Corso 58463: Diritto di Internet

Introduzione

Fonti del diritto: Atti normativi vincolanti per un gruppo o per una comunità

Organi del nostro ordinamento:

- **Legislativo**: Parlamento

- **Esecutivo**: Governo
  Il governo produce delle fonti di legge

- **Giudiziario**: Magistratura (Insieme di giudici)
  Il prodotto giuridico dei giudici è la sentenza, il giudice produce non legge ma la sentenza.

Regola **del precedente** è quella regola in base alla quale il giudice nel decidere una controversia è tenuto a seguire le decisioni prese su casi analoghi da giudici gerarchicamente superiori e talvolta anche dalla stessa corte. Di conseguenza la sentenza del giudice vale come una legge.
Non esiste in Italia la regola del precedente e le sentenze non sono fonti del diritto; quindi, in Italia i precedenti non sono vincolanti per future azioni.

Un principio fondamentale della nostra costituzione è l'istruzione, il diritto alla salute, il diritto al processo.

Gerarchia delle fonti del diritto

1. **Trattati internazionali**
2. **Costituzione Italiana**
3. **Regolamenti e Direttive Europee**
4. **Leggi Ordinarie / Decreti Legge (D.L.) / Decreti Legislativi (D.L.G.S.)**
5. **Regolamenti, Decreto Presidente Consiglio Ministri (D.P.C.M.)**
6. **Leggi regionali / Regolamenti Comunali / Leggi delle provincie Autonome**
7. **Usi e consuetudini**

1) Trattati interazionali

Per **l'Articolo 10 della Costituzione Italiana,** l'Italia si adegua ai Trattati internazionali, che vengono prima della costituzione.

Nei trattati internazionali rientrano anche le Convenzioni Internazionali e le Carte Internazionali.

Esempio: Carta Europea dei diritti fondamentali dell'uomo (Fa parte dei trattati internazionali), trattati costitutivi dell'UE.

Le nazioni unite (ONU) non sono mai riuscite a creare una carta dei diritti dell'uomo mondiale perché, tutte le nazioni del mondo non riescono a mettersi d'accordo su molti aspetti, tra cui il concetto di persona, per molti paesi la donna non è una persona.
Esiste però la Costituzione Europea che vale per tutti i paesi dell'Unione.
I trattati internazionali si possono definire come dei "contratti tra stati".

2) Costituzione Italiana

I suoi principi sono sempre riconosciuti e inviolabili. In vigore dal 1° gennaio 1948, è considerata la legge fondamentale dello stato italiano. I garanti della costituzione sono il presidente della repubblica e la corte costituzionale (controlla la legittimità delle leggi dello stato). Il testo costituzionale in vigore è composto da 139 articoli. La trasformazione delle sue norme può essere disposta solo con legge costituzionale, emanata con una particolare procedura parlamentare.

3) Regolamenti e Direttive Europee

Qual è la differenza tra Regolamenti e Direttive europee?
Direttive: Atti normativi che contengono alcuni principi fondamentali sulla quale i singoli stati membri dell'unione Europea devono declinare in un atto normativo interno. Hanno bisogno di un'azione da parte del Parlamento per essere eseguite.

Regolamenti: Atto di legge europeo automaticamente esecutivo, direttamente applicabile, in alcuni casi può essere recepita e non direttamente applicata tramite una legge di armonizzazione.

Se io adotto una direttiva a livello europeo, dovrò aspettarmi all'interno di ogni paese una legge che tratti l'argomento della direttiva.

NB: La Direttiva detta principi guida.

NB: Se adotto un Regolamento a livello europeo, vale quello, tutti i paesi si devono adeguare a quello

Una direttiva NON può diventare regolamento, alcuni regolamenti però vengono chiamati regolamenti-direttive. Ci sono alcune direttive così specifiche che vengono chiamate direttive-regolamenti.

I confini tra i due atti sono talvolta labili MA entrambi influenzano la politica interna di ogni stato membro.

Se esce un regolamento europeo in aperto contrasto con una legge italiana preesistente la legge preesistente non viene più applicata, quindi il regolamento europeo avrà sempre una valenza maggiore di qualsiasi legge.

Legge posteriore deroga legge anteriore.
La legge che arriva dopo invalida la legge che c'era prima.

La stessa cosa vale con i testamenti, se scrivo più testamenti vale l'ultimo testamento.

Perché si fa così?
Per saltare il lungo processo dell'abrogazione della legge e anche perché il mondo cambia sempre

Abrogazione: Annullamento di una norma giuridica motivato da un provvedimento espressamente abolitivo o, tacitamente, dall'entrata in vigore di una nuova legge

Il diritto nasce dal basso, non è un fenomeno statico, perché prima appare il cambiamento nella società, il diritto arriva dopo (matrimoni gay), perciò si presume che la legge più recente possa meglio rappresentare la direzione della società in quel momento.

Ogni stato membro ha la sovranità in materia penale, in quanto complessa:

- Motivo 1: La libertà personale e di conseguenza le questioni penali sono trattati nelle costituzioni che si trovano ad un livello superiore nella gerarchia delle fonti
- Motivo 2: Per ogni illecito la decisione del legislatore di configurare un reato è una scelta politica, talvolta è più efficace perseguire un illecito tramite procedura civile in quanto la procedura penale potrebbe portare alla prescrizione del reato e alla conseguente impunibilità

4) **Leggi Ordinarie / Decreti Legge (D.L.) / Decreti Legislativi (D.L.G.S.)**

Legge, DL o DLGS sono atti che hanno lo <u>stesso potere</u>.

Quali sono le differenze?

- <u>Legge</u>: È fatta dal parlamento

- <u>DL (Decreto-legge)</u>: È fatto dal governo in situazioni di urgenza e ha lo stesso valore della legge, è direttamente applicabile e ha una durata di 60 giorni. Entro i 60 gg il parlamento può rettificarlo in legge o ignorarlo. In caso di mancata rettifica è come se non fosse mai esistito, perde efficacia in maniera retroattiva (una legge non ha mai effetti retroattivi l'unica eccezione è il DL)

- <u>DLGS (Decreto Legislativo)</u>: È fatto dal governo su delega del parlamento e su specifiche indicazioni e deleghe del parlamento (così il parlamento non perde tempo), una volta entrato in vigore ha lo stesso valore di una legge ordinaria.

Rimpallo normativo: processo classico di redazione degli atti parlamentari;
Camera e Senato si trasmettono a vicenda delle bozze di leggi che vengono esaminate prima dalla Camera poi dal Senato e poi riadottate, funziona allo stesso modo in ambito europeo ma le due parti sono Consiglio Europeo e Parlamento Europeo
Bicameralismo Perfetto (o paritario): il potere esecutivo viene esercitato da due camere rappresentative.

Fatto dal governo = potere esecutivo

Quando gli atti hanno lo stesso potere applico il criterio temporale, mentre applico la gerarchia quando hanno importanza differente

L'Italia è una repubblica parlamentare, il Parlamento viene eletto dal popolo.

I DL e DLGS non essendo fatti dal parlamento, hanno una durata limitata a meno che non vengano ratificati.

Qualora un DL non viene ratificato dal Parlamento (e quindi decade), nulla impedisce al governo di riadattarlo.
Quando il parlamento non è più d'accordo con il DL può chiedere la sfiducia al governo.

Esempio: Se quando c'era il COVID le nuove regole fossero state emanate tramite un DL, e ad esempio dopo le 10 prendevo una multa, una volta decaduto il DL, io avrei avuto diritto a fare ricorso. Ma nella realtà dei fatti, è stato usato il DPCM

5) Regolamenti, Decreto del Presidente del Consiglio dei Ministri (DPCM)

Regolamenti italiani: vengono emanati dalle autorità amministrative indipendenti (autorità per l'energia, autorità trasporti, garante protezione dati, ecc.) sono formati da regole dettagliate emanate nell'ambito della propria autonomia normativa. Hanno la funzione di specificare la legge per renderla più facilmente applicabile alle situazioni concrete. Hanno forza coercitiva, non sono facoltativi.

DPCM: è un regolamento tecnico che si trova ad un livello inferiore nella gerarchia delle fonti e non ha bisogno di tutti i meccanismi di controllo precedenti, ma basta che non contrasti con le leggi sovrastanti, che fanno da meccanismo di controllo.
Il DPCM è un atto esecutivo, se va in contrasto decade immediatamente.
Nel caso del COVID sono stati adottati i DPCM (Decreto Presidente Consiglio Ministri), così non c'è il meccanismo di caduta retroattiva.

6) Leggi regionali – Regolamenti Comunali – Leggi delle provincie

L'unica differenza tra: Leggi regionali / Regolamenti Comunali / Leggi delle provincie Autonome è la scala geografica.

Regioni e parlamento hanno competenze diverse, su alcune materie legifera solo uno delle due, mentre su altre materie legiferano entrambi.
In caso di emergenza lo Stato essendo più competente deciderà in materia di Emergenza o di Sanità.

7) Usi e consuetudini

Comportamenti ripetuti e diffusi nel tempo che i consociati di un determinato gruppo ritengono corretto, le consuetudini variano a seconda del momento storico.
Sono leggi non scritte ma che vengono applicate dai cittadini come se lo fossero.

Esempi:

- Qualche anno fa non era una consuetudine ammissibile che una donna potesse prendere il taxi da sola alle due di notte.
- Discorso di fine anno del presidente della repubblica

Usi e consuetudini variano da paese a paese, ad esempio:

- In Giappone è consuetudine ruttare per far capire che il pasto è stato gradito
- In America è consuetudine dare la mancia

Per alcune consuetudini dipende dal ruolo che diamo alla religione nelle nostre abitudini, oggi non è consuetudine andare a messa ogni domenica, 60 anni fa sì.

Le sanzioni per chi non rispetta usi e consuetudini sono solo morali e sociali.

Illeciti e Sanzioni

Illecito: Comportamento Scorretto

Esistono tre aree di illecito:

1. Illecito Civile: Una controversia tra privati, ovvero è realizzato a danno del privato (la lesione può essere patrimoniale, stimata economicamente, o morale). Il danneggiato ha il diritto di reagire per ottenere che l'atto lesivo venga inibito e che eventuali danni vengano risarciti. Si può avere un giudice pubblico o un giudice privato chiamato anche corte arbitrale
2. Illecito Penale: Detto anche reato, è un illecito che viene realizzato a danno della società civile che prevede la privazione o la diminuzione di un bene individuale: della libertà o del patrimonio. In Italia chi commette un illecito penale può essere condannato con l'ergastolo, con la reclusione o con il pagamento di una multa
3. Illecito Amministrativo: Esempio: una multa, come l'illecito penale è realizzato ai danni della società civile e solitamente viene punito con una sanzione amministrativa di natura economica.

NB: Magistrato e giudice sono sinonimi
NB: Il reato è solo penale, non esiste il reato civile ma l'illecito civile si
NB: Illecito amministrativo e illecito penale non coesistono, o uno o l'altro (generalmente)
NB: L'illecito civile può avvenire anche singolarmente, non per forza insieme ad un illecito penale o amministrativo, per esempio se io vendo un prodotto, mi metto d'accordo con il cliente e dopo lui non mi paga.

Sanzioni: Conseguenza giuridica di un illecito

Tipi di sanzioni:
Giudizio e Risarcimento: per illeciti civili
Detentiva: per illeciti penali
Pecuniaria: per illeciti amministrativi

ESEMPIO: Incidente d'auto

- Illecito civile: Danno materiale, lesione fisica senza dolo o colpa (es: pago il salario dell'operaio che non può lavorare)
- Illecito penale: quando abbiamo un reato (infrante norme del codice penale) oppure danno grave ad una persona (può portare a reclusione/risarcimenti)
- Illecito amministrativo: multa

Quando sussiste il reato?
Il reato esiste solo se ho agito con **dolo** (volontà di infrangere la legge) o con **colpa** (senza volontà diretta ma agendo non seguendo le regole)

Dolo: indica la volontà cosciente di un individuo nel commettere un danno altrui. Se il soggetto ha piena coscienza quando commette l'azione di dolo la legge prevede pene che vanno dalla multa alla reclusione.

Colpa: è associabile all'azione che porta ad un danno, non vi è stata volontà ma viene violata la regola di condotta. Viene spesso associata alla negligenza (mancanza di impegno nel compiere i propri doveri), all'imperizia (mancanza di abilità e di esperienza nella propria professione) e all'imprudenza.

NB: il reato doloso è punito molto più severamente di quello colposo.

Questo corso è principalmente di diritto civile, perché noi dobbiamo parlare di internet.
Le sentenze hanno forza di legge tra le parti di quello specifico processo.

Legge applicabile agli atti giuridici compiuti via internet

Atto giuridico: Un' azione che ora o in futuro può avere una rilevanza in ambito giuridico (uso un social, compro una macchina ecc.)

Nella vita di tutti i giorni i giuristi per sapere qual è il diritto applicabile, utilizzano criteri geografici e territoriali, internet però non è un luogo è un canale di comunicazione decentralizzato; dunque, è difficile se non impossibile identificare la nazione di appartenenza delle parti in causa.

Vi sono tre tesi fondamentali su quale debba essere il diritto da applicare su Internet:

1. Anarchia Totale: Internet come luogo senza Legge. Questa idea dimostra di essere utopistica, soprattutto di fronte a situazioni di conflitto.

PRO: Libertà, diffusione. CONTRO: Truffe, abusi, disorientante.

2 Mondo Virtuale con norme specifiche ad hoc.

PRO: Controllo, chiarezza CONTRO: A chi appartiene il potere legislativo in una rete universale multinazionale?

3 Stesse norme che regolano il mondo "reale", con l'ausilio di strumenti interpretativi.
PRO: Consolidato e conosciuto CONTRO: È nazionale, si basa su un mondo materiale

Si è deciso di adottare l'ultima soluzione, utilizzando misure correttive per applicare la normativa comune al mondo di Internet.

Esiste un'altra teoria sul diritto di Internet, di matrice USA, promossa da due teorici del diritto: Lawrence Lessig (professore di Harvard già noto per aver creato i Creative Commons) e Joel Reidenberg. Si tratta della "LEX INFORMATICA", ovvero l'idea di disciplinare il mondo di Internet tramite una legge informatica, imponendo l'applicazione delle norme di diritto tramite la tecnologia: veicolando il diritto attraverso il mezzo tecnico (Service Provider), ovvero la possibilità di fare solo ciò che è stato concesso tecnologicamente.
La problematica principale di un modello di questo tipo è lo strapotere dei tecnici (Tecnocrazia), che abolirebbe il principio democratico dell'attuale potere legislativo (il Parlamento eletto).

Lex Mercatoria

La lex mercatoria ha lo scopo di proporre un diritto comune di Internet, inteso come l'insieme degli usi e delle pratiche accettate dalle Corti dietro le indicazioni degli utenti, dei governi e dell'industria di Internet.
La lex mercatoria è stata richiamata dai giuristi che si sono occupati della legge applicabile a Internet, che hanno voluto ricostruire in termini di analogia con la lex mercatoria il processo di formazione del diritto applicabile su Internet, con riferimento in particolare all'autoregolazione.
C'è una differenza con la lex informatica che viene intesa come un insieme di regole tecniche che veicolano scelte giuridiche, la lex mercatoria è, invece applicabile ai rapporti fra imprese.

L'espressione lex mercatoria ha tre possibil interpretazioni:

1) la lex mercatoria sarebbe costituita da un insieme ("legal mass") di regole e di principi senza una consistenza interna, senza sistematicità;
2) la lex mercatoria sarebbe costituita dagli usi del commercio;
3) secondo la terza definizione, che qui pare essere al più rilevante, si tratterebbe di un sistema giuridico sovranazionale, che trarrebbe la sua giustificazione e la sua validità dal fatto della sua stessa esistenza o dal principio dell'autonomia delle parti come meta-regola.

Il fondamento della lex mercatoria è, invece, nella teoria classica delle fonti, individuato di volta in volta nella consuetudine, nel diritto corporativo. La difficoltà di inquadramento sistematico nel sistema tradizionale delle fonti del diritto della lex mercatoria deriva dal fatto che al lex mercatoria si colloca al di fuori di quel sistema, rompe un tabu, quello del rapporto fra diritto e Stato, in un duplice senso: introducendo un diritto di origine privata, fuori dal controllo dello Stato, e con-ferendo validità al diritto formato al di fuori dello Stato e delle istituzioni internazionali, e quindi al di fuori degli apparati sanzionatori e indipendentemente dalla legittimazione che proviene dal processo democratico.

Service Provider: Imprese che erogano servizi di vario tipo, appartenenti a settori differenti (Tim, Vodafone ecc.)

Sorge però il problema di un accentramento di potere, l'SP può fare quello che ritiene più opportuno, non è come il parlamento.
Allora per risolvere questo problema si applicano ad Internet le regole tradizionali.
Vantaggi:

- Presunta conoscenza diffusa, i meno esperti non sono tenuti a conoscere le leggi di internet, visto che sono uguali a quelli della vita di tutti i giorni.

Svantaggi:

- La maggior parte delle leggi nascono per il mondo fisico e bisogna riadattarle al mondo virtuale. Qui sorgono alcuni problemi.
- Omogeneità: ogni stato ha le proprie leggi

La legge si applica alla rete tramite **il Modello di legge sul commercio elettronico (MLEC).**
Versione Tradotta (ITA): MLEC - Tradotto.pdf
Versione Originale: MLEC.pdf

Attenzione, è un modello di legge, ovvero un atto di soft-law, che gli stati possono copiare per scrivere le proprie leggi.

L'UNCITRAL (*United Nations Commission for International Trade Law*) è una commissione delle Nazioni Unite che ha il compito di armonizzare e modernizzare progressivamente le regole del commercio internazionale. Ha principalmente due strumenti di azione: Model Law e Convenzioni.

