Digitalizzazione e Diritto del Lavoro

Luciano Imbimbo

February 14, 2025

Contents

1

Digitalizzazione e Diritto

La digitalizzazione ha trasformato profondamente la società, creando nuove sfide e opportunità legali. Per gli ingegneri, comprendere il diritto è essenziale per progettare tecnologie sicure, etiche e conformi alle normative vigenti. Questo approccio è conosciuto come **"Law by Design"**.

1.1 Perché studiare il diritto in ingegneria?

Gli ingegneri hanno un ruolo chiave nello sviluppo di tecnologie che influenzano la vita quotidiana e la società. Comprendere le norme legali permette loro di:

- **Progettare in sicurezza**: garantire che i prodotti rispettino le leggi e proteggano gli utenti.
- **Evitare rischi legali**: prevenire problemi legali che potrebbero compromettere il successo di un progetto.
- **Promuovere l'etica professionale**: contribuire a un uso responsabile della tecnologia.

1.1.1 Law by Design

Il concetto di *Law by Design* implica che il rispetto delle normative deve essere integrato **sin dalla fase di progettazione** di sistemi, prodotti e servizi. In pratica, significa adottare un approccio proattivo per incorporare regole e principi legali nel design tecnologico.
Per esempio, un team che sviluppa un dispositivo IoT per la casa intelligente progetta fin dall'inizio il sistema per rispettare il GDPR:

- I dati raccolti dai sensori (es. temperatura o video) vengono pseudonimizzati.
- L'accesso ai dati è protetto da crittografia avanzata.

- Gli utenti possono facilmente gestire i propri consensi tramite un'interfaccia intuitiva.

L'ingegneria e il diritto si intersecano sempre più frequentemente, specialmente nei seguenti ambiti:

- **Computer Ethics**: esamina le questioni morali legate all'uso dei computer e delle tecnologie digitali. Tra i temi principali: privacy, discriminazioni automatizzate e uso responsabile delle risorse digitali. Per esempio, progettare un algoritmo di selezione del personale che utilizzi un set di dati bilanciato per evitare discriminazioni di genere o razza.

- **Intelligenza Artificiale e Big Data**: la crescita di AI e Big Data pone domande critiche su discriminazioni, sorveglianza di massa, violazioni della privacy, miglioramenti nei servizi sanitari, educazione personalizzata, ecc.. Ad esempio, un'azienda sviluppa un assistente virtuale per supportare i pazienti con consulti medici. Il sistema viene progettato per spiegare chiaramente le sue decisioni (trasparenza) e per evitare di favorire un particolare gruppo di utenti.

- **Diritti Fondamentali e Principi Democratici**: gli ingegneri devono operare nel rispetto dei diritti fondamentali garantiti dalla Costituzione e dalle leggi internazionali, come la libertà personale, protezione dei dati personali, eguaglianza e non discriminazione.

- **Rule of Law (Stato di Diritto)**: lo stato di diritto garantisce l'uguaglianza davanti alla legge e limita gli abusi di potere attraverso: meccanismi di controllo indipendenti, trattamento equo e non discriminatorio.

- **Conoscere i propri diritti e doveri**: essere consapevoli dei propri obblighi e diritti legali è cruciale per operare come ingegneri, cittadini e lavoratori. Ad esempio: diritto di accesso ai propri dati personali e dovere di rispettare le norme di sicurezza nei luoghi di lavoro.

- **Tecnologie di Frontiera**: le tecnologie emergenti, come IoT, Big Data, AI, blockchain e robotica, stanno rapidamente trasformando il panorama legale e tecnico. Uno sviluppatore che implementa soluzioni IoT in ambito sanitario deve garantire la sicurezza dei dati raccolti dai dispositivi e la conformità alle normative sul trattamento dei dati sanitari.

1.2 Fonti del Diritto

Fonti del diritto Italiano

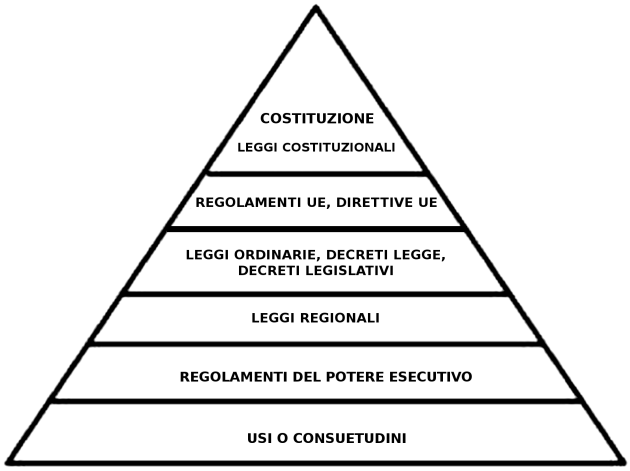

Figure 1.1: Gerarchia delle fonti del diritto italiano

Contrattazione Privata

Gli accordi tra privati assumono rilevanza legale quando regolano rapporti specifici, come:

- Un contratto per lo sviluppo di software su misura.
- Un accordo sulla manutenzione di sistemi IoT.

Sistemi Giuridici

Le regole variano a seconda del contesto nazionale o internazionale. Gli ingegneri devono tener conto delle normative locali e globali, specie in settori globalizzati come l'AI. Ogni norma ha un periodo di validità, indicato dalla sua entrata in vigore e dalla sua eventuale abrogazione. Ogni materia legale é di competenza di un'autorità legale in grado di legiferare o amministrare quella materia (es. privacy dei dati, sicurezza informatica).

Situazioni Soggettive

- **Situazioni Attive**: diritti che un soggetto può esercitare, come accesso ai propri dati personali (art. 15 GDPR) e richiesta di cancellazione dei dati (art. 17 GDPR).

- **Situazioni Passive**: obblighi a cui un soggetto è sottoposto, come rispettare le normative sulla sicurezza informatica nei progetti aziendali.

Soggetti di Diritto

- **Individui**: ogni cittadino, con diritti e doveri riconosciuti dalla legge.
- **Entità Giuridiche**: organizzazioni come aziende e associazioni, che hanno una capacità giuridica autonoma. Ad esempio, una società è responsabile legalmente per le proprie decisioni, come il rispetto della privacy dei clienti.

1.2.1 Digitalizzazione, Diritto e Regolamentazione delle Piattaforme Digitali

L'evoluzione delle tecnologie digitali richiede una regolamentazione che bilanci innovazione, competitività e rispetto dei diritti fondamentali. In questo contesto, il **Digital Services Act (DSA)** si colloca tra le normative più avanzate per garantire un ecosistema digitale sicuro, trasparente ed equo.

