise in **quattro categorie:**

- intermediary services;
- hosting (es.cloud);
- online platform (es. social media)
- very large platform.

Ogni categoria comporta **obblighi specifici, da assolvere entro quattro mesi** dall'assegnazione.

OBBLIGHI PER LE PIATTAFORME:

Gli obblighi principali, comuni a tutte le tipologie, sono:

- **indicare in modo chiaro le condizioni di servizio** e i relativi requisiti;
- **fornire informazioni esplicite sulla moderazione dei contenuti e sull'uso degli algoritmi** per i sistemi di raccomandazione dei contenuti, che potranno comunque essere contestati dagli utenti;
- adottare **trasparenza nei sistemi di suggerimento e nelle pubblicità online** rivolte agli utenti;
- non utilizzare pubblicità mirata rivolta ai bambini o basata su dati sensibili degli utenti;
- **non utilizzare pratiche ingannevoli** volte a manipolare le scelte degli utenti, compresi i dark pattern;

OBBLIGHI PER LE PIATTAFORME:

- **collaborare con le autorità nazionali** se richiesto;
- **denunciare** i reati;
- creare un **meccanismo di reclamo e ricorso** e risoluzione extragiudiziale delle controversie;
- adottare **misure contro le segnalazioni e le repliche abusive**;
- **controllare le credenziali di fornitori terzi,** secondo il principio del "conosci il tuo cliente commerciale" (KYBC), anche attraverso controlli a campione.

Le piattaforme online e i motori di ricerca di grandi dimensioni, a partire da 45 milioni di utenti al mese, presentano rischi più elevati, quindi devono rispettare **obblighi più rigorosi.**

DIGITAL MARKETS ACT
(Regolamento UE sui mercati digitali)
(Regolamento UE 2002/2065)

- 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) debole 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, 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 maggiore possibilità di scelta ai cittadini europei

Per superare questi limiti e agevolare la concorrenza, il DMA 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 riuso 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

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

www.gpdp.it/cookie

Gennaio 2022

IN SINTESI

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