In particolare, l'Uncitral ha redatto tre testi di nostro interesse: due **Model Law** (una relativa al **commercio elettronico,** una alle **firme elettroniche**) e una **Convenzione sulle Comunicazioni Elettroniche**.

I **Model Law** (ovvero dei modelli di legge, di riferimento) possono essere adottati (dall'Unione Europea o dai singoli Stati), sia integralmente che parzialmente, rendendoli quindi a tutti gli effetti vincolanti ("Hard Law", presenti nel diritto vigente e quindi strettamente vincolanti).
Nel caso invece non vengano ufficialmente adottati, non hanno efficacia giuridica diretta ma solo un valore persuasivo di influenza. In questo caso però, considerando l'importanza internazionale delle Nazioni Unite, il valore persuasivo delle Model Law è comunque grande, sia nel mondo del commercio internazionale che nel campo della magistratura dei singoli stati membri: in caso di difficoltà a reperire risposte nel diritto vigente *("Hard Law"*), i Model Law sono utilizzati dai giudici per formare il loro convincimento (come fonti di *"Soft Law",* non vincolanti).

Il **Model Law sul Commercio Elettronico** *(UNCITRAL Model Law on Electronic Commerce – MLEC)* è stata la prima legge redatta per consentire ed agevolare il commercio effettuato con mezzi elettronici, fornendo ai legislatori nazionali norme internazionalmente accettate, volte a

rimuovere ostacoli giuridici all'uso di tali mezzi, contribuendo così alla certezza del diritto in questo campo. L'obiettivo principale della MLEC è di definire i concetti fondamentali necessari a stabilire la parità di trattamento giuridico tra supporto cartaceo e mezzo elettronico (ovvero i tre principi esposti in precedenza).

Articolo 5 - MLEC: Riconoscimento giuridico dei messaggi di dati.
"Information shall not be denied legal effect, validity or enforce-ability solely on the grounds that it is in the form of a data message."
Esempio concreto: Un'informazione resta valida anche se in forma elettronica. Se io porto in tribunale un messaggio, a quel messaggio non può essere negata validità.
Ricorda: Nel caso di una controversia online tra soggetti di nazionalità diversa, si applica la legge di residenza del soggetto che ha subito l'offesa.

Contratti

Articolo 1321 - Codice civile: Il contratto è l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale.

Contratto: nasce nel mondo fisico. Regola il rapporto che ha un contenuto patrimoniale.
Accordo: oltre a bilaterale (tra due parti) può essere plurilaterale tra parti che hanno una volontà convergente. L'effetto vincolante del contratto è soltanto tra le parti che vi hanno aderito.

Tutta la nostra vita è regolata da contratti:

- Comprare un caffè al bar: accordo tra due soggetti regolato da un contratto di compravendita di beni alimentari;
- Contratto telefonico: contratto di lunga durata di somministrazione di un servizio;
- Quando prendo l'autobus: contratto di trasporto con Azienda Municipale;
- Contratto di somministrazione di beni e servizi: acqua, elettricità, gas, etc.;
- Contratto di compravendita di un bene immobile;
- Contratto di prestito con la banca.

Il matrimonio non è un contratto

Articolo 1325 – Codice Civile: Requisiti del contratto

I requisiti del contratto sono:

1) **L'accordo delle parti**
2) **La causa**
3) **L'oggetto**

4) **La forma, quando risulta che è prescritta dalla legge sotto pena di nullità**

Causa: ragione socioeconomica per cui viene fatto un contratto. Quando pensiamo alla causa del contratto noi dobbiamo sempre guardarlo dall'esterno e non sappiamo perché le parti fanno quello che stanno facendo. Se non c'è una causa del contratto, non possiamo capire perché il contratto esiste e quindi diventa invalido.

Forma: È il modo in cui vengono espresse le condizioni del contratto, non c'è una forma stabilita dalla legge.

Accordo tra le parti: il contratto si conclude quando il componete avviene a effettiva conoscenza dell'accettazione.

Un contratto può essere concluso tacitamente

Esempio: salgo sull'autobus

Oggetto: è ciò di cui si parla

Contratto ad oggetto informatico: Un contratto avente ad oggetto un software, o un qualsiasi altro contratto che è inerente all'ambito informatico.

Sono tanti i contratti che hanno oggetto informatico, l'esempio più comune è il contratto di fornitura di sistema informatico, che comprende una serie di prestazioni di natura diversa.

Quali possono essere le prestazioni di un contratto di sistema informatico?

Esempio: Vogliamo fare una nostra impresa oppure siamo dei consulenti tecnologici dell'università, che prestazioni a livello di sistema informatico abbiamo bisogno?

- Computer
- Software standard (Office)
- Software specifici (Gestionali)
- Prestazione hardware
- Stampati

L'UniBO compra 2.500 computer desktop a 800€ l'uno
Per non spendere 2.000.000€ ho un'atra opzione: **il noleggio**

Le imprese oggi non possono permettersi di fermarsi, necessitano di servizi informatici senza interruzione e con il contratto di noleggio c'è spesso anche quello di assistenza.

Quindi l'UniBO sceglierà il contratto di noleggio che comprende 25 computer e 25 server per 1.100€ al mese per 5 anni e con il pacchetto assistenza incluso.

Quindi nel contratto di fornitura di sistema informatico io ho una serie di informazioni di natura diversa perché pensando alla funzione socioeconomica in potrei ricollegare tipologie di contratti diversissime.

Operazione Ermeneutica: I giuristi quando guardano un contratto ragionano a quale tipo di contratto già esistente e già disciplinato dal codice civile si avvicina di più in modo tale da poter qualificare il contratto e dedurne la disciplina che si applica.

Causa mista: quando un contratto racchiude in sé tipologie contrattuali diverse svolgendo un'unica funzione sociale.
Esempio:
Quando devo cambiare automobile, porto al concessionario il mio vecchio veicolo per la permuta. Un po' pago la nuova macchina e un po' permuto la vecchia, questo è un contratto di causa mista tra permuta e vendita.

Esempio 2:
Contratto di parcheggio, quando noi portiamo l'auto facciamo un contratto di deposito e affittiamo un posto auto per un certo periodo di tempo.

Collegamento negoziale: ho contratti distinti tra loro ma che hanno un unico scopo.

La differenza tra collegamento negoziale e causa mista è sostanzialmente che nel collegamento negoziale i contratti singolarmente presi sembrano autosufficienti, nel collegamento negoziale non risiede per forza nella natura del rapporto, può anche essere volontario.

Esempio: Compro un appartamento per 300.000 € e mentre lo compro dico all'agente immobiliare che voglio comprare anche quello adiacente. Non potendo fare subito la compravendita, mi è stato fatto un contratto preliminare. Sono contratti potenzialmente autosufficienti che svolgono un'unica funzione, il compratore voleva comprare l'appartamento e il monolocale per unire, due contratti collegati, l'adempimento di una porta all'adempimento dell'altro.

Se salgo sull'autobus non pago il biglietto, ho **concluso un contratto**? Si, salendo sull'autobus sono già vincolato, se non pago rischio una multa. La conclusione del contratto non ha niente a che vedere con la corresponsione di un prezzo, ma nasce con la volontà, in questo caso implicita, di accordo tra due parti.
La fase dell'**adempimento** (ovvero del pagamento) è scollegata dalla fase di conclusione di contratto. Quindi nel caso di un acquisto di un bene a rate, il contratto viene concluso al principio, anche se l'adempimento contrattuale è successivo.

Ai sensi del Codice Civile può dirsi **concluso** normalmente un contratto nel momento in cui c'è l'**incontro delle volontà**. Per stabilire l'incontro delle volontà in un **Contratto a distanza** (o su Internet):

Articolo 1326 - Codice civile: Conclusione del contratto

Il contratto è concluso nel momento in cui chi ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte

Ovvero quando il soggetto proponente **RICEVE** l'accettazione (la legge è stata scritta nel 1942!).
Esempio concreto: Quando Amazon riceve conferma del mio ordine il contratto è concluso.

Articolo 1323 - Codice civile: Tutti i contratti, ancorché non appartengono ai tipi che hanno una disciplina particolare, sono sottoposti alle norme generali contenute in questo titolo (Codice Civile)

Cioè a tutti i contratti (anche quelli stipulati su Internet) si applicano le norme del Codice Civile, eccetto per i contratti "tipizzati" disciplinati in altre parti del Codice Civile (vendita, appalto, mutuo, locazione, in tutto sono circa 30). Il codice Civile è stato scritto nel 1942, quindi non si potevano conoscere e regolarizzare tutti tipi di contratto esistenti oggi giorno (tipo quelli della *Digital Economy*). I **contratti tipici** sono quelli definiti e descritti nel Codice Civile, gli altri si chiamano **contratti atipici**, regolati da questo articolo del Codice.
Naturalmente il contratto deve **essere lecito anche dal punto di vista penale**, non posso fare un contratto per la compravendita di marijuana o per assassinare una persona (oggetto illecito -> contratto invalido).
In conclusione, l'articolo dice che se c'è accordo tra le parti fatto per modificare, regolare o estinguere un accordo di tipo patrimoniale (quindi se c'è un contratto), qualsiasi sia la natura, la forma, il luogo o il mezzo tramite il quale viene concluso, si applicherà comunque il Codice Civile.

Il contratto viene anche definito come un rapporto giuridico.
R**apporto giuridico:** è il rapporto fra due parti riconosciuto dalla legge.
Può essere di due tipi:
Patrimoniale: è un rapporto valutabile in termini economici.
Non patrimoniale: la prestazione compiuta non è suscettibile di valutazione economica.

In caso di una violazione contrattuale, può essere previsto un risarcimento, che varia se il rapporto giuridico è patrimoniale o non patrimoniale.

Danno in un rapporto giuridico patrimoniale:

- la lesione diretta del patrimonio del danneggiato, si parla di **danno emergente** (Per esempio, nel caso di un incidente stradale, è un danno emergente il costo sopportato per riparare il paraurti dell'auto danneggiata);
- la lesione del patrimonio in prospettiva rappresentata dai minori guadagni che il danneggiato realizzerà in seguito dalla lesione della sua posizione (si pensi ai mancati guadagni del professionista costretto ad un ricovero ospedaliero per essere stato investito mentre attraversava la strada) ed in questo caso si parla di **lucro cessante**.

Danno in un rapporto giuridico non patrimoniale:

- danno **biologico**: danno alla salute
- danno **morale**: il danno conseguente al dolore patito per avere subito un reato
- danno **esistenziale**: il danno relativo a quelle lesioni della sfera personale che determinavano una situazione nella quale la vittima non era più in grado di portare avanti delle attività e delle abitudini che avevano caratterizzato il suo precedente stile di vita.

Fonte: Il risarcimento del danno (dirittierisposte.it)

Ciascun individuo quando nasce viene dotato di **capacità giuridica** dall'ordinamento italiano (ovvero siamo *centro di imputazione di diritti*, possiamo riceverli). Quando si diventa maggiorenni l'ordinamento attribuisce la **capacità di agire**, ovvero la possibilità di concludere contratti. Se compiamo un gravissimo reato, tra le pene accessorie potrebbe esserci tolta la capacità di agire (non possiamo più concludere contratti), tramite l'**interdizione**. La rimozione, da parte di un giudice, della capacità di agire (ad esempio per motivi di sanità mentale) è detta di **inabilitazione**.

Articolo 1 – Codice Civile: *Capacità giuridica*
Capacità di un soggetto di essere titolare di diritto e doversi, si acquista alla nascita (in realtà prima, dal momento in cui siamo stati concepiti), da quel momento siamo proprietari della capacità giuridica (esempio posso fare un testamento ad un concepito, a patto che nasca).

Articolo 2 - Codice Civile: *Capacità di agire*
Capacità di compiere validamente atti giuridici. Questa capacità si acquista quando si diventa maggiorenni (18 anni)

Un bambino, quindi privo giuridicamente della capacità di agire, può comprare un biglietto dell'autobus? O la merendina al distributore automatico? In teoria no: i soggetti interdetti e inabilitati, o i minori, non potrebbero comprare neanche un biglietto dell'autobus. La soluzione adottata dal Diritto vigente, per risolvere questo genere di situazioni, è considerare il fatto che la **cifra spesa è di modico valore**, e che i bambini (o gli l'anziani) abbiano concluso il contratto **nell'interesse e per conto dei genitori** (o del tutore): paradossalmente i bambini agiscono, per la Legge, come rappresentanti legali dei genitori.

Commercio elettronico

Il commercio elettronico viene tutelato principalmente dal DLGS 70/2003, ma anche dal Codice del Consumo (DGLS 206/2005) e dal Codice Civile.

Persona Fisica: è un essere umano, un comune cittadino
Persona Giuridica: identificata in un'azienda o una società

Dividiamo i contratti online in tre categorie:
B2B - Business to Business: è un contratto tra due imprese (Persona Giuridica – Persona Giuridica).
Esempio: L'azienda UniBO compra software dall'azienda Microsoft

B2C - Business to Consumers: è un contratto tra un'impresa e un consumatore (Persona Giuridica – Persona Fisica)
Esempio: Apple vende uno smartphone a Mario Rossi

C2C – Consumers to Consumers: è un contratto tra un consumatore e un consumatore (Persona Fisica – Persona Fisica), viene chiamato anche P2P (Peer to Peer).
Esempio: Mario rossi vende su Facebook Marketplace una bici usata a Giorgio BIanchi

Leggi a tutela:

B2B	B2C
DLGS 70/2003	DLGS 70/2003
Codice civile	Codice Consumo (DLGS

DLGS 70/2003: recepisce una direttiva Europea del 2000 sul commercio elettronico che aveva come obiettivo di accrescere la fiducia nel mezzo elettronico per il commercio sia nel consumatore che per i professionisti, attraverso regole chiare, trasparenti e condivise.

Articolo 6 - DLGS 70/2003: Assenza di autorizzazione preventiva

L'accesso all'attività di un prestatore di un servizio della società dell'informazione e il suo esercizio non sono soggetti, in quanto tali, ad autorizzazione preventiva o ad altra misura di effetto equivalente.

Riassumendo: il servizio di un SP non è soggetto ad autorizzazione preventiva (puoi fare quello che ti pare senza bisogno di autorizzazioni), di solito le norme servono per vietare qualcosa, questa invece serve per incentivare e garantire lo sviluppo del commercio elettronico

Il ***consumatore*** generalmente è una figura tutelata nel quadro normativo. **Le principali forme di tutela sono:**

- **Obblighi informativi** che gravano sul provider *(Art. 7, D.Lgs. 70/2003 e Art 49. Comma 1 del C.d.C., per i soli contratti a distanza)*;
- **Possibilità di recesso** del consumatore *(L'Art. 52, Comma 1, C.d.C.)*;
- **Protezione dalle clausole vessatorie** *(Art. 33 e seguenti, C.d.C.)*
- Scelta del **foro competente** prevista per legge. Al consumatore si devono applicare regole particolari per determinare quale sia la legge applicabile al contratto, ovvero la scelta del foro competente per dirimere eventuali controversie è prevista per legge

Articolo 7 - DLGS 70/2003: Informazioni generali obbligatorie

Indica che il prestatore del servizio deve rendere **facilmente accessibili**, in modo **diretto** e **permanente**, ai destinatari del servizio ed alle autorità competenti, mantenendole sempre **aggiornate**, alcune informazioni sul suo sito web, tra cui:

- il nome, la **denominazione**, o la ragione sociale;
- il domicilio o la **sede legale**;
- gli estremi, compreso **l'indirizzo di posta elettronica**, che permettano di contattare rapidamente il prestatore e di comunicare direttamente ed efficacemente con lo stesso;
- gli elementi di individuazione della competente autorità di vigilanza nel caso l'attività sia soggetta a **concessioni, licenza o autorizzazioni**, e se il prestatore rientra in un ordine professionale regolamentato deve inoltre fornire sia l'**ordine** presso cui è iscritto, con il relativo numero d'iscrizione, il titolo professionale, con indicato lo Stato membro in cui è stato rilasciato, e il riferimento alle **norme professionali** e ad eventuali **codici di condotta**;
- se il prestatore esercita un'attività soggetta ad imposta, il **numero di partita IVA** o un altro numero di identificazione considerato equivalente;
- l'identificazione in modo **chiaro** ed **inequivocabile dei prezzi** e delle tariffe dei diversi servizi forniti, evidenziando se comprendono le **imposte**, i **costi di consegna** o altri elementi aggiuntivi che andranno in ogni caso specificati;
- l'indicazione delle **attività consentite al consumatore** (e al destinatario del servizio) se è un'attività è soggetta ad autorizzazione o se si tratta di un contratto di **licenza d'uso**.

Questa norma tutela le due parti, creando un rapporto di fiducia grazie alle informazioni rese pubbliche, obbligo trasversale. Nel caso dei B2C, il consumatore è più tutelato (perché è un utente debole) e quindi l'impresa ha più obblighi da rispettare, dunque favorendo il commercio elettronico, perché se il venditore è rintracciabile, le persone si sentono più sicure ad acquistare online.

Articolo 8 - DLGS 70/2003: Obblighi di informazione per la comunicazione commerciale

Definisce tutte le regole per una società che intende far pubblicità tramite comunicazioni commerciali con finalità di Marketing anche via SMS o e-mail

Tali comunicazioni sono ben diverse dalle finalità puramente informative: pertanto devono evidenziare in modo **chiaro** ed **inequivocabile**:

- Che si tratta di **comunicazione commerciale**;
- Il nominativo della **persona fisica o giuridica** per conto della quale è effettuata la comunicazione commerciale;
- Che si tratta di un'**offerta promozionale**, con sconti, premi o omaggi e le relative condizioni di accesso;
- Che si tratta di **concorsi o giochi promozionali**, se consentiti, e le relative condizioni di partecipazione.