2

Digital Services Act

2.1 Obiettivi

Gli obbiettivi principali del DSA sono i seguenti:

- Rendere Internet più sicuro e trasparente attraverso il **Principio di equità online e offline**, ciò che è illegale offline deve esserlo anche online. Per esempio una piattaforma non può consentire la vendita di prodotti contraffatti, così come tali vendite sono vietate nei mercati fisici.
- Promuovere **innovazione e competitività** garantendo regole chiare e uniformi.
- Riduzione della frammentazione normativa tra gli Stati membri dell'UE e definizione di regole comuni per i servizi digitali, che migliorano la trasparenza per operatori e utenti.
- Prevenire contenuti illegali, disinformazione e violazioni dei diritti fondamentali, come la libertà di espressione e la protezione della dignità umana.

Il DSA si applica a servizi digitali forniti a utenti nell'UE, **indipendentemente dalla sede del fornitore**. Un'eccezione sono le microimprese e piccole imprese che godono di esenzioni per ridurre il peso degli obblighi.

2.2 Categorie di Servizi Coinvolti

- **Intermediari Online**: Hosting provider, piattaforme di e-commerce, social media.
- **Grandi Piattaforme Online (VLOP)** e **Motori di Ricerca di Grandi Dimensioni (VLOSE)**: Entità con oltre 45 milioni di utenti nell'UE.

Gli obblighi principali per VLOP e VLOSE sono i seguenti:

- Analisi e mitigazione dei rischi: identificare e mitigare rischi come contenuti illegali, disinformazione, violazione di diritti fondamentali e minacce alla sicurezza pubblica o alla dignità personale (es. violenza di genere). Facebook implementa un sistema di moderazione che utilizza AI per rilevare e rimuovere post di incitamento all'odio.
- Trasparenza nella pubblicità.
  - Gli utenti devono sapere perché vedono determinati annunci (*ad transparency*).
  - Vietato il targeting basato su **dati sensibili**, come opinioni politiche o orientamento sessuale.
- Protezione dei minori: le piattaforme non possono raccogliere dati di bambini per scopi di profilazione o pubblicità mirata.
- Meccanismi di reclamo: devono essere implementati sistemi semplici e gratuiti per contestare la rimozione ingiustificata di contenuti.
- Accesso ai dati per la ricerca: i ricercatori qualificati possono accedere ai dati delle piattaforme per studiare fenomeni come disinformazione o rischi sistemici.

2.3 Governance e Sorveglianza

- **Ruolo della Commissione Europea**
  - Monitoraggio e controllo delle grandi piattaforme.
  - Applicazione di sanzioni fino al **6% del fatturato globale** per violazioni gravi.
- **Coordinatori nazionali dei servizi digitali**: collaborano con la Commissione Europea per vigilare sull'applicazione delle norme.

2.4 Conseguenze e Sanzioni

- **Sospensione dei servizi**: le piattaforme possono bloccare utenti che violano ripetutamente le regole.
- **Sanzioni finanziarie**: multa fino al 6% del fatturato globale per violazioni sistematiche.

Per esempio, caso "X" (Ex-Twitter) nel quale c'era mancanza di trasparenza sugli account verificati e sulla pubblicità.

2.5 Confronto con altre normative

- **GDPR (General Data Protection Regulation)**: si concentra sul trattamento dei dati personali e sulla privacy.

  Collegamento: Il DSA e il GDPR condividono obiettivi comuni, come la trasparenza e la protezione degli utenti, ma il DSA copre un ambito più ampio relativo alla gestione delle piattaforme.

- **DMA (Digital Markets Act)**:
  Regola i **gatekeeper** (Google, Amazon) per garantire la concorrenza leale.

  Collegamento: Dove il DMA garantisce che i mercati digitali siano aperti e competitivi, il DSA si occupa della sicurezza e della trasparenza delle piattaforme digitali.

3

Digital Markets Act

3.1 Obiettivi Principali

Il **DMA** si propone di creare un mercato digitale più equo, eliminando le pratiche sleali delle grandi piattaforme digitali, i cosiddetti **gatekeeper**. Questa normativa, insieme al **Digital Services Act (DSA)** e al **GDPR**, forma il quadro giuridico europeo per regolare il comportamento delle piattaforme online, garantendo innovazione, concorrenza e diritti per consumatori e imprese.
Un **gatekeeper** è una piattaforma digitale con un ruolo dominante nel mercato, capace di influenzare significativamente l'accesso a utenti e imprese. Per essere identificata come gatekeeper, una piattaforma deve soddisfare tre criteri principali:

- **Posizione Economica Forte** o **Impatto significativo sul mercato interno**, operando in più paesi UE.
- **Posizione di Intermediazione**: collegare un'ampia base di utenti con numerose imprese.
- **Posizione Solida e Duratura**: detenere questa posizione stabilmente o essere in procinto di ottenerla.

I criteri specifici sono i seguenti:

- Fatturato annuo nello Spazio Economico Europeo (SEE) di almeno **6,5 miliardi di euro**.
- Capitalizzazione di mercato di almeno **65 miliardi di euro**.
- Servizio di piattaforma attivo in almeno **3 paesi UE**.
- **45 milioni di utenti finali al mese** e **10.000 utenti aziendali all'anno**.

3.2 Obblighi e Divieti per i Gatekeeper

I gatekeeper devono rispettare norme che garantiscono equità, trasparenza e concorrenza. Tra queste:

- **Interoperabilità**: consentire a terzi di collegarsi ai propri servizi. (WhatsApp deve permettere la compatibilità con altre piattaforme di messaggistica)
- **Accesso ai Dati**: consentire agli utenti aziendali di accedere ai dati generati dalla loro attività. Per esempio, un'azienda che vende su Amazon deve poter accedere ai dati relativi ai propri clienti (es. cronologia degli ordini).
- **Trasparenza nella Pubblicità**: fornire agli inserzionisti strumenti per verificare l'efficacia delle campagne. Ad esempio, Facebook deve offrire report dettagliati sull'audience raggiunta da un annuncio.
- **Libertà Contrattuale**: Consentire agli utenti aziendali di promuovere i propri servizi indipendentemente dalla piattaforma. Ad esempio, Spotify può vendere abbonamenti direttamente agli utenti, senza obbligarli a passare dall'App Store.

Per garantire una concorrenza leale, il DMA vieta ai gatekeeper di adottare comportamenti discriminatori:

- **Favoritismo**: Vietato privilegiare i propri servizi rispetto a quelli di terzi nel ranking. Google non può posizionare Google Shopping sopra altri servizi simili.
- **Restrizioni all'Uscita**: vietato impedire agli utenti di disinstallare app preinstallate. Gli utenti devono poter rimuovere le app di fabbrica dai loro smartphone.
- **Tracciamento Non Consensuale**: vietato tracciare l'attività degli utenti su altre piattaforme senza consenso esplicito. Facebook non può raccogliere dati di navigazione esterni senza autorizzazione.