Articolo 9, comma 2 - DLGS 70/2003: Comunicazione commerciale non sollecitata

Specifica che la **prova del carattere sollecitato** delle comunicazioni commerciali è **onere del prestatore**, ovvero quando la comunicazione non è richiesta, a maggior ragione bisogna renderla identificabile: una volta in giudizio sarà il prestatore a dover dimostrare che l'utente aveva autorizzato l'invio di comunicazioni commerciali.
Ancora una norma, come quella dell'*Art. 8*, tesa a diminuire e limitare l'effetto invasivo e l'impatto dell'intento commerciale dell'impresa sul cliente.

Articolo 12, comma 3 - DLGS 70/2003: Informazioni Dirette alla conclusione del contratto
Le clausole e le condizioni generali del contratto proposte al destinatario devono essere messe a sua disposizione in modo che gli sia consentita la memorizzazione e la riproduzione

L'obiettivo, la ratio alla base di questa norma è di fornire alle parti delle prove in previsione di un'eventuale contenzioso, in una fase patologica successiva.

Codice del Consumo (DLGS 206/2005): è un codice, ovvero una raccolta delle disposizioni su una determinata materia, in questo caso sulla tutela del consumatore. È stato introdotto con D.Lgs. n. 206/2005 e successivamente integrato/modificato dal D.Lgs. n. 21/2014.

L'obiettivo del Codice del Consumo è quello di tutelare in maniera adeguata il consumatore, ma anche di portare vantaggi per le imprese, sviluppando la concorrenza, la trasparenza e l'informazione al fine di favorire una migliore qualità dei prodotti e dei servizi.

Il Codice del Consumo vale per:
- Contratti conclusi con il consumatore, **solo di tipo B2C**
- Consumatori **residenti in Europa**, in quanto deriva da un regolamento Europeo

Articolo 49 - Codice del Consumo: Informazioni obbligatorie in caso di contratti conclusi distanza
Elenca molte informazioni, tra cui principalmente:

- le **caratteristiche principali** dei beni o servizi, nella misura adeguata;
- **identità** del professionista (come per il D.Lgs. 70/2003) e i suoi **recapiti**;
- se il prezzo è comprensivo di **imposte**;
- se è previsto o meno il diritto di recesso, le sue condizioni, termine e procedure (eventuale costo per la spedizione di reso);
- la **durata** (se applicabile) del contratto.

Diritto di Recesso: Recesso, chiamata anche facoltà di pentimento: quando si conclude un contratto, si è vincolati a norma di Legge. Tuttavia, in alcuni casi, come in quello del contratto a distanza (a parte particolari eccezioni) è possibile per il consumatore recedere da esso, quindi sciogliere il contratto, anche se è stato già effettuato l'adempimento (ovvero il pagamento).

Articolo 52 - Codice del Consumo: Diritto di recesso

Il consumatore ha sempre diritto, salvo alcune eccezioni, al **Diritto di Recesso**, senza dover sostenere **costi aggiuntivi** (tranne esclusivamente per le spese di reso se precedentemente specificato nel contratto), senza l'obbligo di fornire **motivazioni** e stabilendo il **periodo di tutela minimo** in 14 gg.

Il diritto di recesso è teso a **ristabilire la situazione precedente al contratto**. Ciò significa che è facoltà del consumatore decidere se accettare un buono (forma più utilizzata dai prestatori) o richiedere il rimborso in denaro (ripristinare la situazione precedente al contratto: il consumatore restituisce il bene e il prestatore restituisce ciò che il consumatore ha dedotto in controprestazione).

Il diritto di recesso per i contratti a distanza **è imprescindibile**, anche se lo stesso consumatore volesse rinunciarvi, perché si presuppone che a distanza non si ha la possibilità di osservare, toccare con mano e valutare il prodotto.

Tra le informazioni obbligatorie da fornire al consumatore bisogna indicare se le spese di spedizione di reso in caso di recesso devono essere imputate al consumatore: se non è presente la specifica indicazione, non possono essere richieste.

La normativa indica il periodo minimo, è facoltà del prestatore, a suo giudizio, aumentare eventualmente questo periodo (per esempio per strategie di marketing e fidelizzazione del cliente). Non sono necessarie giustificazioni a fondamento del recesso, sono facoltative, anche se spesso il professionista ha interesse di conoscere le motivazioni di recesso per motivi commerciali.

Il prestatore, per suo esclusivo interesse, potrebbe indicare nelle condizioni generali di contratto a distanza che non è consentito il diritto di recesso o che la restituzione del denaro può avvenire esclusivamente tramite un buono d'acquisto, ma sono **clausole illegittime e quindi non valide**, anche se spesso il consumatore, credendole legittime, si attiene a queste condizioni.

Prestazione -> consegnare il bene/servizio
Controprestazione -> pagare un
corrispettivo

Il bene restituito dovrà continuare ad essere idoneo all'uso per cui è stato concepito. Ad esempio la l'etichetta di vendita può essere tolta, perché la sua mancanza non modifica la capacità del bene di essere utilizzato.

Il diritto di recesso è unilaterale: solo il consumatore può esercitarlo.

NB: Solo nei contratti B2C a distanza

Articolo 59 - Codice del Consumo: Eccezioni al diritto di recesso
Contiene l'elenco delle ***eccezioni al Diritto di Recesso*** nei contratti a distanza, tra cui troviamo:

- ✓ la fornitura di **beni su misura o confezionati**;
- ✓ beni **deteriorabili** o alimentari soggetti a breve scadenza;
- ✓ **beni sigillati per motivi di salute** (medicinali) che sono stati aperti;

- ✓ **i prodotti finanziari** soggetti alle variazioni di mercato nel breve periodo;
- ✓ software su supporti fisici la cui confezione è stata aperta o **contenuti digitali già scaricati**;
- ✓ Aste pubbliche

Una regola generale che si evince dalle norme è che il bene può essere restituito solo se può essere provato senza **alterarne le caratteristiche essenziali**.

Legge applicabile: Come faccio a capire quale legge si applica ad un contatto se acquisto un bene proveniente da un altro paese?
Su Internet non è immediato identificare la legge di competenza: la difficoltà è capire in quale materia rientra la questione da trattare, perché a seconda dell'ambito di competenza varia la legge applicabile.
Al contratto a distanza **applico la legge del luogo di residenza del consumatore** a prescindere da chi sia e dove risieda il prestatore, e comunque, anche qualora fosse indicata nel contratto una legge diversa, **il consumatore non può essere privato dei privilegi, benefici e delle tutele minime che gli sono garantite dalla Legge del proprio Stato di residenza**. Per il prestatore si apre uno spazio di autonomia, posso applicare regole e disposizioni diverse da quelle presenti nella norma vigente presso il Paese di residenza del consumatore, ma si rimane comunque vincolati alle **tutele minime** previste da quella norma.

Articolo 66 ter - Codice del Consumo: Carattere imperativo

Questo **livello minimo di tutela appartiene al consumatore** residente in Italia per natura, non gli può essere sottratta ed è inoltre **imprescindibile** (ovvero è una tutela a cui non si può rinunciare). Qualora sia prevista nel contratto una clausola per lui peggiorativa, quella clausola non si applicherà. Se ne deduce che il consumatore italiano che sta concludendo su Internet un contratto, non dovrebbe preoccuparsi di quale sia il diritto applicabile definito dal contratto, infatti in quanto cittadino residente in Italia, riceverà automaticamente tutte le tutele previste dal Codice Italiano.
Se invece la clausola migliorativa è nel regolamento di un altro paese, si applica quella, il consumatore è sempre tutelato.

Esempio: Se compro un libro su un sito spagnolo dall'Italia e lo voglio restituire il quindicesimo giorno, dato che la legge italiana non me lo garantisce, posso vedere se quella spagnola mi dà la possibilità. Se in Spagna, hanno il diritto di recesso garantito per 20 giorni posso restituire il prodotto che ho comprato sul sito.

Articolo 66 bis - Codice del Consumo: Foro competente

Nei processi, prima di andare a parlare del merito (ovvero di ciò che è successo), l'avvocato deve verificare se il Giudice (foro competente) è quello giusto e quale sia la legge applicabile.
Con **Foro di competenza** si intende il **Giudice di competenza (territoriale)** incaricato di decidere della controversia. Se nel contratto (solo se "a distanza") è presente una clausola che indica un foro diverso da quello del consumatore, anche se viene dimostrata una trattativa a riguardo, in base a questa norma è sempre da considerarsi nulla.

Nel Diritto Internazionale la legge applicabile (quindi il foro competente e la relativa lingua, e le normative di riferimento) è fondamentale per poter prevedere l'esito probabile di una causa.

È un grande vantaggio avere come foro di competenza il tribunale di residenza, sia per comodità pratica ed economica che per strategia processuale.

In parole povere:
La legge applicabile e il foro di competenza (giudice) devono essere del paese di provenienza del consumatore, in modo tale che esso sia maggiormente tutelato. Il processo sarà più rapido, le spese saranno minori, e anche il fattore linguistico svolge un ruolo notevole.

NB: Giurisdizione = Foro di competenza= Giudice competente: potere locale (conosciuta anche come Foro o Giudice competete): Autorità o potere locale, o anche l'ambito territoriale in cui si esercita

Adempimento dell'informazione: Quando manca un'informazione rilevante nell'acquisto di un prodotto online.
Chi paga i costi di spedizione? Dipende. Il costo della spedizione lo può pagare il consumatore solo se ciò è dichiarato nel contratto. Se non lo si dice, la spedizione è sempre a carico dell'impresa. Tutto questo lo si dice prima del pagamento, nel contratto. Il contratto lo si trova nella sezione "Condizioni Generali di Uso e Vendita".

Nel B2B
Nei contratti B2B, l'imprenditore decide e predispone quale foro di competenza usare. Nel caso in cui ciò non venga stabilito, si applica la legge del luogo dove ha sede l'impresa che deve "consumare"

Arbitrato: Un giudice privato, che viene scelto. Deve essere composto da 1 o da un numero dispari di arbitri, in modo che non ci siano pareggi di indecisioni. Il venditore di solito sceglie un arbitro, il compratore ne sceglie un altro e i due arbitri ne sceglieranno un terzo.

Uno degli strumenti più utilizzati dai giudici per identificare se un contratto è B2C o B2B (e quindi quale normativa applicare) è la richiesta di una fattura come ricevuta di pagamento.

Ricapitolando:
Predisposizioni che si applicano nel B2B:

1. Gli obblighi informativi sono previsti dal decreto legislativo 70/2003
2. Recessi – Deve essere scritto nel contratto se c'è la possibilità tra imprenditori
3. Legge applicabile (Legge scelta) – La legge può essere scelta dalle parti
4. Giurisdizione
5. Clausole Vessatorie

Predisposizioni che si applicano nel B2C:

1. Informazione (Codice del Consumo + decreto legislativo 702003)
2. Recesso – Facoltà riconosciuta al consumatore che lo può consumare al minimo 14 giorni.

3. Legge applicabile – Quali leggere applicare, di quale paese
4. Foro competente – Giudice competente
5. Clausole Vessatorie

Clausole Vessatorie

Clausole vessatorie: Disposizioni contrattuali che causano uno **squilibrio tra le parti** del contratto, a favore dell'imprenditore e a svantaggio e danno del consumatore. Le clausole vessatorie sono trattate nel C.C. (B2B o C2C) e nel C.d.C. (nel caso di B2C).

NB: Vessare = Infierire

A volte le grandi aziende possono **inserire volutamente clausole che sappiamo essere nulle**. Spesso c'è una scelta precisa di non scrivere contratti del tutto conformi alla Legge: per esempio le aziende sono consapevoli che la clausola che indica un foro di competenza diverso da quello di residenza del consumatore è comunque nulla, ma viene inserita in ogni caso perché c'è la consapevolezza dell'**effetto psicologico deterrente verso il consumatore**, il quale sentendosi svantaggiato (non sapendo che comunque potrebbe usufruire del processo nel suo foro di residenza), è dissuaso dall'agire in giudizio. Allo stesso modo, è dissuaso dall'esercitare il **diritto di recesso** se leggesse sul contratto che esso non è previsto. Di fatto si cerca di sfruttare "l'ignoranza" del consumatore.

Clausole vessatorie nei contratti B2C: Codice del Consumo

Articolo 33 - Codice del Consumo: Clausole vessatorie nel contratto tra professionista e consumatore

Nel contratto concluso tra il consumatore ed il professionista si considerano vessatorie le clausole che, malgrado la buona fede, determinano a carico del consumatore un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto

Per aumentare la tutela nei confronti del consumatore e facilitare il lavoro di valutazione del giudice, il legislatore ha previsto le clausole da considerarsi presumibilmente vessatorie (fino a prova contraria) nel comma 2, tra le quali:

- ✓ a) Escludere o limitare la responsabilità in caso di **morte o danno del consumatore** (per colpa imputabile al professionista);
- ✓ b) Escludere o limitare **le possibilità d'azione** (ovvero effettuare una richiesta in sede di giudizio) e i diritti del consumatore nei confronti del professionista;
- ✓ c) Escludere la possibilità di stabilire la **sede del foro competente** sulle controversie in una località diversa da quella di residenza o domicilio elettivo del consumatore;

Queste norme **presuppongono una valutazione**: la clausola va interpretata dal giudice che stabilisce se è da considerarsi effettivamente vessatoria.

Articolo 34, comma 4 - Codice del Consumo: Accertamento della vessatorietà delle clausole
Non sono vessatorie le clausole o gli elementi di clausole che siano stati oggetti di trattativa individuale

In questo comma si esplicita il (fino a prova contraria) dell'articolo precedente. L'imprenditore deve dimostrare che ci sia stata una trattativa specifica.

Esempio: Vendita che ha per oggetto un vecchio utensile medioevale:

1) Dico al cliente che si tratta di un oggetto d'esposizione, e che non va utilizzato, ma viene venduto solo per fine espositivo. Questo accordo è negoziato, tramite mail o con una trattativa comunque documentabile, limitando la mia responsabilità per morte o danno in caso di utilizzo diverso dall'esposizione.
2) Il consumatore non si limita ad esporlo, ma lo utilizza e arreca danno. In prima analisi, ai sensi dell'Art. 33, comma 2, la clausola è da annullare in quanto vessatoria.
3) L' imprenditore però asserisce di aver ben specificato di non usarlo, ma solo di esporlo, posso quindi far valere e non annullare la clausola di esclusione di responsabilità. Ma ciò non basta, serve una trattativa dimostrabile, una prova in cui il venditore e il consumatore acconsentivano a quella clausola, in una specifica discussione di cui esiste traccia, da portare come prova in giudizio.

Articolo 35 - Codice del Consumo: Forma ed interpretazione
Le clausole vessatorie devono essere sempre redatte in modo chiaro e comprensibile

Articolo 36 - Codice del Consumo: Nullità do protezione
Le clausole considerate vessatorie ai senti degli articoli 33 e 34 sono nulle mentre il contratto rimane valido per il resto.
Il secondo comma dice che: in caso di comprovata trattativa sono da considerare nulle le clausole che:

- ✓ Abbiano come effetto limitare la responsabilità dell'impresa in caso di morte;
- ✓ Anche in mancanza di adempimento da parte dell'impresa (per esempio consegnare il bene) negano al consumatore il potere di agire in giudizio;
- ✓ Prevedono l'estensione dell'adesione del consumatore a clausole che non ha potuto conoscere (allegare al contratto visibile uno celato).

Questo comma ha come scopo la tutela del consumatore incauto che, nonostante comprovata trattativa, accetta comunque le clausole vessatorie qui elencate, che sono di comprovato squilibrio e quindi in nessun caso valide.

Infine, il terzo comma stabilisce che la nullità di una clausola è un diritto unilaterale che va solo a vantaggio del consumatore.

- Riassumendo:

- ✓ Primo Livello **(Art 33, comma 1)**: Clausole vessatorie quelle in cui il consumatore riesce a dimostrare **uno squilibrio** ai suoi danni;
- ✓ Secondo Livello **(Art 33, comma 2 e Art 34, comma 4):** Esiste una lista di clausole che si **presumono pericolose** a priori, per le quali però l'imprenditore può liberarsi dalla presunzione dimostrando che le ha specificatamente trattate con il consumatore;
- ✓ Terzo Livello **(Art 36, comma 2):** lista di clausole che nonostante la trattativa dimostrata, vanno **sempre considerate vessatorie**.

Clausole vessatorie nei contratti B2B (Codice Civile):

Articolo 1341 - Codice Civile: Condizioni generali di contratto

Le condizioni generali di contratto predisposte da uno dei contraenti sono efficaci nei confronti dell'altro, se al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle usando l'ordinaria diligenza.

In ogni caso non hanno effetto, se non sono specificamente approvate per iscritto, le condizioni che stabiliscono, a favore di colui che le ha predisposte, limitazioni di responsabilità, facoltà di recedere dal contratto o di sospenderne l'esecuzione, ovvero sanciscono a carico dell'altro contraente decadenze, limitazioni alla facoltà di opporre eccezioni, restrizioni alla libertà contrattuale nei rapporti coi terzi, tacita proroga o rinnovazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziaria.

Esempio: Se un contratto ha una clausola vessatoria, avremo due click: uno per concludere il contratto e un'altra per accettare le clausole vessatorie.

CONTRATTI B2B a distanza

Fonti:

- Codice Civile (essendo del 1942, si parla di contratti in generale, non nello specifico verso i consumatori o le aziende)
- Trattati e Convenzioni internazionali
- Decreto legislativo 70/2003 (Obblighi informativi)

Diritto di recesso nei contratti a distanza B2B:

Non si applicano le norme sul recesso tipiche dei contratti B2C (definiti nel codice del consumo), ma si può negoziare liberamente senza limiti, imposizioni o restrizioni, sia nella durata che nelle modalità. Il recesso negoziato può essere reciproco o unilaterale.

Può avere qualsiasi durata, di 1 giorno come di 100. Se non lo si negozia, non sarà possibile recedere dal contratto.

Il **recesso** si distingue dalla **risoluzione**, che invece avviene a seguito di un inadempimento da parte di una delle due parti, quindi se accade la parte che non lo ha compiuto, può risolvere il contratto, sciogliendo quindi il vincolo contrattuale.

Secondo la **1341, comma 2 c.c.** se una clausola crea squilibrio può essere considerata nulla, se non la si è fatta firmare specificatamente. La vessatorietà si decide caso per caso, in relazione alla situazione concreta.

Legge applicabile:
Regolamento Roma4 (Regolamento (CE) 593/2008): quando le parti sono in situazione di parità contrattuale (B2B) la legge applicabile è la legge scelta dalle parti. Se non indicata il regolamento prevede che sia applicata la legge del Paese che presenta il collegamento più stretto con il contratto. Per esempio nel caso di una fornitura di computer, la prestazione caratteristica è la produzione del bene, quindi si applicherà la legge del paese del produttore.

Quando ci sono più di due soggetti in un contratto e nasce una controversia, verrà valutata a seconda dei due soggetti in lite qual è la prestazione caratteristica.

Foro di competenza: Il discorso è molto complesso, nel nostro caso possiamo semplificare considerando che nei contratti B2B può essere scelto dalle parti (con doppia sottoscrizione per sicurezza) o generalmente risulta essere il foro della parte che NON inizia il giudizio (il convenuto).

[Per esame: Contratti B2C: definizione di contratto, conclusione contratto, difficoltà dei contratti a distanza. Norme, tutele, diritto informativo, recesso, norme vessatorie e norme su foro competente].

Privacy

Privacy: è il diritto alla riservatezza delle informazioni personali e della propria vita privata.
È un diritto stabilito anche a livello europeo dalla **Carta Europea dei Diritti dell'Uomo (CEDU)**.
Ci sono due "anime" del concetto di privacy:

1) **Diritto alla riservatezza**: Diritto di escludere gli altri dall'accesso a dei dati che riguardano la mia sfera intima esempio: usanze religiose, dati patrimoniali, dati di salute, cartella clinica, in pratica si considera che la propria vita privata sia paragonabile ad una proprietà e come tale abbiamo il diritto di escluderne gli altri. Il diritto alla riservatezza è un diritto proprietario esiste dagli ultimi anni del 1800, quando è sorta la necessità di escludere gli altri dalla propria vita privata. (Nascita della proprietà privata).
2) **Diritto alla protezione dei dati personali:** è un diritto attivo, non si basa sul principio di esclusione, ma su un diritto di controllo, anche in maniera operativa. Ha come oggetto l'informazione, il dato che riguarda il soggetto, è un diritto che si dice che è "positivo" in quanto si ha il controllo dei dati che al giorno d'oggi hanno una forte potenza economica, molto più rispetto ai tempi passati: l'utilizzo di questi dati su larga scala avviene per finalità macro-commerciali, come la profilazione. Per dati personali si intende tutti i dati che mi

riguardano, esempio: quale corso frequento all'Università, se ho cercato un viaggio alle Maldive oppure quante sorelle ho.

Questi due diritti sono disciplinate da diverse fonti normative:
In ordine di importanza, si parte dalla Carta di Nizza, conosciuta come **Carta dei diritti fondamentali dell'Unione Europea (CDFUE)** da non confondere con la sopracitata **Carta Europea dei Diritti dell'Uomo (CEDU).**
È l'insieme dei principi e dei diritti che sono ritenuti fondamentali tra accordi tra stati dell'Unione Europea (un po' come se fosse la costituzione dell'UE).
Maggiori info: Carta dei diritti fondamentali dell'Unione europea (unibo.it)
Gli articoli 7 e 8 trattano della privacy.
L'articolo 7 tratta della riservatezza, mentre l'articolo 8 è il diritto alla protezione dei dati personali.
Entrambi gli articoli fanno parte del Titolo II chiamato "libertà"

Articolo 7 - CDFUE: *Rispetto della vita privata e della vita familiare (ovvero diritto alla riservatezza)*
Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Articolo 8 - CDFUE: Protezione dei dati di carattere personale
1. Ogni persona 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 persona 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. (Garante)*

Analizziamo il comma 3:
Il garante è una persona fisica che rappresenta un'autorità amministrativa indipendente dal governo che ha il compito di verificare che il trattamento dei dati personali sia correttamente svolto, in caso contrario può applicare sanzioni amministrative, tramite ispezioni effettuate anche con il supporto della Guardia di Finanza. La sanzione amministrativa per un illecito trattamento di dati può arrivare fino a 20 milioni di euro, oppure fino al 4% del fatturato annuo se superiore ai 20 milioni (Art. 83 GDPR). Ogni garante viene eletto ogni sette anni. Ogni stato ne ha uno.

Regolamento Privacy 679 del 2016 GDPR (General Data Protection Regulation)

In quanto regolamento Europeo si trova gerarchicamente al di sopra delle nostre leggi, è uguale per tutti gli stati membri ed è direttamente applicabile.

In Cina e in America la protezione del dato personale ha caratteristiche completamente diverse e le norme sono molto meno rigide di quelle Europee (per esempio in America non è considerato un diritto costituzionale, mentre in Cina vale meno ancora). Il Regolamento è applicabile per tutte quelle aziende che trattano dati di europei, anche se non sono europee. È nato dall'esigenza di una maggiore unificazione delle norme a livello europeo sul trattamento dei dati.

I due anni di tempo tra l'adozione (2016) e l'entrata in vigore (maggio 2018) sono serviti per dare il tempo agli stati nazionali di adattare le loro normative al GDPR. Per la prima volta questo diritto è gestito a livello europeo. Il nostro Codice Privacy (D.Lgs 196/2003 - Codice Privacy), che discende da una direttiva Europea chiamata direttiva madre sul trattamento dei dati personali), che è stato in vigore fino al 25 maggio 2018, ora è diventato una norma molto frammentata, fatta di articoli abrogati, modificati e aggiunti, che serve esclusivamente a riempiere i vuoti non trattati dal regolamento (come disciplinare i reati e sanzioni amministrative supplementari). Il codice diventa quindi una sorta di legge d'armonizzazione, tra la normativa esistente e il regolamento adottato.
Molti altri Stati Europei hanno utilizzato questa stessa formula.
Questo "nuovo" Codice Privacy è stato adottato solo ad Agosto 2018, creando quindi in Italia un vuoto normativo di circa 2 mesi che ha creato non pochi problemi nella gestione dei dati personali.
Sul sito del Garante è presente la versione del Codice Privacy con evidenziate tutte le modifiche.
La scelta, opinabile, di non creare un nuovo decreto e modificare quello vecchio è stata fatta semplicemente per non modificare il numero della legge di riferimento.

Maggiori info:
REGOLAMENTO (UE) 2016/ 679
Vediamo ora gli articoli più importanti:

Articolo 1 - GDPR: *Oggetto e finalità*

1. *Il presente regolamento stabilisce norme relative alla protezione delle **persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla **libera circolazione** di tali dati.*
2. *Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali*
3. *La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*

Non vale per le persone giuridiche (ovvero le imprese). È una novità rispetto al vecchio Codice Privacy. Applicare il regolamento per le imprese è un costo. Quindi il fatto che sia limitato alle sole persone fisiche e non alle persone giuridiche è un vantaggio economico per le aziende.

È regolamentato sia il dato in sé, che la sua circolazione. La **segretezza** e la **protezione del dato personale** sono due cose diverse: il dato può e deve circolare: è necessaria la sua circolazione per motivi culturali, sociologici, economici, scientifici. Il sistema, quindi, non è ermeticamente chiuso, ma bilanciato tra la protezione dei dati personali e la necessita della società civile moderna di farli circolare.

Articolo 2 - GDPR: *Ambito di applicazione materiale*

1) Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

2) Il presente regolamento non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

3) Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98.

4) Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

L'articolo 2 del GDPR non si applica sono online, ma anche nella vita reale.
Esempio: Devo raccogliere delle firme.

Articolo 3 - GDPR: *Ambito di applicazione territoriale*

1) Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

2) Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

3) Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Titolare: azienda che sta facendo il trattamento dei dati.

Se il titolare è stabilito nell'unione europea, qualsiasi trattamento di dati che faccia è soggetto ai GDPR anche se il trattamento è decentralizzato dall'UE.

https://it.wikipedia.org/wiki/Sentenze_Schrems

Articolo 4 - GDPR: *Definizioni*

1) *«dato personale»:* ***qualsiasi informazione*** *riguardante* ***una persona fisica identificata o identificabile*** *(«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*

È considerato anche il singolo dato, non solo il flusso di dati. Con l'aggettivo "identificabile" la sfera del dato personale si estende enormemente, perché qualsiasi dato potrebbe identificare in maniera diretta una persona.

Anche un dato senza alcun riferimento al soggetto, ma che permetta indirettamente l'identificazione, per esempio tramite l'incrocio di altri dati, diventa comunque un dato personale a tutti gli effetti. Quindi il dato personale è un concetto dinamico, che va sempre riferito al contesto, nel senso che anche se un'informazione isolata non è in grado di portare all'identificazione di un individuo, il fatto che detta informazione possa essere utilizzata per l'identificazione tramite incrocio con altri dati ne determina comunque la natura di dato personale.

La differenza tra dato personale e il suo opposto, ovvero il **dato anonimo**, cambia a seconda del numero di soggetti che formano il campione a cui ci riferiamo. Per esempio "avere i capelli rossi" può essere o non essere dato personale, la situazione varia molto a seconda del contesto: la classe universitaria, l'università, il comune di Bologna, tutta la nazione. In questo caso si parla di approccio relativistico, quando il dato è personale o anonimo non in base al dato in sé, ma in base al contesto.

Questo concetto di relativismo è stato oggetto di discussione da parte del "Gruppo Articolo 29", formato da tutti i garanti europei, che ha redatto un parere volto ad interpretare meglio la definizione di dato personale in un contesto mutevole: **andrà considerato personale, il dato verso il quale c'è un interesse economico tale, da giustificarne il trattamento.**

Il dato può essere considerato anonimo, solo quando lo sforzo da sostenere per l'identificazione del soggetto non è più economicamente conveniente.

"Qualsiasi informazione" significa anche che il formato (scritto, audio, video, etc.) nel quale sono conservati i dati è irrilevante al fine dell'applicabilità della tutela dei dati personali.

Tale principio si applica a tutti i dati, ad esclusione dei dati anonimi e dei dati che si riferiscono a persone giuridiche.

Obiettivo di molte aziende è riuscire a rendere completamente anonimi i dati personali, in modo da poterli liberamente trattare senza l'obbligo di aggiungere costi di gestione per l'applicazione del regolamento.

Ogni tipo di operazione compiuta sul dato è soggetta al Regolamento Privacy, ad esempio anche il ritrovamento di un documento d'identità per strada, la sua visione, al solo scopo di rintracciarne il proprietario è un trattamento soggetto alle regole del GDPR.

Il ***dato personale*** è qualsiasi dato renda rende identificabile una persona fisica, non una giuridica.

Un dato può essere personale o meno a seconda del contesto.

Esempio: Se dico "il ragazzo con la maglietta nera ha detto una cosa sbagliata" non sto dando un dato personale, perché è generico. Se però dico "il ragazzo con la maglietta nera che si chiamava Dario Berardi ha detto una cosa sbagliata" il dato allora diventa personale.

Colleghiamoci un attimo alla regola 26:

26) "È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca"

Online è sempre possibile risalire ad una persona, ciò vuol dire che qualsiasi dato sia a me riferibile che venga acquisito telematicamente è sempre un dato personale? NO,

Leggendo il 26, c'è un criterio di ragionevolezza, perché anche se in modo astratto posso ricondurre dei dati ad una persona, se questo processo avesse un costo eccessivo e sarebbe difficile secondo le tecnologie di cui dispongo quel dato per me sarebbe anonimo e posso non rispettare il regolamento, facendone un uso anonimo anche al di fuori.

I principi di protezione dei dati non dovrebbero venire applicati a dati anonimi, se faccio un sondaggio e chiedo quanti studenti iscritti al corso sono fuorisede o no ma non mi segno nessun dato quelli sono dati anonimi(?), se li segno perché voglio ricordarmi quanti uomini o donne hanno risposto e mi segno i nomi, SOLO i nomi di battesimo non sono personali, se invece numero le

persone che mi rispondono e ho un altro elenco a cui il numero corrisponde un criterio per identificare la persona in modo univoco (se avessimo per esempio il Nome e il Cognome) allora i dati che ho raccolto NON sono più anonimi ma diventano dati personali.

Separare l'informazione dalla persona che me l'ha data (come se fossero due pezzi di puzzle separati), è un'operazione molto frequente al giorno d'oggi, che nonostante non rende anonimo il dato, esso è molto più sicuro. Per questo motivo questa tecnica viene utilizzata quando si vuole avere più sicurezza. Questo viene chiamata **pseudonimizzazione** dei dati.

La pseudonimizzazione è una tecnica che consiste nel trattamento dei dati personali in modo tale che non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive.

L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati.

Torniamo a parlare dell'articolo 4, in particolare del comma 4

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Profilazione: (al centro del dibattito quando si parla di trattamento di dati personali, principalmente dalle grandi aziende del web) è una qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

La società Cambridge Analytics si occupava di profilazione.

Quando dobbiamo verificare se un trattamento è lecito o illecito, possiamo farlo tramite 2 variabili: QUANDO e COME è stato fatto

L'articolo 5 - GDPR: Disciplina i principi del trattamento ovvero **come** deve essere fatto un trattamento dei dati personali
L'articolo 6 - GDPR: Ci dice **quando** può essere, mediante le condizioni di liceità in base a quale base giuridica è stato fatto.

***Articolo 5 - GDPR**: Principi applicabili al trattamento di dati personali*

1a) Principio di liceità, correttezza e trasparenza: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato

1b)Principio di limitazione della finalità: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali.

1c) Principio di minimizzazione dei dati: Il titolare del trattamento deve utilizzare i dati racconto solo nei limiti del raggiungimento dello scopo per i quali sono stati richiesti.

1d) Principio di esattezza: I dati inseriti rispetto alle finalità del trattamento devono essere eliminati o rettificati tempestivamente, senza ritardi.

1e) Principio limitazione della conservazione: è strettamente collegato al principio di minimizzazione, il titolare dovrebbe conservare i dati solo per il periodo in cui è necessario che li conservi.

1f) Principio di integrità e riservatezza: i dati devono essere trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate.

2) Principio di responsabilizzazione (Accountability): Il principio di accountability stabilisce che **è responsabilità del titolare** scegliere qual è la **misura di sicurezza più adeguata** a proteggere il dato che sta trattando. Non sono uguali da azienda ad azienda, ma sono diverse. Per questo motivo è un principio che consente di valutare caso per caso. Inoltre stabilisce che il titolare ha **l'onere di essere in grado di provare di aver adottato quella specifica misura**. Quindi il trattamento del dato personale deve essere tracciato: per esempio inserendo le modalità di trattamento e le misure precauzionali all'interno del documento di designazione o di un documento chiamato "Registro dei Trattamenti", obbligatorio per tutte le società che trattano dati personali. Tale registro, redatto dal titolare e dai responsabili esterni, contiene le caratteristiche e le metodologie dei singoli trattamenti. Il principio di responsabilizzazione è rischioso in caso di **Data Breach** (violazione dei dati personali).

Articolo 6 - GDPR: *Liceità del trattamento*

Comma 1: Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

1A) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (*per un trattamento lecito bisogna fornire un'adeguata informativa (obbligatoria per tutti coloro che trattano dati personali) e ottenere un esplicito consenso per specifiche finalità. Generalmente serve una firma per ogni finalità.*)

Ci sono alcuni casi, previsti sempre dall'Articolo 6, comma 1, per cui è previsto che il trattamento sia lecito anche **in assenza di un consenso**:

*1B) Il trattamento è lecito **se necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (comma 1, lett. b);*

Significa che non c'è bisogno di richiedere un consenso se il trattamento dei dati personali è strettamente finalizzato alla pura esecuzione di un contratto che ho sottoscritto: resta implicito il fatto che se accetto un contratto, accetto anche che vengano trattati i miei dati personali ai fini contrattuali, nelle modalità descritte dall'informativa, che resta obbligatoria.

*1C) Il trattamento è lecito se è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento (comma 1, lett. c);*

Per esempio, la comunicazione agli organi preposti di alcuni dati finanziari dei clienti per scopi di antiriciclaggio, in quanto previsti e obbligatori nel rispetto di una normativa vigente.

*1D) il trattamento è necessario per la salvaguardia degli **interessi vitali** dell'interessato o di un'altra persona fisica (comma 1, lett. d);*

*1E) il trattamento è necessario per l'esecuzione di un compito di **interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (comma 1, lett. e);*

Per esempio, nell'esercizio del diritto di cronaca (o di stampa), per motivi di comprovata sicurezza pubblica, per motivi d'istruzione, per finalità di cura o per finalità di ricerca. I casi per valutare l'eventuale interesse pubblico sono previsti dalla normativa, più specificatamente nel codice privacy, art. 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante).

Ma tutti i dati sono uguali? NO, infatti oltre al dato personale, ci sono altre categorie particolari di dati chiamati dati sensibili che sono trattati nell'articolo 9.

Articolo 7 - GDPR: *Condizioni per il consenso*

Prima di parlare dell'articolo in sé va fatta qualche precisazione e data qualche nozione/definizione:

L'interessato o soggetto è la persona fisica a cui sono riferiti i dati. Il concetto di proprietà, si sposa male con la proprietà di dati perché la proprietà per definizione come concetto nostro giuridico contiene tra le facoltà il fatto che è esclusiva.