Il DMA prevede sanzioni severe per i gatekeeper che non rispettano le norme:

- Multa fino al **10% del fatturato globale annuo**.
- Multa fino al **20% per violazioni ripetute**.
- **Sanzioni periodiche** fino al **5% del fatturato medio giornaliero**.
- Misure correttive, come l'obbligo di vendere parti dell'attività.

Ad esempio, se un gatekeeper come Apple continua a favorire i propri servizi nonostante gli avvertimenti, potrebbe essere multata o obbligata a separare il servizio App Store dal resto della sua attività.

3.3 Vantaggi del DMA

- Per i Consumatori: Maggiore scelta tra servizi digitali, possibilità di cambiare piattaforma facilmente e prezzi più competitivi.
- Per gli Utenti Aziendali: Accesso ai dati generati dalla piattaforma e libertà di promuovere i propri servizi senza restrizioni.
- Per le Piattaforme Non Gatekeeper

3.4 Confronto con Altre Normative

Il **DMA** si inserisce in un quadro normativo europeo ampio, distinguendosi e collaborando con altre normative:

- **GDPR (General Data Protection Regulation)**
  Mentre il GDPR si concentra sulla privacy, il DMA regola le dinamiche di mercato.
- **DSA (Digital Services Act)**
  Il DSA disciplina le responsabilità delle piattaforme, mentre il DMA regola il comportamento dei gatekeeper. Il **DMA** e il **DSA** sono complementari.
- **Direttiva sull'E-Commerce** Il DMA approfondisce e aggiorna questi obblighi per le piattaforme più grandi.

Apple, considerata un gatekeeper, ha imposto commissioni elevate (fino al 30%) agli sviluppatori di app sull'App Store. Con l'introduzione del DMA:

- **Libertà contrattuale**: Spotify può vendere abbonamenti direttamente agli utenti sul proprio sito.
- **No favoritismo**: Apple non può promuovere Apple Music rispetto a Spotify nel ranking dell'App Store.

4

GDPR

Il **Regolamento UE 2016/679**, noto come **General Data Protection Regulation (GDPR)**, è la normativa europea che regola il trattamento dei dati personali. Entrata in vigore il **24 maggio 2016** e applicabile dal **25 maggio 2018**, il GDPR ha sostituito la Direttiva 95/46/CE, introducendo un sistema uniforme di protezione dei dati nei Paesi UE.

4.1 Obiettivi del GDPR

- **Protezione uniforme dei dati personali**: garantire un alto livello di tutela dei dati in tutta l'Unione Europea.
- **Libera circolazione dei dati**: favorire l'innovazione e lo sviluppo economico eliminando barriere normative tra gli Stati membri.

4.2 Elementi Principali del GDPR

4.2.1 Ruoli e Responsabilità

Il GDPR introduce ruoli specifici per il trattamento dei dati:

- **Titolare del Trattamento**: chi decide finalità e mezzi del trattamento dei dati. Ad esempio una banca che raccoglie i dati dei clienti per aprire conti correnti.
- **Responsabile del Trattamento**: chi esegue il trattamento per conto del titolare. Per esempio, una società IT che gestisce i server per un'azienda bancaria.
- **Data Protection Officer (DPO)**: figura obbligatoria in casi specifici (es. enti pubblici o aziende che trattano dati su larga scala). A funzioni di consulenza, monitoraggio, formazione e gestione delle violazioni. Ad

esempio, un ospedale che gestisce dati sanitari nominerebbe un DPO per garantire conformità alle norme.

4.2.2 Misure di Sicurezza

La sicurezza dei dati è centrale nel GDPR. Le principali misure sono le seguenti:

1. **Data Protection by Design e by Default**.
   - **By Design**: Incorporare la protezione dei dati fin dalla progettazione di sistemi e processi. Un'app di messaggistica che utilizza cifratura end-to-end per proteggere le conversazioni.
   - **By Default**: Impostare la protezione come standard. I social network dovrebbero raccogliere solo i dati strettamente necessari per funzionare.
2. **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)**
   - Necessaria per trattamenti ad alto rischio, come profilazione o utilizzo di dati biometrici.
   - Analizza i rischi e propone misure per mitigarli.

Gli individui, definiti "interessati", hanno diritti specifici sul trattamento dei propri dati:

1. **Accesso**: Conoscere quali dati sono trattati e come.
2. **Cancellazione (diritto all'oblio)**: Richiedere la rimozione dei dati personali.
3. **Portabilità**: Trasferire i propri dati a un altro titolare in un formato strutturato.
4. **Limitazione**: Bloccare il trattamento in situazioni specifiche.

Ad esempio, un utente di un social network può chiedere una copia dei propri dati per trasferirli a un'altra piattaforma o chiederne la cancellazione in caso di cambio di servizio.

4.2.3 Gestione delle Violazioni (Data Breach)

Un **Data Breach** è una violazione di sicurezza che compromette dati personali. Può includere:

- Furto o accesso non autorizzato.
- Perdita accidentale di dati.

In caso di violazione l'azienda titolare del trattamento deve notificare l'evento all'**Autorità di Controllo** entro **72 ore** ed informare gli interessati se la violazione comporta rischi elevati. Ad esempio, un hacker accede ai dati dei clienti di un negozio online. L'azienda deve notificare il Garante per la Protezione dei Dati e avvisare i clienti, adottando misure per contenere il danno.

4.2.4 Sanzioni

Il GDPR prevede multe severe per i trasgressori: fino a **20 milioni di euro** o al **4% del fatturato globale annuo**, a seconda di quale sia più elevato.

4.2.5 Autorità di Controllo

Ogni Stato membro dispone di un'autorità nazionale per il controllo della conformità. In Italia é il **Garante per la Protezione dei Dati Personali**.

4.2.6 Certificazione e Sigilli

Il GDPR promuove l'adozione di **certificazioni** per dimostrare la conformità delle aziende. I sigilli e le certificazioni aiutano i consumatori a identificare le aziende che rispettano gli standard.

4.3 Collegamenti con Altre Normative

- **Digital Markets Act (DMA)**: Mentre il GDPR tutela i diritti individuali e i dati personali, il DMA regola la concorrenza tra piattaforme online, garantendo equità nei mercati digitali.
- **Digital Services Act (DSA)**: Regola contenuti e sicurezza online, completando la protezione dei dati fornita dal GDPR.