Il titolare del trattamento è (per esempio Facebook), chi è in carica per quel trattamento dei dati. La persona fisica che determina la finalità dei mezzi del trattamento dei dati personali. Per esempio, io ho un negozio di libri S.r.l., che fa un sondaggio per sapere se vogliamo ricevere delle informazioni. Questi vengono raccolti in una lista per fare pubblicità darle ad altre aziende. Il titolare di questa

attività è libreria S.r.l. che ha reagito tramite il suo legale rappresentate. Il titolare del trattamento può essere una persona fisica o giuridica, considerato “il capo” del trattamento dei dati, quello che ne determina la finalità, come in questo caso per marketing.

Il titolare del trattamento va distinto con il responsabile del trattamento. Il titolare del trattamento non svolge materialmente lui le operazioni di trattamento, almeno non tutte. Quasi sempre viene nominato infatti un responsabile esterno (possono essere anche aziende esterne) che si occupano del trattamento dei dati. «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

L'incaricato è la persona fisica che materialmente svolge il trattamento dei dati personali, che può essere una persona fisica o un’organizzazione.

Quando faremo un esame orale, i prof che ci ascoltano compilano un verbale, che è una raccolta dei dati personali. Chi lo farà è una persona autorizzata da parte dell’università che è il titolare di quel trattamento dei dati personali, la cui finalità è quella per lo svolgimento dell’esame.

Data breach: la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità, - la divulgazione non autorizzata dei dati personali.

La nomina degli incaricati deve essere fatta per iscritto. Questa è una classica cosa per la quale quando viene la guardia di finanza e ci fa i controlli, ci chiede se sono stati trascritti da qualche parte.

Adesso torniamo a parlare dell’articolo 7 nello specifico:

1) Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Impone al titolare del trattamento la conservazione dell’informazione, dei log che dimostrano che c’è stato un effettivo consenso (o la registrazione audio, o il foglio firmato), per un’eventuale fase patologica successiva.
Il regolamento non specifica mai la forma del consenso, che può essere di qualunque genere, specifica solo che il titolare ha obbligo di dimostrare che ci sia stato.

2) Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

Modulo di consenso legittimo: Indicare la finalità di trattamento. Indicare entrambe le alternative, in maniera chiara, visibile ed equiparabile a livello grafico. Non è possibile che la casella del consenso sia "pre-cliccata": l'unica opzione "pre-cliccabile" è quella meno invasiva per l'interessato, ovvero quella di negare il consenso di default.

3) L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

La revoca può essere fatta in ogni momento e con semplice modalità. Se per concedere il consenso si è semplicemente cliccato una casella online, il prestatore non potrà chiedere una raccomandata per effettuare la revoca, quindi con un metodo più oneroso e complicato di quello utilizzato per il consenso.

4) Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Se l'interessato viene obbligato ad esprimere il consenso come condizione vincolante per l'esecuzione di un contratto, anche per quei dati che non sono necessari all'esecuzione del contratto, andrà considerata come una **forzatura** e quindi il consenso non potrà essere considerato libero. Alcune piattaforme online (come Facebook), hanno applicato il GDPR chiedendo ai loro utenti il consenso al trattamento dei loro dati personali, specificando però che in assenza del consenso non potranno più usufruire dei servizi forniti. In pratica si tratta di "prendere o lasciare" ("*take it or leave it*"). Tale comportamento è in fase di valutazione anche a seguito di una denuncia di un'attivista austriaco, Max Schrems.

Invece, nel caso in cui i dati personali siano strettamente necessari per eseguire un contratto non è necessario il consenso, ma resta obbligatoria l'informativa.

Quando si esprime un consenso si sta esercitando un diritto di controllo sui propri dati personali. Il diritto alla protezione del dato personale è un diritto della personalità, ovvero che appartiene a ciascun individuo in quanto essere umano, è così importante che non può essere negato a nessuno, al pari del diritto alla salute, alla vita, etc.
Essere forzati a rinunciare ad un diritto della personalità, è sempre considerato un illecito.

L'accettazione dell'informativa è diversa dall'espressione del consenso. Quando il trattamento dei dati è necessario all'esecuzione del servizio, l'accettazione dell'informativa ha lo scopo di dimostrare, a posteriori in giudizio, che è stata fornita l'informativa all'interessato.

Un consenso può essere considerato **legittimo** solo se è:

- ✓ **LIBERO** (Atto volontario, senza costrizioni, condizionamenti, minacce (minaccia di un dato ingiusto). Se è libero o meno di accettare.)

- ✓ **INFORMATO** (serve informativa e L'interessato deve essere stato informato sulle caratteristiche del trattamento su cui presta il consenso, ovvero deve aver preso visione dell'informativa)
- ✓ **REVOCABILE**
- ✓ **SPECIFICO** (È un consenso per una specifica finalità. Se aggiungo una finalità diversa a quel trattamento devo chiedere il consenso)

Cosa accade se il consenso non è legittimo? Per esempio, nella richiesta di un consenso senza aver fornito l'informativa, o non libero, o non specifico (per esempio richiedendo il consenso per tutti i dati personali del soggetto)?
Il prestatore sta trattando i dati personali in maniera illecita e quindi è soggetto a possibili sanzioni penali, civile e amministrative (**fino a 20 milioni di euro o 4% del fatturato mondiale se superiore**).
Le sanzioni vengono combinate dai singoli garanti dei singoli Stati membri e da loro raccolte nelle casse dello Stato, metà delle quali viene utilizzato per garantire il corretto funzionamento degli organismi di garanzia, quindi a finalizzare le attività del Garante.
Il Garante ha totale autonomia nell'effettuare controlli, anche senza la denuncia del diretto interessato.

Inoltre, il consenso **non può essere retroattivo**: se si trattassero dati personali prima di chiedere un consenso, anche se venisse fornito successivamente, non sarebbe un trattamento legittimo.

Opt-in: richiesta di consenso preventiva per il trattamento dei dati.
Opt-out: trattamento dei dati a cui solo in un secondo momento l'interessato potrà opporsi.

Il metodo **Opt-in** è quello classico e legittimo per il trattamento dei dati per finalità di

marketing. Ci sono due eccezioni per l'utilizzo del metodo **Opt-out** in maniera legittima:

1) Per le comunicazioni di marketing diretto a **mezzo telefonico**. Per opporsi al quale ci si può iscrivere al registro pubblico delle opposizioni.
2) Per le comunicazioni marketing **via Email**, aventi ad oggetto **prodotti simili** a quelli già acquistati in precedenza dall'interessato. Bisognerà specificare che è una comunicazione commerciale, ed inoltre il mittente nella stessa mail, dovrà inserire un link con la possibilità di revoca del consenso per tale tipologia di trattamento.

Se si crea un sito web che offre un servizio andranno forniti i documenti seguenti:

- *"Terms and Conditions"* (chiamato anche condizioni generali di contratto, contratto, accordo tra le parti). L'accettazione di questo documento non è l'espressione di un consenso al trattamento dei dati personali, ma è l'accettazione di un accordo contrattuale;
- *"Informativa"* (ovvero le condizioni del trattamento dei dati personali, dette anche condizioni privacy o privacy policy - deve essere sempre presente);
- *"Modulo del consenso"* (quando necessario), deve essere facilmente distinguibile dal contratto.

Concludendo, per trattare lecitamente i dati personali occorre che vi sia una combinazione tra:

- **Informativa + pura esecuzione contrattuale**

- **Informativa + consenso lecito (Libero, informato, revocabile e specifico)**
- **Informativa + legge (o regolamento) che specifica che la finalità è di interesse pubblico**
- **Informativa + interesse legittimo previsto da normativa (conservazione di documenti per eventuali contenziosi, o comunicazioni previste per legge)**

L'articolo 5 integra alcune caratteristiche per un trattamento lecito, definendo che i dati personali debbano essere:

- Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**«liceità, correttezza e trasparenza»**), ovvero nelle modalità appena descritte e trattate in questi appunti;
- Raccolti per finalità **determinate** (non mutevoli), **esplicite** (quindi che saranno dichiarate nell'informativa) e **legittime** (non illegali). In caso di modifica delle finalità, andrà richiesto un nuovo consenso;
- **adeguati**, **pertinenti** e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);
- **esatti**, se necessario, aggiornati; andranno adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**«limitazione della conservazione»**);
- trattati in maniera da garantire un'adeguata **sicurezza dei dati personali**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale («**integrità e riservatezza**»).

Come già discusso, se l'interessato è un **soggetto minore**, ovvero che in Italia non ha raggiunto i 18 anni, non ha la capacità di agire legalmente. Il regolamento europeo specifica che il minore può esprimere lecitamente il consenso al trattamento dei propri dati personali (solo online) se ha almeno 13 anni. Essendo l'argomento delicato, il Regolamento delega allo Stato membro la decisione finale per la definizione dell'età minima per l'espressione di un lecito consenso. L'Italia ha scelto come **età minima i 14 anni**. La scelta è stata fatta poiché alcuni gravi reati, possono generare la condanna dei soggetti implicati fin dai 14 anni.
È molto complicato per i provider riconoscere se il soggetto ha più di 14 anni, proprio per la natura intrinseca di Internet. Alcuni metodi usati dai provider per diminuire questo rischio, sono la richiesta di un'autodichiarazione o la richiesta di una copia del proprio documento d'identità.

I soggetti ATTIVI nel trattamento dei dati personali (definizioni in Art. 4):

- **Titolare**: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.*

Ovvero è colui che decide le finalità, che scrive l'informativa ed elabora le misure di sicurezza per il trattamento. Sono i soggetti che rispondono sempre giuridicamente verso l'esterno in caso di problematiche.

- **Responsabile**: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.* (Rispondono verso l'esterno solo quando non hanno adempiuto agli obblighi imposti dal titolare per trattamento dei dati)

- I **Soggetti autorizzati** a trattare i dati (dal Titolare o dal Responsabile).

  Non rispondono direttamente di eventuali illeciti di trattamento, ma il titolare potrà agire "in regresso", ovvero internamente, contro di loro. All'interno dell'azienda è buona abitudine avere designato tutte queste figure che trattano i dati personali, con quali dettagli ed in che modo. Ciò consente al titolare di avere una mappa delle responsabilità da presentare anche in caso di verifiche ispettive.

- **L'atto di designazione**: specifica quali saranno i dati che il destinatario potrà trattare, come e con quali finalità.

È una catena di responsabilità: in caso di problematiche sul trattamento, come una fuga di notizie, l'unico primo responsabile è sempre il titolare. Egli potrà rifarsi sulla persona autorizzata al trattamento in un secondo momento, ma per tutti i soggetti esterni all'azienda lui è l'unico responsabile.

Es. Come fa il titolare a mantenere il controllo sui dati comunicati al commercialista che riguardano i suoi clienti? Farà firmare un contratto di designazione simile a quello stipulato all'interno della sua azienda con le persone autorizzate, con il responsabile esterno del trattamento (il commercialista). Il contratto riporterà i dati trattati, le responsabilità, le finalità, le modalità.
Anche in questo caso, l'unico responsabile verso l'interessato resta solo e soltanto il titolare.

È convenzione far firmare il contratto di designazione per il trattamento dei dati personali ai soggetti esterni in concomitanza con la firma del contratto di fornitura del servizio che il soggetto esterno dovrà erogare. Allegati del contratto: designazione a responsabile esterno al trattamento.

Esternalizzazione dati personali in maniera legittima. Ad esempio, una struttura ospedaliera che volesse donare tutti i propri dati per fini di ricerca all'università, ha diverse alternative:

1: Designare l'università come responsabile esterno (ma sarà sempre l'ospedale che risponderà nei confronti dei terzi);
2: Richiesta del consenso a tutti gli interessati (soluzione estremamente impegnativa);
3: Anonimizzazione dei dati;

4: Designo l'università come co-titolare (autorizzato preventivamente in informativa);

Data Protection Officer (DPO): è un soggetto che fa da controparte al titolare, ovvero agisce come se fosse il punto di riferimento del Garante nell'ambito della struttura del titolare. Deve essere nominato obbligatoriamente in alcuni casi specifici, elencati nell' **Art. 37**: se il trattamento è effettuato da **autorità pubblica** (Università, Comune, Ospedale, etc.), o quando vi è un'attività di trattamento che implica il **monitoraggio sistematico** degli interessati (es. videosorveglianza, sistemi di profilazione), o ancora nel caso in cui siano trattati **particolari categorie di dati**, ovvero quelli che in passato erano chiamati "dati sensibili" (orientamento politico, sessuale, religioso, lo stato di salute, le caratteristiche psicofisiche, etc.).
Il compito principale del Data Protection Officer è di vigilare e di verificare che il titolare adempia correttamente a tutti gli obblighi previsti dalla legge, anche partecipando per esempio alle riunioni fondamentali in maniera di privacy, verificando che le informative siano scritte e fornite correttamente, rendendo disponibili i documenti al Garante in caso di richiesta.
È una figura di garanzia, a tutela degli interessati, all'interno delle realtà aziendali. Può essere un soggetto esterno o può anche fare parte dell'azienda stessa, deve avere una comprovata indipendenza e autorità, poiché nel caso rilevasse problematiche nel trattamento, dovrà essere in grado di opporsi alle decisioni del titolare e di dichiarare il fatto al Consiglio di Amministrazione (dichiarazione di contrarietà della conformità, che quindi resta agli atti).
La designazione, dove non prevista obbligatoriamente per Legge, è comunque raccomandabile, o perlomeno da valutare in termini di costi/benefici. Va valutata attentamente l'eventuale conflitto d'interessi: il DPO non può essere un dipendente dell'azienda, che ha altre funzioni e obiettivi, o per esempio non può essere colui che in passato ha redatto le informative o definito le metodologie in materia privacy all'interno della società.

Articolo 8 - GDPR: *Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione:*

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno **16 anni**. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

   Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.
2. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.
3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

In tutta l'Europa, il trattamento dei dati personali da parte dei Social Network, è lecito, ove il minore abbia almeno 16 anni, se l'età dovesse essere inferiore, il trattamento sarà lecito solo se un tutore ha dato l'autorizzazione.

Dopo i 16 anni di età, le regole variano a seconda degli stati membri.

Come si fa a dimostrare che chi conclude il contratto è maggiorenne? Bisogna avere una dimostrazione per rendere il contratto valido.

Articolo 9 – GDPR: *Trattamento di categorie particolari di dati personali:* ci dice che i dati particolari (una volta denominati sensibili), non devono essere trattati salvo il consenso ESPLICITO dell'interessato. I dati particolari sono:

- L'origine razziale o etnica
- Le opinioni politiche, convinzioni religiose o filosofiche
- L'appartenenza sindacale
- I dati genetici e i dati biometrici intesi a indentificare in modo univoco una persona fisica
- I dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

NB: quando si parla di dati personali fa sempre riferimento al GDPR.

Articolo 24 - GDPR: *Responsabilità del titolare del trattamento*
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento è stato effettuato conformemente al regolamento.

Articolo 39- GDPR: *Compiti del responsabile della protezione dei dati*
1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

L'articolo 13 tratta invece le condizioni per scrivere un'informativa sulla privacy corretta

Articolo 13 – GDPR: *Informazioni fa fornire qualora i dati personali siano raccolti presso l'interessato*

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) L'identità e i dati di contatto del titolare del trattamento
b) I dati di contatto del responsabile della protezione dei dati
c) Finalità del trattamento
d) Interessi perseguiti dal titolare del trattamento o da terzi
e) Destinatari o categorie di destinatari dei dati
f) L'intenzione del titolare tra trattamento di trasferirei dati personali in un altro paese o ad un'altra organizzazione internazionale

Una volta che do il consenso al trattamento dei miei dati, quali diritti mi rimangono su quei dati?

Diritto all' accesso: Diritto da parte dell'interessato a richiedere informazioni al titolare riguardo ai dati personali che sta trattando. Se i dati sono trattati lecitamente, tutte le informazioni sul trattamento dovrebbero essere state già fornite all'interessato.

Articolo 15 – GDPR: *Diritto all'accesso dell'interessato*

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sua o meno in corso un trattamento di dati personali che lo riguardano, e in tal caso di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) Finalità del trattamento
b) Categorie di dati trattati
c) Destinatari o categorie di destinatari
d) Periodo di conservazione dei dati
e) La possibilità di richiedere la rettifica, la cancellazione dei dati, la limitazione del trattamento o l'opposizione al trattamento
f) Diritto di reclamo a un'autorità di controllo

…

In particolare, la novità introdotta dall'articolo 15 comma 3 è che il titolare del trattamento è tenuto a fornire una copia di tutti i dati personali oggetto di trattamento.

1) Modalità di trattamento (informativa)

2) Elenco di tutti i dati che il titolare sta trattando sul conto dell'interessato

Il diritto di accesso rappresenta, proprio per il potere che conferisce all'utente, una "porta aperta" sull'operato del titolare del trattamento, riconoscendo, ad ogni persona fisica, la possibilità di controllare nel tempo le tracce lasciate dai propri dati e di intervenire, eventualmente, per cambiare le cose. Quando utilizziamo i social network, abbiamo la possibilità di scaricare per intero tutti i dati in possesso di quel titolare (es. Facebook, Instagram ecc.) che è collegato al diritto alla rettifica dei dati.

Articolo 16 – GDPR: *Diritto alla rettifica dei dati*

Trattato dall'Art. 16 del GDPR: l'interessato può richiedere la correzione dei dati errati. Prima delle leggi sulla privacy era molto complicato ottenere questo diritto, infatti era necessario dimostrare che tale informazione ledeva la propria immagine. Il titolare del trattamento è obbligato, a proprie spese, a rettificare i dati senza ingiustificato ritardo.

Articolo 20 – GDPR: *Diritto alla portabilità dei dati*

È il diritto di portare i miei dati da una azienda ad un'altra.

Esempio: Sono un venditore che vuole cambiare fornitore, tutti i miei dati personali che ha collezionato il mio vecchio fornitore voglio che siano trasferiti al nuovo significa che il primo fornitore non può chiedermi nessuna somma di denaro, nessuna opposizione se io voglio fare il trasferimento dei dati.