Queste normative europee si integrano per creare un ecosistema digitale sicuro, equo e rispettoso dei diritti degli utenti.

5

Data Act

Il **Data Act** è una normativa chiave dell'Unione Europea, inserita nella strategia europea per i dati, con l'obiettivo di regolamentare l'accesso e l'uso dei dati generati da dispositivi e oggetti connessi (**Internet of Things - IoT**). La normativa entrerà in vigore l'11 gennaio 2024, ma la sua applicabilità effettiva è prevista per settembre 2025. Questo periodo intermedio consente alle organizzazioni di prepararsi adeguatamente all'attuazione della nuova regolamentazione. La normativa si colloca in modo complementare al Data Governance Act, un altro importante strumento legislativo che è già in vigore da settembre 2023. Mentre il Data Governance Act si concentra sui meccanismi di condivisione dei dati tra diversi settori e Stati membri, il Data Act si propone di stabilire regole più specifiche sull'accesso e l'utilizzo dei dati generati da dispositivi e oggetti connessi.

5.1 Obiettivi principali

- Creare un ecosistema di dati più **equilibrato** e **trasparente**.
- Chiarire chi può **accedere**, **utilizzare** e **trarre valore** dai dati.
- Stimolare la **digitalizzazione** e l'**innovazione** nell'UE, con un focus sulla competitività globale.

Per esempio, un produttore di auto connesse non può limitare l'accesso ai dati diagnostici del veicolo solo ai propri centri assistenza. Gli utenti devono poter condividere i dati con tecnici indipendenti o altre piattaforme di servizio.

5.2 Misure Chiave del Data Act

Il Data Act garantisce **diritti di accesso** equi per produttori,utenti e terze parti. I produttori non possono imporre condizioni contrattuali o tecniche

che limitino l'accesso ai dati da parte degli utenti o di terze parti autorizzate. Ad esempio, un'azienda che produce droni agricoli deve consentire agli agricoltori di trasferire i dati dei voli a una piattaforma di analisi indipendente per migliorare la pianificazione delle colture.

Interoperabilità

Introduzione di standard tecnici per garantire che i dati possano essere **condivisi e utilizzati** senza problemi tra dispositivi e piattaforme diverse.

- Riduzione dei costi legati all'integrazione di tecnologie diverse.
- Promozione di una competizione leale tra fornitori di servizi.

Un sistema di irrigazione agricola basato su IoT può combinare dati meteorologici provenienti da sensori di terze parti per ottimizzare l'irrigazione.

5.3 Vantaggi del Data Act

Per i consumatori

- **Maggiore controllo sui dati**: Gli utenti possono trasferire i dati generati dai propri dispositivi a fornitori di servizi terzi.
- **Più scelta e concorrenza**: I consumatori non sono vincolati a utilizzare solo i servizi post-vendita dei produttori.

Un utente con un elettrodomestico connesso, come una lavatrice, può scegliere di farla riparare da un tecnico indipendente usando i dati diagnostici forniti dal dispositivo.

Per le imprese

- **Accesso ai dati per l'innovazione**: I fornitori di servizi aftermarket possono utilizzare i dati per migliorare i propri servizi e sviluppare soluzioni innovative.
- **Ottimizzazione operativa**: Le aziende possono monitorare i propri processi produttivi in tempo reale per ridurre i costi e aumentare l'efficienza.

Un'azienda manifatturiera utilizza i dati dei macchinari connessi per pianificare interventi di manutenzione preventiva, riducendo i tempi di inattività.

5.4 Impatto del Data Act

Sostenibilità e Green Deal

Il Data Act promuove la **riparazione e manutenzione** dei prodotti, contribuendo a ridurre i rifiuti elettronici e allungando la vita utile dei dispositivi. Un utente può aggiornare il software di un termostato connesso invece di sostituirlo, prolungandone l'utilizzo e riducendo i rifiuti.

Agricoltura di precisione

Gli agricoltori possono sfruttare i dati IoT per ottimizzare l'uso delle risorse come acqua e fertilizzanti, aumentando la produttività e riducendo l'impatto ambientale. Sensori IoT posizionati nel suolo raccolgono dati su umidità e nutrienti, fornendo indicazioni per un'irrigazione mirata che evita sprechi d'acqua.

PMI e Innovazione

Il Data Act favorisce l'accesso equo ai dati anche per le piccole e medie imprese, che possono così partecipare attivamente all'economia dei dati senza dover affrontare barriere insormontabili (riduzione del divario competitivo tra grandi aziende e PMI). Una PMI nel settore logistico può accedere ai dati sui flussi di traffico generati da sensori stradali per migliorare le proprie operazioni di consegna.

5.5 Conclusioni

Il **Data Act** rappresenta una svolta per l'economia digitale dell'Unione Europea, favorendo:

- **Trasparenza**: Regole chiare su chi può accedere ai dati e come possono essere utilizzati.
- **Sostenibilità**: Riduzione degli sprechi elettronici e promozione della riparabilità dei prodotti.
- **Innovazione**: Stimolo alla competitività e alla creazione di nuove soluzioni tecnologiche.

6

Data Governance Act

Il **Data Governance Act** è una normativa dell'Unione Europea concepita per promuovere l'utilizzo efficace dei dati e potenziare la fiducia nella condivisione di informazioni tra pubblico, privato e cittadini. Fa parte della più ampia strategia europea volta a creare un **mercato unico dei dati**, garantendo che questi siano utilizzati in modo trasparente, sicuro e nel rispetto dei diritti fondamentali.

6.1 Obiettivi principali

- **Facilitare il riutilizzo dei dati pubblici** protetti, ad esempio dati personali o segreti commerciali.
- **Regolare gli intermediari dei dati** per migliorare la trasparenza e la fiducia tra fornitori e utenti.
- **Incentivare il data altruism**: la condivisione volontaria di dati per finalità di interesse generale.

Dati sanitari protetti possono essere condivisi, in forma anonimizzata, con istituti di ricerca per sviluppare trattamenti innovativi per malattie rare. In questo modo si promuove il progresso medico senza compromettere la privacy dei cittadini.
Il riutilizzo dei dati detenuti dal settore pubblico è regolamentato in modo rigoroso per proteggere interessi come:

- **Riservatezza commerciale** (es. segreti industriali).
- **Proprietà intellettuale** (es. brevetti).
- **Protezione dei dati personali** (es. dati sensibili relativi alla salute).

I ruoli degli enti pubblici sono i seguenti:

- **Facilitare il consenso** dei soggetti interessati, quando necessario.
- **Fornire consulenza** sulle normative di protezione dei dati.
- **Creare ambienti sicuri** per il trattamento dei dati protetti (ad esempio sandbox digitali).

Per esempio, un'università che intende utilizzare dati statistici relativi a un censimento nazionale deve essere supportata dalle autorità pubbliche per accedere ai dati in conformità con le normative sulla privacy.

6.2 Open Data Directive e Principio FAIR

La **Open Data Directive**, strettamente legata al DGA, stabilisce che i dati pubblici e quelli finanziati con fondi pubblici devono essere accessibili e utilizzabili in linea con il principio **FAIR**:

- **Findable** (rintracciabili).
- **Accessible** (accessibili).
- **Interoperable** (interoperabili).
- **Reusable** (riutilizzabili).

Inoltre, la direttiva identifica dati di rilevanza strategica, che devono essere resi disponibili in formato aperto, come:

- Dati geografici.
- Statistiche.
- Informazioni meteo.
- Dati legali.
- Dati aziendali.
- Informazioni sui trasporti.

Ad esempio, una banca dati contenente informazioni geografiche viene resa disponibile tramite API per supportare la pianificazione di infrastrutture, come nuove reti di trasporto pubblico.

6.2.1 Intermediari per i Dati

Gli **intermediari per i dati** svolgono un ruolo cruciale nel garantire la condivisione sicura e trasparente dei dati tra diversi attori (pubblico, privato, ricerca). Questi intermediari non possono utilizzare i dati per scopi propri (es. commerciali) e devono garantire la neutralità nei confronti dei fornitori e degli utenti dei dati.
Ad esempio, un servizio intermedio consente a un'azienda di logistica di condividere i dati sulle rotte di trasporto con enti di ricerca per ottimizzare le infrastrutture urbane, garantendo al contempo che tali dati non siano venduti a terzi per fini commerciali.

6.2.2 Altruismo per i Dati

Il **data altruism** promuove la condivisione volontaria dei dati da parte di individui e organizzazioni per scopi di interesse generale, senza alcun compenso economico diretto. Le finalitá principali sono le seguenti:

- **Salute pubblica** (es. ricerca su nuove terapie).
- **Lotta al cambiamento climatico** (es. monitoraggio ambientale).
- **Miglioramento della mobilità** (es. sviluppo di reti di trasporto intelligenti).

6.2.3 Interoperabilità

Per garantire la **condivisione fluida** dei dati tra sistemi diversi, il DGA promuove lo sviluppo di **spazi europei dei dati** in settori chiave, tra cui:

- **Sanità**: lo **European Health Data Space (EHDS)** facilita l'accesso a dati sanitari in tutta l'UE, migliorando l'efficienza dei trattamenti medici.
- **Trasporti**: piattaforme interoperabili migliorano la gestione dei flussi logistici.

Ad esempio, Uun sistema interoperabile consente a un ospedale tedesco di accedere ai dati clinici di un paziente italiano per fornire cure tempestive in caso di emergenza.

6.3 Collegamenti con il Data Act

Il **Data Governance Act** e il **Data Act** sono complementari nella strategia europea per i dati:

- **DGA**: si concentra sui **meccanismi di condivisione dei dati** (fiducia, intermediari, riutilizzo).

- **Data Act**: regola **chi può accedere** ai dati e come possono essere utilizzati per generare valore.

Nel contesto di un progetto di agricoltura di precisione, il DGA facilita la condivisione di dati meteorologici tra enti pubblici e privati, mentre il Data Act definisce i diritti di accesso ai dati generati dai dispositivi IoT usati dagli agricoltori.
In conclusione, il **Data Governance Act** rappresenta un elemento essenziale nella costruzione di un'economia basata sui dati, con implicazioni rilevanti nei seguenti campi:

- **Ricerca e innovazione**: accesso sicuro e regolamentato a dati sensibili.
- **Sviluppo sostenibile**: strumenti per affrontare le sfide globali, come il cambiamento climatico.
- **Competitività**: promozione di un mercato unico dei dati, inclusivo e trasparente. Grazie alla complementarità con il Data Act, l'UE mira a creare un ecosistema digitale capace di bilanciare innovazione e protezione dei diritti fondamentali.

7

Direttiva NIS2

La **Direttiva NIS2**, entrata in vigore nell'Unione Europea, mira a rafforzare la **cybersicurezza** e a garantire la resilienza delle reti e dei sistemi informativi critici, fondamentali per la società e l'economia. Questa direttiva sostituisce la precedente NIS, ampliandone il campo di applicazione e introducendo nuovi requisiti per affrontare le minacce emergenti.

7.1 Obiettivi principali

- **Migliorare la sicurezza delle reti e dei sistemi informativi** nell'intera Unione Europea.
- **Prevenire e mitigare i rischi di cybersecurity** attraverso misure proattive.
- **Promuovere standard internazionali**, come la ISO/IEC 27001, per uniformare le pratiche di sicurezza.

Un'azienda energetica utilizza sistemi crittografici avanzati per proteggere i dati sensibili dei sensori nelle sue centrali elettriche, riducendo il rischio di attacchi informatici che potrebbero compromettere la continuità del servizio.

7.1.1 Requisiti fondamentali (Art. 18)

Le aziende devono adottare una serie di misure obbligatorie, tra cui:

- **Sicurezza della supply chain**: proteggere i fornitori e i processi esterni da vulnerabilità (ad esempio, evitare che malware entri attraverso software forniti da terze parti).
- **Crittografia e cifratura**: assicurare che i dati sensibili siano protetti sia durante la trasmissione che nell'archiviazione.
- **Segnalazione di incidenti**: notificare rapidamente incidenti significativi alle autorità competenti, garantendo una risposta tempestiva.

7.1.2 Igiene digitale (Art. 89)

La direttiva sottolinea l'importanza dell'**igiene digitale**, ovvero pratiche di base per prevenire rischi informatici. Tra queste:

- **Aggiornamenti regolari** dei software.
- **Utilizzo di password forti** e autenticazione a più fattori.
- **Creazione di reti di risposta alle crisi** come l'**EU-CyCLONe (European Cyber Crisis Liaison Organization Network)** per coordinare le risposte agli attacchi su larga scala.

Un ente pubblico mantiene aggiornati i firewall e utilizza un sistema di autenticazione multifattoriale per accedere ai dati sensibili, riducendo i rischi di attacchi ransomware.

7.2 Decreto Legislativo n. 138/2024

Questo decreto recepisce la Direttiva NIS2 nell'ordinamento italiano, definendo il quadro normativo nazionale per la cybersicurezza.

- **Cybersicurezza**: misure per proteggere reti, sistemi e dati da attacchi informatici.
- **Incidenti di sicurezza**: eventi che compromettono la riservatezza, l'integrità o la disponibilità di dati o servizi critici.
- **Quasi-incidenti**: situazioni potenzialmente pericolose che, grazie a interventi tempestivi, non si concretizzano in danni.