Tale diritto può essere applicato solo se il trattamento avviene sulla base di un consenso scritto.

In passato per motivi commerciali e di marketing non veniva data la possibilità di trasferire le informazioni tra diversi sistemi informativi (tecnica del *"lock-in"*), obbligando l'interessato a rimanere fedele al marchio o a dover trasferire manualmente tutte le sue informazioni.

Dal punto di vista della protezione dei dati personali questa mancanza di flusso è un limite all'esercizio del diritto alla portabilità dei dati personali, ora riconosciuto dal regolamento tramite l'Art. 20.

Articolo 21 – GDPR: *Diritto di Opposizione*

L'opposizione al trattamento è un diritto che può essere esercitato in qualsiasi momento, ci sono tre tipologie di diritto di opposizione:

- Trattamenti per scopi di pubblico interesse o per legittimo interesse
- Opposizione ai trattamenti di marketing
- È quello i trattamenti per finalità storiche, scientifiche statistiche

Diritto all'oblio: Nasce in Italia, intorno agli anni '90. Viene aperta un'indagine sui fatti che coinvolgono un politico per un presunto reato. Alla fine del processo, viene assolto perché il fatto non sussiste. Qualche anno dopo si presenta per le elezioni, ma nei primi risultati sui principali motori di ricerca al suo nome è associata la notizia dell'apertura delle indagini e non quello della chiusura con assoluzione piena. Il politico agisce in giudizio in quanto considera che questo sia un grave danno alla propria reputazione, anche in vista del suo interesse nel ricandidarsi. In primo e in secondo grado i giudici ritengono che la libertà d'espressione dei giornali prevalga sulla richiesta del politico, nell'ultimo grado di giudizio la sentenza della Cassazione[6] conferma che dagli archivi dei giornali non può essere cancellata la notizia dell'apertura delle indagini, sia perché non si può alterare una realtà storica e sia poiché esiste e va tutelato il diritto di cronaca. Ciononostante, la Cassazione aggiunge che le banche date dei giornali sono obbligate ad aggiungere e rendere facilmente reperibile assieme alla notizia sull'apertura delle indagini, l'informazione dell'assoluzione in formula piena.

In questa prima fase di nascita del diritto all'oblio si configura come uno **strumento non finalizzato alla cancellazione** o rimozione dell'informazione, ma alla sua **contestualizzazione**, quindi ad un'integrazione di dati.

Il diritto all'oblio NON è quindi la possibilità di ottenere la rimozione di notizie «scomode» o «sgradite» dalla pubblica circolazione, di «ripulire» la reputazione macchiata da arresti, condanne o anche solo critiche, **ma è il diritto a salvaguardare la propria identità personale in rete**. La pretesa di ottenere **l'aggiornamento di notizie** che, sia pure in origine corrette, siano potenzialmente lesive in quanto prive di attualità (essendosi ridotto il loro rilievo in termini di pubblico interesse) **non è sufficiente a bilanciare il rapporto tra diritto alla protezione dei dati personali e il diritto alla reputazione dell'interessato**.

Le leggi che regolamentano il diritto all'oblio si applicano esclusivamente alle persone fisiche e non alle aziende.

Articolo 17 – GDPR: *Diritto alla cancellazione (Diritto all'oblio)*
L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali

Questo diritto è soggetto ad alcune condizioni (elencati sempre nel comma 1):

- I dati personali non sono più necessari per le finalità per cui sono stati trattati;
- Se il trattamento fosse basato sul consenso, dopo la revoca del consenso;
- Se il dato fosse trattato in modo illecito;
- Se esistesse una Legge che ne richieda la cancellazione;

Nel comma 3 vengono riportati invece i limiti opposti, ovvero quando un titolare può opporsi alla cancellazione:

- Per l'esercizio del diritto alla **libertà di espressione e di informazione** (va fatto un bilanciamento tra i due diritti);
- In alcuni casi di **interesse pubblico** nel settore della sanità, della ricerca, statistiche, se la richiesta di cancellazione possa anche potenzialmente pregiudicare il conseguimento delle finalità di trattamento;
- Se come titolare sto adempiendo ad un **obbligo legale** (come la conservazione delle fatture, o i registri di un'università) o per esercitare la facoltà di difesa in giudizio (entro i termini di prescrizione).

Nessun'altra scusa può essere utilizzata per rifiutarsi di eliminare i dati personali, sempre che le condizioni della richiesta siano legittime.

Ricapitolando l'articolo 17 del GDPR che si occupa del diritto all'oblio tratta:

- Diritto alla non pubblicazione di notizie passate
- Diritto alla ripubblicazione di notizie passate
- Diritto alla cancellazione di notizie passate

Ci sono alcuni casi dove vengono pubblicati i dati di altre persone senza il consenso, allora chi subisce l'offesa, oltre al diritto all'oblio può farsi ripagare il danno che di tipo morale.

Per ottenere il diritto all'oblio devo fare un reclamo (Disciplinano dall'articolo 77 del DGPR) al garante www.garanteprivacy.it

Il diritto all'oblio solitamente si applica solo alle persone fisiche, ma non esiste una norma che vieti l'applicazione alle persone giuridiche

Curriculum Vitae:
Dal punto di vista legislativo non è più necessario esplicitare il consenso al trattamento dei dati personali all'interno del curriculum, in quanto una recente legge stabilisce che se è l'interessato che invia direttamente il CV ad una azienda, è chiara la finalità d'utilizzo.

Diritti alla personalità

Il ruolo degli Internet Services Provider è fondamentale nella società di oggi in quanto tutte le informazioni transitano nella rete all'intero delle loro infrastrutture.

È perciò necessario conoscere quali sono le loro responsabilità.

*Q*ualora l'illecito o il comportamento dannoso sia commesso direttamente dal *Provider*, la responsabilità non potrà che essere riconosciuta interamente in capo allo stesso. A tal riguardo, è lo stesso **Codice di regolamentazione dell'AIIP** – Associazione Italiana Internet Provider – a statuire che "*il fornitore di contenuti è responsabile delle informazioni che mette a disposizione del pubblico*".

Diverso e più complesso è il caso in cui i comportamenti illeciti siano stati causati degli **dagli utenti** che usufruiscono dei servizi forniti dal *Provider*.

Articolo 2043 – Codice Civile: Responsabilità del provider

È un articolo fondamentale. Chi ha causato un danno ingiusto è obbligato a risarcire.

È, pertanto, necessario comprendere se, nella pubblicazione di contenuti illeciti ad opera di un utente, sia configurabile una condotta, dolosa o colposa, che configuri una responsabilità in capo al *Provider*.

Esempio: diffamo un'azienda e mi vengono richiesti i soldi per i danni ingiusti nei confronti di una cattiva reputazione verso l'azienda.

Questa norma vale sia nell'ambito reale che in quello virtuale.

Articolo 17 - DLGS 70/2003: Assenza dell'obbligo generale di sorveglianza

1. Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto:

a. ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione;
b. a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente.

Primo comma:

Nel primo comma leggiamo che in questo articolo c'è l'assenza di un obbligo di sorveglianza da parte del provider. (Inusuale, non c'è una legge che dice che se passiamo con il verde non prendiamo la multa)

Esempio:

YouTube, per esempio, non è obbligato a sapere preventivamente (fare una verifica) che il contenuto caricato da un utente sia lecito o meno. Vale per qualsiasi cosa, persino per il motore di ricerca.

Ci sono 3 ragioni che hanno portato all'adozione di questa norma:

1. Se qualcuno ci infama su YouTube e io chiedo il risarcimento per il danno, lo chiedo sia a YouTube (provider) che alla persona che mi ha infamato, poiché il risarcimento al provider sarebbe molto più conveniente anziché richiederlo direttamene alla persona che ci diffama (che non garantisce il risarcimento). Da parte dai giudici ci potrebbe essere la tentazione di considerare colpevole il provider.

In parole povere: In caso di diffamazione solo chi ci ha diffamato ci dovrebbe risarcire e non YouTube

2. Se ogni provider avesse una commissione che valutano i contenuti pubblicati, ci sarebbe un blocco di mercato, poiché lo sviluppo tecnologico dei provider sarebbe rallentato. Limitare i costi del provider e favorire lo sviluppo tecnologico.

In parole povere: Limitare i costi del provider

3. Supponiamo che noi siamo un consulente legale di un qualsiasi provider di una qualsiasi piattaforma di memorizzazione e non esistesse questa norma. Riceviamo una segnalazione in cui ci viene detto che un video ha diffamazione nei confronti di una persona. Dovremmo valutare che sia vero valutando che ci sia una valida diffamazione, comparare i due interessi in gioco etc... Nella realtà però se ci arrivasse, lo cancelleremmo e basta, non avrebbe senso valutare video per video se c'è diffamazione o meno. Nessuna piattaforma terrebbe online un video potenzialmente segnalato da diffamazione, l'effetto sarebbe una censura dei video. Quindi lo si fa per evitare la censura di qualsiasi video, altrimenti il provider cancellerebbe il video ogni volta che riceverebbe una segnalazione.

In parole povere: Se arrivasse una segnalazione di possibile diffamazione, servirebbe un controllo manuale che poi porterebbe all'eliminazione sicura del contenuto (perché sarebbe rischioso per il provider mantenere contenuti già segnalati), quindi si creerebbe una storta di censura perché si dovrebbero cancellare innumerevoli contenuti

Secondo comma:

Il prestatore è tenuto ad informare l'autorità giudiziaria se ritiene o viene a conoscenza di attività illecite che si svolgono sulla sua piattaforma

Terzo comma

Nel terzo comma si capisce quando un provider è responsabile.

Se viene richiesto dall'autorità giudiziaria o amministrativa, avente funzioni di vigilanza la rimozione del video, ma non lo si effettua, si prevede una sanzione al provider.

Prima di procedere legalmente dobbiamo vedere se è stato violato qualche diritto alla personalità

Diritto della personalità: i diritti della personalità, come il diritto alla vita e il diritto alla salute, hanno le seguenti 3 caratteristiche:

1) Sono diritti **"assoluti"**, ovvero che non hanno bisogno di un destinatario: possono essere esercitati nei confronti di tutti i consociati, vale a dire che valgono verso chiunque.
2) Sono diritti **"indisponibili"**, ovvero che (tranne in alcune eccezioni) non possono essere oggetto di contratto. Nel resto del mondo, come negli USA, ciò non è sempre vero.
3) Sono diritti **"imprescrittibili"**, per loro non esiste quindi l'istituto della prescrizione.

Vengono riconosciuti a tutte le persone fisiche e in alcuni casi anche alle persone giuridiche (un'azienda non gode di diritto alla vita o alla salute, ma alla reputazione si). Sono un insieme aperto o non tassativamente disciplinati (ovvero significa che **si** possono aggiungere altri diritti o crearne di nuovi).

Si crea un diritto nuovo perché cambia la società e si necessita un diritto per un'esigenza diversa da quelle precedenti.

Esempio:

2) Se io dispongo di un diritto di proprietà di casa mia, vendo casa mia, cedo il mio diritto su quell'immobile. Un diritto indisponibile NON può essere ceduto, venduto o acquistato.

Alcuni diritti della personalità:

1) **Diritto alla vita** (per eccellenza)**:** È talmente scontato che non è disciplinato da nessuna norma in Italia, si deduce siccome la pena di morte è vietata
2) **Diritto alla salute** (fisica e/o mentale): Articolo 32 Costituzione e art.5 Codice Civile.
3) **Diritto all'onore:** Diritto che viene offeso tramite l'ingiuria. Diritto di non vedere offesa l'immagine che io ho di me stesso.

Una volta era concesso il Delitto d'onore, ovvero era depenalizzato il reato di omicidio se la persona che aveva ucciso aveva lesionato l'onore dell'omicida.

Ingiuria = offesa

Reputazione: onore = diffamazione: ingiuria

Diffamazione: lesione dell'immagine che gli altri hanno in me.

Diffamazione > Ingiuria

4) **Diritto all'immagine: Il diritto di tutelare la propria immagine fisica**: per esempio quando viene utilizzata la mia immagine per scopi commerciali senza il mio consenso.

Caso "Lucio Dalla": una compagnia di cuffie per l'ascolto di musica ha utilizzato per una pubblicità la sagoma chiaramente identificabile in Lucio Dalla. L'immagine sul manifesto pur non essendo una fotografia, richiamava inequivocabilmente la figura dell'artista. Il cantautore venne risarcito, in quanto non aveva ricevuto compenso né aveva dato il consenso all'utilizzo della propria immagine.

Allora come può essere "disponibile", quindi oggetto di contratto, se si tratta di un diritto della personalità e quindi "indisponibile" per natura? Negli USA nacque e si diffuse rapidamente nel mondo, l'abitudine a sfruttare l'immagine dei soggetti famosi. A causa della forte influenza della cultura USA verso il nostro continente, nacque di conseguenza la necessità di un compromesso: si decise che sarebbe stato possibile sfruttare il diritto all'immagine di un individuo, ma solo con il **consenso** e solo a patto che ciò non **ledesse la sua dignità**.

5) **Diritto all'identità personale:** Diritto a tutelare la propria immagine sociale.

Es. 1: Due ragazzi vengono ritratti abbracciati e tale immagine viene utilizzata, senza consenso, per una campagna pubblicitaria contro l'aborto. C'è una lesione: si offre ai consociati un'immagine sociale non reale dei due soggetti ritratti.

Es. 2: Durante un'intervista contro il fumo, il Dott. Veronesi affermò che fosse meno nocivo fumare le sigarette elettroniche rispetto a quelle tradizionali. Venne utilizzata la sua citazione, estrapolata e decontestualizzata, per una campagna pubblicitaria a favore delle sigarette elettroniche.

Questo diritto è stato creato dai giudici, non esiste una definizione normativa del diritto all'immagine o del diritto all'identità personale, esiste solo in forma giurisprudenziale, tramite le

sentenze della Corte di Cassazione. L'unica fonte dei diritti della personalità è l'Articolo 2 della Costituzione, che però non li cita direttamente.

Articolo 2 - Costituzione

La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.

6) **Diritto alla reputazione**: Diritto a mantenere un'alta opinione sociale da parte della propria collettività (vale anche per le persone giuridiche). Ogni individuo ha diritto che gli altri appartenenti della propria comunità pensino bene di lui e nel caso in cui dovessero pensar male, lo devono fare in termini non offensivi.

   Es. "Caso TripAdvisor": Qualche anno fa è stato condannato un soggetto che aveva espresso un commento negativo ad una struttura commerciale, anche con toni offensivi e volgari. Il commento, che poteva pur essere veritiero, è stato comunque giudicato lesivo e l'autore condannato per diffamazione dai giudici. Non tanto per via del contenuto del commento, ma soprattutto per i toni non consoni rispetto all'ambiente di diffusione (in questo caso Internet).

Non serve la menzogna per la diffamazione, basta che la modalità in cui una verità viene espressa sia offensiva (*Art. 595 c.p.*). Si tratta di un reato, quindi si può procedere anche in via **penale**.

Se un diritto della personalità venisse violato, prima di agire in giudizio, è possibile richiedere la rimozione dell'evento dannoso, contattando direttamente la fonte.

1) Se l'immagine non venisse rimossa, è possibile esercitare **un'azione inibitoria** presso il Tribunale Civile, allo scopo di far cessare un comportamento lesivo per il soggetto titolare del diritto. Se dimostrata la dannosità, viene attuata generalmente in termini "veloci", in circa 30 giorni.
2) Sarà possibile richiedere un risarcimento del danno, secondo *l'Art. 2043 del Codice Civile*, sia per atti soggettivi del danneggiante di **dolo** (azione intenzionale), che di **colpa** (azione causata da imprudenza, imperizia o negligenza). Il dolo o la colpa sono la condizione all'accesso al risarcimento del danno.

Es: Insulto/commento negativo sul web:
-> La richiesta per un'azione inibitoria ha per oggetto la rimozione del contenuto lesivo;

-> Può essere di tipo doloso (diretta e consapevole) o colposo (indirettamente, senza volontà diretta, con leggerezza);
-> È possibile chiedere il risarcimento del danno:

Es: Insulto sul web verso l'ex coniuge (moglie), sia a livello personale che professionale:
-> Diritto leso: Diritto alla reputazione, eventualmente anche all'identità personale a seconda degli insulti.
-> C'è l'azione, c'è il dolo o la colpa, c'è il danno economico (l'ex coniuge professionista perde clienti, Art. 2043) e c'è un danno morale (sofferenza psicologica causata alla madre).

Quindi Danno economico	->	Diminuzione patrimoniale
Danno morale	->	Patimento psicologico/emotivo (sofferenza umana)

Il danno morale può essere di due tipi: Patrimoniale o non patrimoniale
Danno patrimoniale: è il più facile poiché è facilmente suscettibile da valutazione economica. Es: Perdo il lavoro.
Danno non patrimoniale: Non suscettibili di valutazione economica, ma vengono comunque quantificati in sede di valutazione economica. Non facilmente suscettibili di valutazione economica e viene valutata economicamente, secondo il codice civile, per equità da parte del giudice.
All'interno di questo danno non patrimoniale, oltre che ai danni morali presenti, vi sono i danni biologici (Esempio: mi mette sotto una macchina e perdo l'uso delle gambe e faccio il professore. Bisogna distinguere il danno patrimoniale e biologico "perdo gambe" dal fatto di "fare il professore" danno biologico).

Es: Specializzandi esaminati per lavorare in Università. Pubblicato online risultati con nomi con codice fiscale e stipendio.
-> Gli studenti fanno causa per violazione del diritto alla protezione dei dati personali (senza consenso, senza informativa e nessun interesse pubblico).
-> La causa viene vinta dagli studenti, ma non viene riconosciuto nessun danno. Il danno patrimoniale non esiste. Il danno morale è stato valutato nullo.
È stato valutato come un fatto ingiusto, c'è della colpa, ha creato un fastidio, ma non ha creato nessun danno (economico o morale), quindi non prevede alcun risarcimento.