7.3 EU Digital Acts

Gli atti digitali europei, tra cui la Direttiva sul Commercio Elettronico e il Regolamento P2B, regolano il funzionamento delle piattaforme digitali e le loro relazioni con utenti e fornitori.

7.3.1 Direttiva sul Commercio Elettronico

Questa direttiva regola:

- **Libertà di stabilimento** e fornitura di servizi digitali nell'UE.
- **Responsabilità degli intermediari online**, distinguendo tra:
    1. **Hosting passivo**: piattaforme che memorizzano contenuti senza intervento attivo (es. Dropbox) e che non sono responsabili per il contenuto degli utenti.

2. **Hosting attivo**: piattaforme che moderano o organizzano attivamente i contenuti (es. Amazon) e che possono essere ritenute responsabili per violazioni, come contenuti fraudolenti.

Una piattaforma di e-commerce che promuove specifici prodotti tramite algoritmi è responsabile per eventuali truffe legate a questi articoli.

7.3.2 Regolamento P2B (Platform-to-Business)

Il regolamento garantisce maggiore **trasparenza e correttezza** nei rapporti tra piattaforme e fornitori di servizi o prodotti.

- Introduce obblighi per spiegare i criteri di **ranking** (ad esempio, come sono classificati i prodotti nei risultati di ricerca).
- Stabilisce procedure per la gestione dei reclami da parte degli utenti commerciali.

Un fornitore commerciale può contestare una posizione svantaggiosa nel ranking su una piattaforma di prenotazioni alberghiere e richiedere una revisione trasparente.

7.4 Integrazione con GDPR e Data Governance Act

- **Direttiva NIS2 e GDPR**: Entrambe mirano a garantire sicurezza e protezione, ma la NIS2 si concentra sulla resilienza delle infrastrutture digitali, mentre il GDPR tutela i dati personali.
- **NIS2 e DGA**: La sicurezza promossa dalla NIS2 è essenziale per costruire la fiducia necessaria alla condivisione dei dati regolata dal DGA.
- **Digital Acts e GDPR**: Gli atti digitali si integrano con il GDPR, garantendo che la trasparenza e la responsabilità delle piattaforme rispettino i diritti degli utenti.

8

EU Chips Act

La crisi della pandemia da COVID-19 e la guerra in Ucraina hanno evidenziato l'**estrema dipendenza dell'UE dalle importazioni** di semiconduttori, principalmente da Paesi extra-UE come Taiwan, leader globale grazie a **Taiwan Semiconductor Manufacturing Company (TSMC)**. Questi eventi hanno esacerbato la carenza di chip, causando ritardi nella produzione di beni essenziali e dimostrato la vulnerabilità delle catene globali di approvvigionamento. Difatti nel 2021, la carenza di semiconduttori ha rallentato la produzione di automobili e dispositivi elettronici, come smartphone e console di gioco, portando a un aumento dei prezzi per consumatori e aziende.

8.1 Obiettivi principali

L'EU Chips Act si pone tre obiettivi fondamentali:

- **Affrontare la carenza di semiconduttori** attraverso investimenti mirati e strategie di lungo periodo.
- **Rafforzare la leadership tecnologica europea**, puntando su innovazione e competitività nel settore.
- **Preparare l'UE a future interruzioni** delle supply chain, costruendo una base industriale solida e resiliente.

Questi obiettivi sono parte di una visione più ampia di **autonomia strategica** dell'UE, che mira a ridurre la dipendenza da fornitori esterni in settori critici.

8.2 Modalità di intervento dell'UE

8.2.1 2.1 Chips for Europe e Orizzonte Europa

Il programma **Chips for Europe**, parte del piano **Orizzonte Europa**, concentra gli sforzi su:

- **Promozione dell'innovazione**: Investimenti in ricerca e sviluppo (R&S) per migliorare la capacità tecnologica.
- **Finanziamenti pubblici e privati**: Un totale di **43 miliardi di euro entro il 2030**, destinati a progetti di innovazione, infrastrutture e formazione.

8.2.2 Coordinamento

L'UE ha istituito un meccanismo di **coordinamento** guidato dal **Consiglio Europeo**, coinvolgendo Stati membri, Commissione Europea e stakeholder del settore per:

- Evitare duplicazioni di sforzi.
- Garantire un flusso di informazioni tra i vari attori.
- Prevenire interruzioni della supply chain.

Una piattaforma di coordinamento UE evita che un evento imprevisto, come il blocco del **Canale di Suez**, interrompa la distribuzione dei semiconduttori a livello continentale.

8.3 Iniziative chiave del Chips for Europe

8.3.1 Piattaforma di progettazione

La piattaforma di progettazione è un **ambiente virtuale basato su cloud** che consente:

- **Collaborazione tra aziende, università e centri di ricerca**.
- Accesso aperto e trasparente a strumenti di progettazione avanzati.
- Sviluppo di semiconduttori innovativi, riducendo i costi di ricerca.

8.3.2 Linee pilota

Le linee pilota sono strutture di sviluppo per testare e produrre chip su **scala ridotta**, promuovendo innovazione tecnologica. Si concentrano su tre aree strategiche:

1. **Sviluppo sub-2 nm**: Miniaturizzazione estrema dei semiconduttori.
2. **Tecnologia FD-SOI a 10 nm e inferiori**: Soluzioni per dispositivi a basso consumo.
3. **Integrazione eterogenea**: Combina più tecnologie in un unico chip.

8.3.3 Chip quantistici

Il Chips Act promuove lo sviluppo di semiconduttori **basati su principi quantistici**, essenziali per:

- Crittografia avanzata.
- Simulazioni molecolari.
- Calcolo ad alte prestazioni.

8.4 Centri di competenza

I **27 centri di competenza** sparsi nell'UE forniscono:

- **Accesso a infrastrutture avanzate** per la progettazione e il testing.
- **Formazione tecnica specializzata** per ingegneri e ricercatori.
- Supporto alle PMI per entrare nel mercato dei semiconduttori.

8.5 Fondo Chips

Il **Fondo Chips** facilita l'**accesso ai finanziamenti** per PMI, start-up e scale-up, offrendo:

1. **Fondi misti** tramite il programma **InvestEU** e il **Consiglio Europeo per l'Innovazione**.
2. **Supporto finanziario** per progetti ad alto potenziale tecnologico.

Una start-up olandese ottiene un finanziamento dal Fondo Chips per sviluppare microprocessori ottimizzati per l'intelligenza artificiale.

8.6 Collegamenti con altre normative

- **Direttiva NIS2**: La sicurezza dei semiconduttori è cruciale anche per proteggere le infrastrutture critiche digitali, in linea con le misure di resilienza promosse dalla NIS2.
- **GDPR e DGA**: I semiconduttori avanzati, come quelli quantistici, sono essenziali per garantire la privacy e la condivisione sicura dei dati.

9

AI ACT

Il **Regolamento sull'Intelligenza Artificiale (AI Act)**, proposto dall'Unione Europea, mira a stabilire regole per garantire l'uso etico e sicuro dei sistemi IA. Classifica tali sistemi in base al livello di rischio.

- **Rischio inaccettabile**: Sistemi vietati perché pericolosi o manipolativi.
- **Rischio alto**: Regolati con obblighi stringenti (predizioni sanitarie e creditizie)
- **Rischio limitato**: Richiedono trasparenza minima (es. chatbot).
- **Rischio minimo**: Nessuna regolamentazione specifica (es. filtri antispam).

9.1 Sistemi Vietati

- Sistemi che utilizzano tecniche subliminali, manipolative o ingannevoli per distorcere il comportamento
- Sistemi che sfruttano le vulnerabilitá legate all'etá, alla disabilitá o alle condizioni socioeconomiche
- Sistemi di categorizzazione biometrica che deducono attributi sensibili (ad eccezzioni di filtraggio per sicurezza pubblica)
- Social scoring, valutazione di individui o gruppi in bas al comportamento sociale o a tratti personali
- Sistemi per valutare il rischio che un individuo commetta reati basandosi esclusivamente sul profilo o sui tratti della personalitá
- Sistemi per la compilazione di database di riconoscimento facciale attraverso lo scarping non mirato di immagini facciali da Internet

- Sistemi per dedurre le emozioni nei luoghi di lavoro o negli istituti scolastici
- Sistemi per l'identificazione biometrica remota in tempo reale.

Un sistema IA che discrimina basandosi sull'etnia viola i principi fondamentali dell'AI Act.

9.2 Sistemi di AI ad Alto Rischio

Sistemi utilizzati come componenti di sicurezza o prodotti tenuti a sottoporsi ad una valutazione di conformitá da parte di terzi. Tra questi:

- Sistemi che eseguono compiti procedurali limitati
- Sistemi che migliorano il risultato di un'attivitá umana precedentemente completata
- Modelli decisionali che non contrastano con la valutazione umana precedentemente completata

I sistemi di IA sono sempre considerati ad alto rischio se tracciano profili di persone riguardante i seguenti ambiti: rendimento lavorativo, saluti, preferenze, interessi, comportamento e situazione economica.

9.2.1 Obblighi

- Stabilire un sistema di fgestione del rischio
- Condurre la governance dei dati
- Redigere la documentazione tecnica per dimostrare la conformitá e fornire alle autoritá le informazioni necessarie per valutare tale conformitá
- Fornire le istruzioni per l'uso
- Consentire ai distributori di implementare la supervisione umana
- Progettare per raggiungere adeguati livelli di accuratezza, robustezza e sicurezza informatica
- Stabilire un sistema di gestione della qualitá

Un software IA utilizzato per selezionare CV deve essere trasparente e non discriminatorio nei confronti di genere, etnia o età. Un altro esempio é la legalIA, cioé sistemi utilizzati per valutare il rischio di diventare vittima di un crimine e valutare procedimenti penali.

9.3 4. Intelligenza Artificiale Generale (GPAI)

Sistemi IA avanzati utilizzabili in molteplici contesti (es. GPT-4). I sistemi GPAI possono essere utilizzati come sistemi di IA ad alto rischio o integrati in essi.
Tutti i fornitori di modelli GPAI devoo fornire la documentazione tecnica, le istruzioni per l'uso, rispettare la direttiva sul copyright e pubblicare una sintesi dei contenuti. Devono inoltre, condurre valutazione dei modelli, test avversari, tracciare e segnalare gli incidenti gravi e garantire le protezioni di cybersecurity.

10

IP Law

La proprietà intellettuale (PI) è un insieme di diritti che consente ai titolari di proteggere le proprie invenzioni, creazioni e idee innovative, impedendo ad altri di sfruttarle senza autorizzazione. Questo ambito legale si estende su diverse categorie, come brevetti, marchi, diritti d'autore, segreti commerciali e design. Ogni categoria risponde a specifiche esigenze di tutela e offre un quadro normativo che varia dal livello nazionale a quello internazionale.

10.1 Che cos'è la Proprietà Intellettuale?

La PI rappresenta un diritto assoluto che garantisce ai creatori il monopolio sull'utilizzo, la riproduzione o la commercializzazione delle loro invenzioni o opere. Si tratta di una forma di proprietà intangibile che comprende elementi come:

- Brevetti (patents): proteggono innovazioni tecniche per un massimo di 20 anni.
- Marchi (trademarks): identificano e distinguono prodotti o servizi attraverso simboli, parole o segni grafici.
- Diritti d'autore (copyright): offrono tutela a opere creative come software, musica, immagini e testi.
- Segreti commerciali (trade secrets): coprono informazioni preziose mantenute riservate, come formule o processi industriali.
- Disegni industriali (design): proteggono l'aspetto estetico di un prodotto.

10.2 Perché è importante la Protezione della PI?

La protezione della PI svolge un ruolo cruciale nello stimolare l'innovazione tecnologica e nel garantire che gli investimenti in ricerca e sviluppo siano

adeguatamente ricompensati. Senza un sistema di protezione efficace, gli innovatori potrebbero essere scoraggiati dal creare nuovi prodotti, poiché i concorrenti potrebbero sfruttare le loro idee senza costi. Inoltre, la PI contribuisce a:

- Garantire la qualità dei prodotti.
- Aumentare il valore di mercato delle invenzioni.
- Facilitare l'attrazione di investimenti e finanziamenti.
- Promuovere la concorrenza e il trasferimento tecnologico.

10.3 Le Diverse Tipologie di Protezione

Un aspetto interessante della PI è la varietà degli strumenti disponibili. Ogni tipo di diritto si applica a situazioni specifiche:

Brevetti

I brevetti proteggono invenzioni tecniche nuove, inventive e applicabili industrialmente. Sono concessi dopo una procedura rigorosa che include l'esame della novità e dell'inventività. In Italia, è possibile richiedere brevetti attraverso l'Ufficio Italiano Brevetti e Marchi (UIBM), mentre a livello europeo ci si può rivolgere all'Ufficio Europeo dei Brevetti (EPO). Un brevetto europeo, ad esempio, può coprire fino a 42 Stati membri con una sola domanda.