Articolo 2059 – Codice Civile: Danni non patrimoniali
Il danno non patrimoniale deve essere risarcito solo nei casi determinati dalla legge

Ad oggi, tramite la legge, tramite la Giurisprudenza o tramite il recepimento di disposizioni europee si può richiede un risarcimento per un danno non patrimoniale anche nel caso di violazione dei diritti della personalità.

Per quantificare economicamente un danno non patrimoniale ci si basa spesso sulle sentenze precedenti (nel caso di illeciti online) o, ultimamente, basandosi su alcune tabelle che sono state redatte dal tribunale di Milano.

Se il soggetto danneggiante deve risarcire un danno ma non è capiente (o non lo sono i suoi tutori), il danno non viene risarcito e la vittima rimane senza compensazione.

7) **Diritto alla riservatezza:** Diritto di escludere gli altri da quello che è la mia vita personale.

A tutelare i diritti della personalità ci sono alcuni articoli del Codice Penale

Articolo 594 - Codice Penale: Ingiuria (Abrogato nel 2016)

Chiunque, offende l'onore o il decoro di una persona presente è punito con la reclusione fino a sei mesi o con la multa fino a euro 516.

Articolo 595 - Codice Penale: Diffamazione

Chiunque, fuori dei casi indicati nell'**articolo** precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1032.

Bisogna distinguere però:

L'immagine della persona fisica: la mia foto che viene pubblicata in giro

L'immagine sociale: la considerazione che hanno gli altri di noi (reputazione)

Articolo 7 - Codice civile: Tutela del diritto al nome

La persona, alla quale si contesti il diritto all'uso del proprio nome o che possa risentire pregiudizio dall'uso che altri indebitamente ne faccia, può chiedere giudizialmente la cessazione del fatto lesivo, salvo il risarcimento dei danni.
L'autorità giudiziaria può ordinare che la sentenza sia pubblicata in uno o più giornali.

Diritti relativi al ritratto: si occupano dell'immagine della persona fisica e fanno parte della LEGGE 22 aprile 1941, n. 633 (Diritto d'auotre)

Articolo 96 – Legge 633/1941

Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa, salve le disposizioni dell'articolo seguente.

Dopo la morte della persona ritrattata si applicano le disposizioni del 2°, 3° e 4° comma dell'art. 93.

Articolo 97 – Legge 633/1941

Non occorre il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico.

Il ritratto non può tuttavia essere esposto o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata.

Firme elettroniche

Documento: qualsiasi strumento che funga da contenitore di informazioni.

Un atto notarile è un documento, così come le condizioni generali di un contratto di Amazon, l'unica differenza è che uno è cartaceo e l'altro è sul web.

Non viene definita la forma, ma solo la funzionalità

Forme di contratto e sistema delle prove:
Un contratto di trasporto non richiede alcuna forma specifica: è un contratto a tutti gli effetti, non richiede alcuna formalità, può essere concluso semplicemente con un'azione, come il salire sull'autobus.
Mentre altri contratti, specificati nel Codice Civile, devono avere assolutamente forma scritta (sinonimo di scrittura privata): compravendita di beni immobili, locazioni, contratti di lavoro, bancari, assicurativi o nel caso di donazioni.

Tutti questi documenti non hanno la stessa valenza giuridica, si differenziano per l'affidabilità dell'informazione e anche dalla firma.

Nell'ordinamento italiano il legislatore ha scelto un sistema delle prove di **tipo vincolato**, ovvero a dare un peso diverso predeterminato rispetto al tipo di prove presentate durante un dibattimento:

- un documento con sottoscrizione autografa è considerato piena prova;
- un documento non firmato viene sempre considerato come un principio di prova;
- se un testimone riferisce la propria versione dei fatti, essa verrà considerata un principio di prova.

Il giudice non è libero di decidere il valore legale di una prova prodotta in giudizio, bensì il valore di ogni prova è predeterminato già nel Codice Civile: ad ogni tipo di documento è associato un diverso valore, determinato in base alle garanzie associate al tipo di documento.

È necessario quindi comprendere quali siano le firme elettroniche che sono equivalenti alla firma autografa, equiparabili quindi alla sottoscrizione di un atto scritto.

Un contratto si dice concluso quando vi è un incontro tra le parti. Anche su WhatsApp si può concludere un contratto. Ci sono però alcuni contratti che secondo il Codice civile, c'è bisogno che la firma di un contratto sia scritta.

A seconda del tipo di firma elettronica cambia la valenza e la forza giuridica del documento

I testi normativi da considerare sono:

1) Regolamento eIDAS - 910/2014 (*Electronic Identification Authentication Signature*, del 2014, in vigore dal 2016)
2) Regolamento CAD – DLGS 82/2005 (Codice dell'Amministrazione Digitale)

Firma autografa: è la firma apposta ad un documento cartaceo quando si agisce di proprio pugno.

Percorso iniziato in Italia negli anni '90, prima nazione al mondo a normare la firma elettronica, tramite la Legge Bassanini, che prevedeva la possibilità di firmare i documenti informatici tramite la firma digitale, riconoscendo un'equivalenza tra la firma digitale e quella autografa. Venne scelta una specifica tecnologia: la firma digitale.

Firma digitale: crittografia a chiavi asimmetriche, per firmare servono due chiavi, una privata e una pubblica. Il messaggio viene firmato con una chiave privata e utilizzando quella pubblica è possibile verificarne l'autenticità.

Il processo di nascita della firma elettronica è stato condiviso e migliorato, dalla comunità europea che, applicando il concetto di **equivalenza funzionale**, ha aperto la strada allo sviluppo e all'utilizzo di nuove tecnologie di firma.

Firma elettronica (definizione generale): insieme di dati acclusi oppure connessi tramite associazione logica ad altri dati elettronici utilizzati dal firmatario per firmare (mi riconducono al firmatario). Qualsiasi e-mail sempre è una firma elettronica.

Infatti, nel regolamento eIDAS troviamo tre tipi di firme elettroniche:

- Firma elettronica Semplice (FE),
- Firma elettronica Avanzata (FEA),
- Firma elettronica Qualificata (FEAQ).

Oltre alla Firma Digitale, già prevista dall'ordinamento italiano, nel Regolamento CAD, che possiamo definire come sottoinsieme della firma qualificata.

Articolo 3 – eIDAS: Definizioni

Il livello di firma elettronica più basso è quello della **firma elettronica semplice**: *dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.*

Definizione di **firma elettronica avanzata**: *una firma elettronica che soddisfi i requisiti di cui all'articolo 26* (ovvero possiede determinati requisiti, non tecnologici, ma funzionali).
Questo metodo di firma garantisce una maggiore sicurezza circa l'identificabilità del soggetto che sta firmando.

Definizione di **firma elettronica avanzata qualificata**: *una firma elettronica avanzata creata da un dispositivo per la creazione di una **firma elettronica qualificata** e **basata su un certificato** qualificato per firme elettroniche;* (ovvero una firma elettronica avanzata con l'aggiunta di un certificato).
Certificato elettronico: un terzo soggetto garantisce digitalmente (certifica) l'identità del soggetto firmatario.

Articolo 25 – eIDAS: Effetti giuridici delle firme elettroniche

1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.
2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.
3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

Articolo 26 – eIDAS: Requisiti di una firma elettronica avanzata

Una firma elettronica avanzata soddisfa i seguenti requisiti:
a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;
c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e
d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Principio di neutralità tecnologica: La **neutralità tecnologica** è il **principio** secondo il quale non è giusto scommettere su una sola tecnologia; al contrario è meglio prevedere un approccio flessibile alle diverse tecnologie a disposizione, senza che una prevalga necessariamente sulle altre.

Nel mondo fisico, dove si utilizza la firma autografa, la connessione unica al firmatario si fa con la perizia calligrafica (analisi degli *specimen,* ovvero dei campioni di firma). Per fare questa connessione nel mondo digitale, una possibile soluzione è creare una connessione di firma con strumenti più complessi e sicuri.

Esempi di firma elettronica semplice:
Pin del cellulare, login per accesso alla mail, firma su tablet del postino.

Esempi di firma elettronica avanzata:
All'apertura di un conto corrente in banca pongo una firma su tablet (firma grafometrica).

È una firma avanzata solo se prima di firmare, vengo identificato: ovvero si effettua un processo di riconoscimento "*de visus*", tramite carta d'identità. Inoltre generalmente servono più firme, per fornire gli *specimen* di firma.
Quindi la firma elettronica avanzata è un processo di firma, formato da più azioni.

Esempi di firma elettronica digitale:
Badge che il professore utilizza per verbalizzare gli esami. C'è l'identificazione all'emissione del badge e un sistema di crittografia a chiavi asimmetriche che certifica la firma.
Chiavetta fornita da banca per disposizioni di home-banking

Le tre firme naturalmente hanno diversi effetti ed applicazioni giuridiche.

Se autenticata da un notaio, la stampa di una mail è considerabile come un documento con firma elettronica semplice, ovvero con valenza legale. Ha però un livello di sicurezza basso, quindi può essere contestato dalla controparte (password comune, utilizzo di account di altra persona). In questo caso, e in tutti i casi di documenti sottoscritti con firma elettronica semplice, è il **giudice che valuta liberamente,** se tale documento è da considerarsi con piena valenza legale, ovvero se può essere equiparato ad un documento cartaceo sottoscritto con firma autografa.
Vengono valutati principalmente tre requisiti di affidabilità del documento: integrità, immodificabilità e sicurezza del processo.

Scrittura autenticata: Riguarda altri campi oltre alle firme elettroniche. Per avere una scrittura / firma autenticata devo rivolgermi ad un notaio o a un funzionario abilitato (impiegato comunale).

Per avere una firma autenticata vado dal notaio, firmo il mio documento davanti a lui (che sia cartaceo o tramite firma elettronica) e lui rilascia l'autenticazione dichiarando che sei stato proprio tu a firmare.

La firma autenticata non può essere disconosciuta.

Scrittura qualificata: Prestatori di servizi fiduciari qualificati: Sono soggetti che rilasciano certificati qualificati a norma di un regolamento EU

La firma qualificata viene rilasciata da un dispositivo che viene rilasciato da un prestatore di servizi commerciali insieme a un certificato di firma che ne dà l'identificazione del soggetto.

Gli articoli 28,29,30 parlano delle firme qualificate e dei certificati per qualificarle

Attenzione: **NON** bisogna confondere la scrittura qualificata da quella autenticata

Qualificata: firme elettroniche rilasciata tramite dispositivi al soggetto che lo ha richiesto

Autenticata: quella specifica firma su quello specifico contratto è stata fatta davanti alla presenza di un notaio che conferma di aver visto tutto

La regola è diversa nel caso di un documento sottoscritto con una firma elettronica avanzata (o digitale):

Articolo 20 - DLGS 82/2005 (CAD): Validità ed efficacia probatoria dei documenti informatici

Un documento elettronico può essere considerato equiparabile ad una scrittura privata se firmato con firma elettronica avanzata o con firma digitale o previa identificazione informatica attraverso un processo […] con modalità da garantire sicurezza, integrità e immodificabilità del documento e riconducibilità manifesta ed equivoca all'autore.

Nel caso in cui durante un procedimento, venisse disconosciuta la firma apposta ad un documento convenzionale (firma autografa) verrebbe avviata una verifica tramite la consulenza di un perito calligrafico. A seconda dell'esito della perizia, essa verrà considerata piena prova o meno.

Nel caso di firma elettronica avanzata, il processo di disconoscimento è molto più complicato: giuridicamente è possibile solo se il soggetto dimostra che in quel momento era impossibilitato a firmare oppure che inequivocabilmente qualcuno lo ha obbligato a firmare. Un'altra strada è quella di attaccare il processo di firma elettronica avanzata (dimostrando che non è stato chiesto il documento d'identità o che il documento è stato modificato). Le aziende che utilizzano tale firma però utilizzano processi e procedure standardizzate, ad elevata sicurezza e affidabilità, difficilmente confutabili.

In conclusione, e in maniera complementare, possiamo definire che:
- la difficoltà probatoria per le firme elettroniche avanzate è maggiore rispetto al documento cartaceo convenzionale;
- la firma elettronica avanzata ha maggior tenuta legale della firma cartacea, in quanto è molto più difficile disconoscerla. Per questo motivo in molti casi diventa il metodo di sottoscrizione preferito per alcune tipologie di aziende (come le banche).

La firma digitale possiede ancora più forza probatoria rispetto a tutte le altre tipologie di firma. Per essa infatti, essendo basata su un dispositivo di controllo, esiste un principio di "inversione della prova" rispetto agli altri tipi di firma, compreso quella autografa, dove può venir valutata la paternità della firma tramite la perizia calligrafica: in questo caso non discute più della provenienza della firma (è associata ad un dispositivo e ad una password in modo univoco), ma si discute sul possesso e la custodia del dispositivo di firma. È il firmatario che deve dimostrare che la firma non è stata disposta per una sua volontà, ma che altri hanno firmato al suo posto, a causa della perdita di possesso del dispositivo.

È buona norma quindi ricordarsi di effettuare immediatamente la denuncia in caso di furto o smarrimento del dispositivo di firma, poiché rimane l'unico metodo per dimostrare successivamente in giudizio di non essere l'autore di un eventuale documento (con una data posteriore alla denuncia) sottoscritto con firma digitale.

Gli atti che necessitano di forma scritta (o scrittura privata) hanno valenza legale solo se sottoscritti con firma elettronica avanzata. Se l'oggetto del contratto è un bene immobile (vedi Art. 1350 c.c.) l'unica firma elettronica riconosciuta è quella di tipo avanzata qualificata (come quella digitale). Se sottoscritto con altri tipi di firma elettronica, il contratto è nullo.

Articolo 21 - DLGS 82/2005 (CAD): Ulteriori disposizioni relative ai documenti informatici

2-bis). Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo.

2-ter. Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110, ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti.

Riassumendo:

Stabilisce quale tipologia di firma serve per la validità di un contratto nel quale il codice civile prevede la forma scritta.

Se voglio vendere casa mia con un documento elettronico, si può fare ma il documento va firmato con firma elettronica qualificata

Identificazione Elettronica

MEME: On the internet no body know your're a dog

Problemi dell'identità digitale:

1) Verifica di chi utilizza il dispositivo
2) Verifica del contesto in cui agisce l'utilizzatore

Identificazione Elettronica: È il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica. (Articolo 3 – eIDAS)

Marcatura temporale: Modalità per legare determinati dati costituiti in forma elettronica ad una certa data e ad una certa ora per provare che questi ultimi esistevano in un determinato momento

Contrassegno (glifo): Serve per verificare la firma elettronica una volta che il documento viene stampato su carta

Esempio: un QRcode che consente tramite l'inquadratura di verificare che quel documento viene da quell'amministrazione.

Sigillo elettronico: è un sigillo che viene rilasciato, non serve a consentire la verifica dopo che si è stampato, ma è una SORTA di firma che viene rilasciata alle persone giuridiche, perché la vera firma elettronica viene rilasciata solo alle persone fisiche

Articolo 36 – eIDAS: Requisiti dei sigilli elettronici avanzati

Un sigillo elettronico avanzato soddisfa i seguenti requisiti:

- a) è connesso unicamente al creatore del sigillo;
- b) è idoneo a identificare il creatore del sigillo;

- c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e
- d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

Articolo 43 – eIDAS: Effetti giuridici di un servizio elettronico cerficato (PEC)

1. Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.

2. I dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato.

Posta Elettronica Certificata (PEC): Effetti giuridici molto differenti tra mail classica e PEC: l'invio di un PEC è paragonabile nel mondo fisico ad una raccomandata con ricevuta di ritorno: utile quando serve una certezza giuridica riferita ad un momento preciso di ricezione. Rispetto alla raccomandata tradizionale, inoltre, ha ancor più valore legale in quanto è "certificato" anche il contenuto del messaggio. Attenzione, la PEC contiene comunque solo una **firma elettronica semplice** (non avanzata e non qualificata). È sempre possibile firmare con firma digitale gli allegati, in modo da aumentare la sicurezza e la valenza legale della comunicazione.

Il nome e cognome alla fine del testo di una mail convenzionale non hanno alcun valore legale, sono considerati semplicemente testo della mail.

Diritto d'autore

Il diritto d'autore nasce a Venezia nel 400 con l'introduzione della macchina da stampa. Non nasce come diritto a tutele dell'autore, ma solo lo stampatore.

In Europa questo concetto si evolve anche grazie al Romanticismo, che sposta il soggetto di tale diritto dall'editore/stampatore all'autore, valorizzandone l'aspetto creativo.

Legge 22 aprile 1941, n. 633 (Legge sul diritto d'autore): non tutela solo l'editore, ma anche l'autore dell'opera. È un diritto di tipo privativo (ovvero la possibilità di escludere terzi e richiedere compensi). Il software, quando possiede un carattere creativo (e non quando lo si scrive per conto di un'azienda), viene considerato un'opera creativa, e tutelato quindi dal diritto d'autore.

Il compito di determinare cosa e quando qualcosa è effettivamente un'opera d'arte tutelata dal diritto d'autore è determinata solo a posteriori da un giudice.

Il diritto d'autore nasce assieme all'opera, non devo richiederlo, l'importante è che l'autore dimostri di essere lui il primo creatore dell'opera. È necessario fornire una **data certa** (in senso giuridico) al momento della creazione dell'opera, per prevenire future complicazioni. Si può stipulare un atto pubblico (tramite Notaio), prassi però complicata e onerosa. Un'altra possibilità è quella di apporre una marca temporale sull'opera o, se si tratta di un'opera digitale, auto-inviarsi una PEC con allegata l'opera. In alcuni casi (per opere musicali, cinematografiche e anche in caso di software), si può registrare l'opera alla Siae. Questa operazione non fa nascere il diritto d'autore sull'opera, ma semplicemente fornisce data certa della creazione.
Si necessita di una data certa perché il copyright non tutela l'idea, ma la sua forma espressiva e il suo linguaggio.