Marchi

I marchi servono a identificare prodotti o servizi. La loro registrazione può essere effettuata a livello nazionale, europeo (Marchio dell'Unione Europea) o internazionale (attraverso l'Organizzazione Mondiale della Proprietà Intellettuale, WIPO). Essi possono essere rinnovati ogni 10 anni, rendendoli una forma di protezione potenzialmente perpetua.

Diritti d'Autore

Questi diritti nascono automaticamente con la creazione di un'opera e proteggono produzioni originali come opere letterarie, artistiche, software e altre espressioni creative. La protezione include sia diritti economici (licenze e sfruttamento) sia diritti morali (riconoscimento dell'autore).

Segreti Commerciali

I segreti industriali proteggono informazioni riservate che hanno valore commerciale, come formule o processi di produzione. La protezione è garantita fino a quando l'informazione rimane segreta.

Disegni Industriali

Il design protegge l'aspetto esteriore di un prodotto. Un disegno registrato può essere tutelato fino a 25 anni, mentre un design non registrato è protetto per un massimo di 3 anni.

10.4 Sfide e Considerazioni

Nonostante i benefici, la protezione della PI presenta alcune sfide significative. I costi di registrazione e mantenimento possono essere elevati, e i procedimenti legali per far valere i diritti possono essere complessi e costosi. Inoltre, esistono alternative alla registrazione, come mantenere il segreto sulle proprie invenzioni o pubblicarle per impedirne il brevetto da parte di altri. Tuttavia, queste soluzioni offrono una protezione limitata rispetto ai diritti esclusivi garantiti da brevetti o marchi.

10.5 Il Tribunale Unificato dei Brevetti

Dal 2024, Milano ospiterà una divisione del Tribunale Unificato dei Brevetti, che gestirà controversie relative a brevetti europei classici e unitari. Questo tribunale rappresenta un passo avanti nella creazione di un sistema più uniforme e specializzato per la risoluzione delle dispute in materia di PI in Europa.

11

Tipologie di Lavoro

11.1 Lavoro Subordinato

Il lavoratore opera sotto la **direzione e controllo** di un datore di lavoro, con obblighi precisi e orari stabiliti, in cambio di una **retribuzione**.

- Rapporto di subordinazione gerarchica.
- Retribuzione regolare secondo quanto previsto dal Contratto Collettivo Nazionale di Lavoro (CCNL).
- Tutela previdenziale (malattia, ferie, maternità, ecc.).

11.1.1 Contratto a Tempo Indeterminato

È la forma contrattuale standard nel diritto del lavoro italiano, che garantisce **stabilità occupazionale**.

- Periodo di prova: massimo **6 mesi**.
- Obbligo di preavviso in caso di dimissioni o licenziamento, secondo il CCNL applicabile.
- Tutele per il lavoratore: malattia, maternità, disoccupazione, ecc.

11.1.2 Contratto a Tempo Determinato

Prevede una durata **limitata**, con scadenza definita al momento della stipula.

- Durata massima: **12 mesi** (estendibile a **24 mesi** in specifici casi).
- Limitazioni: non può essere usato per sostituire lavoratori in sciopero o in unità con recenti licenziamenti collettivi.
- **Diritto di precedenza**: il lavoratore ha priorità nelle assunzioni a tempo indeterminato entro 12 mesi dalla fine del contratto.

11.1.3 Contratto Part-Time

Contratto che prevede un orario ridotto rispetto al **tempo pieno standard** (40 ore settimanali). Esisstono diverse tipologie:

- **Orizzontale**: Lavoro giornaliero con meno ore rispetto al tempo pieno.
- **Verticale**: Lavoro a tempo pieno solo in alcuni giorni o periodi della settimana.
- **Misto**: Combinazione delle modalità precedenti.
- **Clausole flessibili**: Consentono al datore di lavoro di modificare orari e giorni di lavoro previo accordo con il dipendente.

11.2 Lavoro Para-subordinato

È una forma intermedia tra lavoro subordinato e autonomo. Si tratta di una collaborazione **continuativa e coordinata**, ma senza un vincolo gerarchico diretto.

- Continuità e coordinamento con il committente.
- Assenza di orari fissi o subordinazione diretta.
- Utilizzo frequente per collaboratori professionali.

Ad esempio, un consulente IT che lavora stabilmente per una società, seguendo specifici progetti senza essere un dipendente.

11.3 Lavoro Autonomo

Il lavoratore gestisce la propria attività in modo **indipendente**, assumendosi i rischi economici e organizzativi.

- Nessun rapporto gerarchico o orario imposto.
- Retribuzione basata sulla prestazione effettuata.
- Flessibilità nell'organizzazione del lavoro.

Ad esempio, un avvocato che offre consulenza legale a più clienti senza vincoli contrattuali con uno specifico datore.

11.4 Contratti Speciali

11.4.1 Apprendistato

Contratto destinato alla **formazione professionale** e all'inserimento dei giovani nel mondo del lavoro. Esistono diverse tipologie:

- **Per qualifica o diploma professionale**.
- **Professionalizzante**: per imparare un mestiere specifico.
- **Alta formazione**: per conseguire titoli accademici o di ricerca.

11.4.2 Lavoro Intermittente (A Chiamata)

Prestazione lavorativa fornita solo su richiesta del datore di lavoro.

- Utilizzabile da giovani sotto i **24 anni** o lavoratori sopra i **55 anni**.
- Non consentito in caso di licenziamenti collettivi o cassa integrazione recenti.

Ad esempio, un ristorante chiama un cameriere per lavorare solo nei weekend di maggiore affluenza.

11.5 Altre Tipologie di Lavoro

11.5.1 Prestazioni Occasionali

Lavoro saltuario, **non continuativo** e con limiti economici.

- Limite massimo di **5.000 euro annui** per prestatore.
- Contratto spesso utilizzato per attività di breve durata.

11.5.2 Tirocini e Stage

Percorsi formativi che permettono ai giovani di **acquisire competenze pratiche**.

- **Curriculari**: Previsti nei piani di studio universitari.
- **Extracurriculari**: Finalizzati all'inserimento nel mercato del lavoro.

11.6 Controversie di Lavoro

Le controversie possono sorgere tra lavoratori e datori di lavoro

11.6.1 Controversie Individuali

Dispute riguardanti singoli lavoratori, spesso legate a:

- Licenziamenti.
- Retribuzioni non corrisposte.

11.6.2 Controversie Collettive

Dispute che coinvolgono gruppi di lavoratori o sindacati, spesso relative a:

- Contratti collettivi.
- Miglioramento delle condizioni lavorative.

Ad esempio, i sindacati scioperano per ottenere un aumento salariale nel CCNL.