L'idea non può essere tutelata né dal diritto d'autore né dalla proprietà industriale. Quindi se per esempio viene copiata la trama di un'opera, non c'è plagio.
Ciò accade perché i legislatori hanno scelto di non porre dei limiti giuridici alle idee, in quanto sarebbe stato un vero ostacolo verso il progresso. Trasponendo la situazione al software, è tutelato solamente il codice, il linguaggio e la forma espressiva, ma non l'idea e l'algoritmo alla base dell'applicazione.

Esempio: Se io credo un social dove si possono pubblicare foto, non posso vietare agli altri di farlo, ma grazie al diritto d'autore non possono usare il mio stesso codice.

Bisogna distinguere il diritto d'autore dal brevetto.
Brevetto: si riferisce alle invenzioni industriali, non creative. Il brevetto ce l'ho dal momento in cui lo registro. Prima di brevettare l'invenzione, l'invenzione non è mia. La tutela esclusiva del brevetto è di 20 anni, ha dei costi significativi e può essere limitato geograficamente.

Il software non può essere brevettato in quanto opera creativa

Riassumendo i concetti principali sul Diritto d'Autore:

1. Sorge alla **nascita** dell'opera.
2. Deve essere caratterizzata da un aspetto di **creatività**.
3. Ne viene tutelata la **forma** e l'espressione, non l'idea.

Il diritto d'autore è composto da due parti:

Diritto d'autore morale: diritto al riconoscimento della paternità dell'opera (posso avere solo il diritto morale, senza quello patrimoniale). Questo diritto non si esaurisce mai e non è cedibile.

Esempio: Se Beethoven muore e dopo 80 anni io canto le sue canzoni, non posso dire che le ho fatte io, posso comunque cantarle gratis.

Diritto d'autore patrimoniale: La legge dice che il diritto patrimoniale dura 70 anni decorrenti dalla morte dell'autore. Dopo i 70 anni, l'autore non avrà più l'esclusiva. Quindi il diritto di utilizzazione economica scade.

Esempio: Dopo 80 anni dalla morte di Beethoven, anche se ereditariamente ha passato i diritti ai suoi figli, io casa discografica posso fare comunque un album con le sue sinfonie senza dover pagare nulla ai figli dell'artista defunto.

Inoltre, come tutti i diritti di tipo economico, **possono essere modulati**, tramite la conclusione di contratti. Le licenze sono particolari tipi di contratto che hanno come oggetto il diritto patrimoniale d'autore all'utilizzo di un software.

Il concetto di ghostwriter nasce in USA, dove non esiste lo stesso concetto di diritti d'autore europeo. Tale situazione è comunque tollerata in Europa, nonostante i diritti d'autore morali, come diritti della personalità, siano indisponibili.

Se l'autore di un'opera è una collettività, il diritto d'autore appartiene e viene condiviso da tutti.

Le aziende di software possono inserire una clausola nel contratto d'assunzione in cui si afferma che tutti i diritti patrimoniali derivanti dalle opere dei dipendenti vengano trasferite alla società. Mentre rimarrà inviolato l'esercizio dei diritti morali.
Acquistando un diritto di licenza, nonostante non sia evidente nel contratto, è sempre possibile:

- Copiare il software al fine di creare una copia di backup
- Modificare il codice al fine di renderlo compatibile con altri programmi
- Studiarlo al fine di comprenderne l'idea e l'algoritmo alla base del software

Una raccolta di appunti può essere un'opera d'arte? Si, se presenta un aspetto minimo di creatività. Come si può scrivere un contratto che disciplina i diritti d'autore di quest'opera? È impegnativo e poco funzionale scrivere un contratto apposta, ci si può affidare alle Creative Commons. Sono delle regole che disciplinano classificandoli, i vari tipi di utilizzo delle proprie opere in maniera immediata e condivisa. Il sistema si basa su un approccio contrario rispetto alla legge che disciplina il diritto d'autore (di tipo proprietario): apponendo il simbolo Creative Commons si sta comunicando che si cedono alla collettività tutti i diritti d'autore patrimoniali su quell'opera, secondo diverse modalità (riconoscimento dell'autore, utilizzo salvo fini commerciali, condivisione delle regole di licenza, non modificabilità). I simboli CC rappresentano dei contratti! Non esiste una legge specifica che li riconosca, ormai fanno parte degli usi e consuetudini, conosciuti, utilizzati e riconosciuti anche in ambito legale.

Articolo 12 – Legge 633/1941

L'autore ha il diritto esclusivo di pubblicare l'opera.
Ha il diritto esclusivo di utilizzare economicamente l'opera in ogni forma e modo, originale o derivato, nei limiti fissati da questa legge, ed in particolare con l'esercizio dei diritti esclusivi indicati negli articoli seguenti.

E' considerata come prima pubblicazione la prima forma di esercizio
del diritto di utilizzazione.

Articolo 20 – Legge 633/1941

(Indipendentemente dai diritti esclusivi di utilizzazione economica dell'opera, previsti nelle disposizioni della sezione precedente, ed anche dopo la cessione dei diritti stessi, l'autore conserva il diritto di rivendicare la paternità dell'opera e di opporsi a qualsiasi deformazione, mutilazione od altra modificazione, ed a ogni atto a danno dell'opera stessa, che possano essere di pregiudizio al suo onore o alla sua reputazione)).

Tuttavia nelle opere dell'architettura l'autore non può opporsi alle modificazioni che si rendessero necessarie nel corso della realizzazione. Del pari non potrà opporsi a quelle altre modificazioni che si rendesse necessario apportare all'opera già realizzata.

Però se all'opera sia riconosciuta dalla competente autorità statale importante carattere artistico spetteranno all'autore lo studio e l'attuazione di tali modificazioni.

Articolo 21 – Legge 633/1941

“L’autore di un’opera anonima o lo pseudonimo ha sempre il diritto di rivelarsi e di far riconoscere in giudizio la sua qualità di autore”

Esempio: Mario rossi alias zerocalcare avrà sempre il diritto di rivelarsi e di far riconoscere in giudizio la sua qualità di autore.

Articolo 25 – Legge 633/1941

I diritti di utilizzazione economica dell'opera durano tutta la vita dell'autore e sino al termine del settantesimo anno solare dopo la sua morte.

Articolo 103 – Legge 633/1941: SIAE

È istituito presso il Ministero della cultura popolare un registro pubblico generale delle opere protette ai sensi di questa legge.

Nel registro di cui al primo comma sono registrate le opere soggette all'obbligo del deposito

con la indicazione del nome dell'autore, del produttore, della data della pubblicazione e con le altre indicazioni stabilite dal regolamento.

Alla Società italiana degli autori ed editori è affidata, altresì, la tenuta di un registro pubblico speciale per i programmi per elaboratore. In tale registro viene registrato il nome del titolare dei diritti esclusivi di utilizzazione economica e la data di pubblicazione del programma, intendendosi per pubblicazione il primo atto di esercizio dei diritti esclusivi.

La registrazione fa fede, sino a prova contraria, della esistenza dell'opera e del fatto della sua pubblicazione. Gli autori e i produttori indicati nel registro sono reputati, sino a prova contraria, autori o produttori delle opere che sono loro attribuite.

La tenuta dei registri di pubblicità è disciplinata nel regolamento.

I registri di cui al presente articolo possono essere tenuti utilizzando mezzi e strumenti informatici.

Articolo 102 bis – Legge 633/1941: Banca dati

L'articolo spiega a cosa serve l'utilizzo di una banca dati (database) e norma i diritti per il creatore e gli utilizzatori.

Banche di dati sono raccolte di dati (informazioni, opere, fotografie, registrazioni audio). Secondo le regole normative appena esposte, anche una banca di dati può essere tutelata dalla legge sul diritto d'autore, se il singolo dato è creativo (per esempio il catalogo fotografico di una mostra), o la banca dati è creativa nel metodo di organizzazione delle informazioni. Negli anni 80 però, la magistratura ha riconosciuto uno sforzo del costitutore per la creazione di banche dati anche senza l'elemento di creatività (del dato o dell'organizzazione) al fine trovare un metodo per tutelare anche questo tipo di attività. Ad oggi esiste un diritto, chiamato "sui generis", che contraddistingue le opere non necessariamente caratterizzate da un aspetto di creatività, che riconosce al costitutore della banca di dati la possibilità di escludere la copia o l'estrazione di dati da parte di terzi per 15 anni. In questo modo, oltre a tutelare lo sforzo effettuato, viene riconosciuta anche la possibilità di creare dei contratti di licenza per l'utilizzo.
Legge di tutela delle banche dati è di livello europeo, si chiama "sui generis" perché, purché inserito nella legge sul diritto d'autore, è un diritto di tipo diverso, con regole particolari.

Open Source: sono tutti i software scaricabili gratuitamente e che sono messi a disposizione dagli autori stessi come: "Linux e Firefox". Posso utilizzarli e modificarli ma devo rispettare due regole fondamentali:

- Non posso guadagnarci
- Non posso appropriarmene

Danni Informatici

Danno Informatico: è quello che il cliente del fornitore subisce in coincidenza di un malfunzionamento del sistema informatico.

Il danno può essere Diretto o Indiretto

Esempio: Supponiamo di essere l'impresa Alfa s.r.l., che vende riduttori tramite il suo e-commerce. Siamo costretti a stare fermi tre giorni a causa della frittura di un server.

L'azienda ha 500 dipendenti e un fatturato di 40 milioni l'anno

Danno Diretto: direttamente provocato dal malfunzionamento

L'azienda perde i dati ed è costretta a stare chiusa per tre giorni in attesa del ripristino del server

Danno Indiretto: indirettamente provocato tramite il malfunzionamento

Non riesco a rispettare gli ordini, avevo 1000 consegne da fare e 1000 clienti chiedono il risarcimento, con la conseguente perdita della fiducia della clientela.

Ma non solo, essendo un'azienda con 500 dipendenti, solo per il fatto di esistere e solo per poter pagare i dipendenti ho dei costi di circa 100.000€ al giorno.

Risulta molto difficile calcolare esattamente il danno indiretto.

Articolo 1223 – Codice Civile: Risarcimento del danno

Il risarcimento del danno per l'inadempimento o per il ritardo deve comprendere così la perdita subita dal creditore come il mancato guadagno, in quanto ne siano conseguenza immediata e diretta.

Articolo 1224 – Codice Civile: Danni nelle obbligazioni pecuniarie

Nelle obbligazioni che hanno per oggetto una somma di danaro, sono dovuti dal giorno della mora gli interessi legali, anche se non erano dovuti precedentemente e anche se il creditore non prova di aver sofferto alcun danno. Se prima della mora erano dovuti interessi in misura superiore a quella legale, gli interessi moratori sono dovuti nella stessa misura.

Al creditore che dimostra di aver subito un danno maggiore spetta l'ulteriore risarcimento. Questo non è dovuto se è stata convenuta la misura degli interessi moratori.

Danno emergente: è il costo tipo che subisco in conseguenza a quel danno.

Esempio: "Quanto mi costa chiamare un tecnico per chiamare un guasto?"

Lucro cessante: Mancato guadagno in quanto ne siano conseguenza immediata e diretta.

Esempio: "Perdita cliente".

Articolo 1225 – Codice Civile: Prevedibilità del danno

Se l'inadempimento non dipende da dolo (voluto) il risarcimento è limitato al danno che poteva prevedersi nel tempo in ciò è sorta l'obbligazione. Criterio della prevedibilità del danno.

Prevedibilità del danno: Considerata alle normali utenze e il normale svolgimento del contratto

Reati Informatici

Quando si parla di REATI, facciamo riferimento al Codice Penale

Nel diritto penale si applica un principio fondamentale, ovvero la "necessaria specificità dei reati".

A differenza del diritto civile, nel diritto penale non si può interpretare la legge per analogia (non posso dire che un caso è simile ad un altro e applicare la stessa norma), nel diritto penale l'articolo 1 lo vieta, perché non si parla di sanzioni ma di limitare la libertà personale.

Articolo 1 – Codice Penale: Reati e Pene

Nessuno può essere punito per un fatto che non sia espressamente previsto dalla legge come reato, né con pene che non siano da essa stabilite.

Rispetto alle previsioni originali del Codice Penale, diverse fattispecie di reati non potevano essere sanzionati per il principio di legalità.
È stato necessario introdurre nel diritto nuovi tipi di reati "ad hoc", nati con l'avvento delle tecnologie informatiche. Questo processo si è sviluppato con:

- l'introduzione di nuovi reati: frode informatica, accesso abusivo al sistema informatico ecc.
- la modifica di norme preesistenti, atte a reprimere illeciti già noti, ma ora con nuovi strumenti tecnologici: diffamazione, furto d'identità, sexting
- il recepimento e ratifica di convenzioni internazionali *(come la L. 48/2008 per la convenzione di Budapest, o la convenzione di Lanzarote*).

Articolo 635 bis – Codice Penale: Danneggiamento di informazioni, dati e programmi

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Quando in una norma trovo la voce a querela della persona offesa, il pubblico ministero non fa partire le indagini a meno che la vittima non vada dai carabinieri a sporgere una denuncia

Con la dicitura: "Salvo che il fatto costituisca più grave reato", si intende quando la querela è d'ufficio.

Esempio: Se il reato è grave e quindi è perseguibile d'ufficio il procuratore ha il dovere di avviare l'indagine, senza aspettare la denuncia.

(Se una persona viene uccisa è grave e non può andare a sporgere denuncia e quindi partono automaticamente le indagini)

Spesso quando si parla di "più grave reato", si ha a che fare con concorso che può essere di diverso tipo:

Concorso di reati: quando faccio un reato per fare un altro reato

Esempio: Rubo una macchina (reato) per fare una rapina (reato)

Concorso materiale: quando i reati sono commessi a distanza di tempo, la pena è la somma della pena dei reati commessi

Esempio: Rubo una macchina e due settimane dopo vado a fare una rapina

Concorso formale: con la stessa condotta commetto più reati

Esempio: Con un solo colpo di pistola sparo uccido più persone (ho uno sconto della pena)

Articolo 635 quater – Codice Penale: Danneggiamento a sistemi informatici

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Articolo 615 ter – Codice Penale: Accesso abusivo a sistema informatico

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Viene considerato come la violazione di domicilio

Esempio: Ma se io sono a conoscenza delle credenziali di accesso che mi sono state fornite da una persona, faccio un reato se accedo al suo account?

Do la password della posta elettronica a mio marito, lui accede ad essa e trova delle e-mail scambiate con il mio amante. Mio marito porta quelle e-mail in tribunale come prova per chiedere il divorzio.

Io per salvarmi, denuncio mio marito per accesso abusivo al sistema informatico e gli faccio fare 3 anni di carcere (povero marito cornuto e carcerato).

Se io conosco una password il fatto non mi legittima ad accedere al sistema informatico, quindi è perseguibile, il reato si consuma anche solo per il fatto di acceder all'account di un altro individuo.

Articolo 640 ter – Codice Penale: Frode Informatica

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.

La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. (ipotesi di phishing)

La frode informatica può concorrere con gli altri reati, se si viene puniti per frode non è escluso che io venga punito anche per danneggiamento e accesso abusivo a sistema informatico.

Intelligenza Artificiale

Termine ombrello che si riferisce a sistemi o macchine che imitano l'intelligenza umana.

Machine learning = utilizza algoritmi per analizzare i dati, apprende da essi e poi prende delle decisioni in autonomia. Tipi di apprendimento:

- Supervised learning: gli fornisco informazioni che userà in autonomia;
- Unsupervised learning: crea le sue basi di dati senza guida;
- Reinforcement learning: gli dico se è corretto o no.

Deep learning = struttura gli algoritmi per generare una rete neurale artificiale che apprende dai dati e prende decisioni in autonomia.

Problemi
1. Explainability: perché il sistema ottiene quel risultato? Soprattutto dove c'è poca supervisione più sono potenti i nodi neurali meno è comprensibile.
2. GIGO (Garbage IN Garbage OUT): attività costosa, il sistema deve essere accurato per funzionare correttamente.
3. BIAS (pregiudizio deviante): pregiudizi umani trasmessi all'AI nella somministrazione dei dati, non mi consente di vedere le cose in modo oggettivo, grande problema in contesti scientifici dove si svolge l'analisi dei dati. es//Gli afroamericani contraggono le stesse malattie dei bianchi ma non possono accedere alle cure e non sono registrati nei database perciò da un'analisi dei dati risulterà che gli afroamericani hanno meno probabilità di contrarre malattie quando in realtà non è così.
4. Scorciatoie.

Responsabilità: di chi è se qualcosa va storto?
1. Autonomia

2. Opacità
3. Complessità
4. Imprevedibilità = Spurious correlation: connessioni tra dati che magari non hanno valore, non c'è connessione rilevante e non è provato il rapporto di causa effetto.

→ L'Italia si adegua all'UE, nel 2021 nasce la bozza del regolamento europeo sull'intelligenza artificiale denominato AI Act.
Es// Il Ministero dell'Interno ha acquistato un sw che usa il riconoscimento facciale ma il garante della privacy ha bloccato il real time, il riconoscimento dell'identità utilizzando il sw durante ad esempio una manifestazione, cioè in tempo reale.
Es// Moral Machine - guida automatica e responsabilità del guidatore.

→ Responsabilità penale: si basa sull'elemento oggettivo, nesso causale tra condotta ed evento, e sull'elemento soggettivo, il nesso psichico (dolo intenzionale, colpa non intenzionale). Quindi la responsabilità penale mi indica di chi è la colpa, invece quella civile mi indica chi paga il risarcimento, magari nessun responsabile ma qualcuno deve comunque risarcire, spesso il produttore a prescindere dal tipo di errore.