

DIRITTO

A.A. 2022-2023

Sommario

GDPR.....	3
Titolare del trattamento	5
Incaricato	5
Interessato	5
Responsabile della protezione dei dati (DPO)	6
Autorità di Controllo (Garante Privacy)	6
Liceità del Trattamento	7
Data Breach	8
Notifica di una violazione di dati	8
Comunicazione di una violazione di dati	8
DIRITTO PENALE.....	9
Il Reato.....	9
Bene Giuridico / Interesse Tutelato.....	10
La Colpevolezza.....	11
La Preterintenzione	11
DIFFAMAZIONE E SOCIAL NETWORK	12
Ingiuria:.....	12
Diffamazione:.....	12
Libertà di Pensiero:.....	12
Truffa:	13
Atti di concorrenza sleale:	13
DOCUMENTI E FIRME ELETTRONICHE	15
Fonti Normative:.....	15
Tipi di Documenti:.....	15
Firme Elettroniche:	15
POSTA ELETTRONICA CERTIFICATA (PEC)	17
COME FUNZIONA UN PROCESSO PENALE	18
COMPUTER CRIME.....	20

ACCESSO ABUSIVO A SISTEMI INFORMATICI O TELEMATICI	20
DANNEGGIAMENTO INFORMATICO	21
REVENGE PORN	21
Calunnia	21
FONDAMENTI DI DIRITTO INDUSTRIALE E PROPRIETA INTELLETTUALE	22
Cos'è un BREVETTO?.....	22
Il MARCHIO	23
Tipologie di marchi:	23
Requisiti di un Marchio:.....	24
Uso del Marchio.....	24
LEGGE SUL DIRITTO D'AUTORE.....	26
I CONTRATTI.....	27
CONTRATTI TELEMATICI	28
Distinzione importante:	28
Il Diritto Di Recesso.....	28
Clausole Vessatorie.....	29
Modalità di Conclusione del Contratto.....	29
RESPONSABILITA' INTERNET SERVICE PROVIDERS (ISP)	30

GDPR

(Regolamento europeo per la data protection) in vigore dal 25 maggio 2018.

Precedentemente c'era il Codice Privacy, Decreto Legislativo (D.lgs.) 196 del 2003, al quale è stata applicata l'**abrogazione selettiva**.



Abrogazione Selettiva:

il nuovo codice non sostituisce interamente il precedente (abrogazione) ma invece lo integra ed aggiorna con normative. In questo modo alcune delle norme del codice precedente restano in vigore mentre quelle che vanno in contrasto con quello nuovo vengono sostituite o rimosse interamente.

Si tratta di un approccio innovativo basato sull'**accountability** (responsabilizzazione sostanziale) del Titolare, che è responsabile per la **compliance** (conformità) ai principi privacy e deve essere in grado di dimostrarla. L'approccio è **risk-based**, ovvero basato sulla protezione dei dati dell'utente e sull'**effettivo rischio** per ogni azienda.

Proattività:

Al titolare è richiesto di **prevenire** e non correggere, nonché **dimostrare** che il trattamento è effettuato conformemente al GDPR, tramite elaborazione di un idoneo sistema documentale di gestione della privacy e policies interne da **esibire** in caso di richiesta da parte delle autorità.

Le misure a protezione dei dati devono essere **adottate già al momento della progettazione** di un prodotto o software (**design**). Va inoltre **garantito che vengano trattati unicamente i dati necessari per ogni specifica finalità (default)**.

Noi studiamo **trattamento** dei **dati personali** per persone fisiche.

Persone fisiche: gente vera e propria identificabile.

Persone giuridiche: non persone quindi aziende, enti.

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 nome, numero di identificazione, dati relativi all'ubicazione, identificativo online oppure a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica culturale o sociale.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione.

Trattamento di categorie particolari di dati personali:

Ex Dati sensibili (articolo 9 comma 1): dati che rivelano l'**origine razziale o etnica**, le **opinioni politiche**, le convinzioni **religiose o filosofiche**, l'**appartenenza sindacale**, nonché trattare **dati genetici**, **dati biometrici**, dati relativi alla salute, **vita sessuale** o **orientamento sessuale** della persona.

Ex Dati Giudiziari (articolo 10): dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (include anche processi penali ancora in corso).

L'email di lavoro di un dipendente è un dato personale?

Dipende:

- Se l'e-mail è associata ad uno specifico individuo (m.bianco@company.com) è un dato personale.
- Se l'e-mail è generica per la funzione della società (Hroffice@company.com) non è un dato personale.

Persone decedute e nascituri:

Persone decedute: il GDPR esclude dal proprio ambito di applicazione i "dati personali delle persone decedute", tuttavia ci sono delle casistiche nel quale ancora si applica:

- Nel caso non si possa accertare la morte della persona;
- Nel caso in cui il dato del defunto è indirettamente riferibile anche ad una persona in vita (ex dati sanitari su malattie genetiche che potrebbe avere anche il figlio).

A seguito del decesso, i dati diventano accessibili e trattabili dagli eredi o altri soggetti legati al defunto nel caso in cui abbiano un interesse proprio o agiscano a tutela dell'interessato (a meno che lo stesso interessato non avesse vietato tale esercizio quando ancora in vita). In ogni caso si potrebbe applicare un diverso regime di protezione derivante alla luce di altre normative nazionali (ad esempio: obblighi di confidenzialità del medico)

Nascituri: né il GDPR né il codice privacy prevedono nulla espressamente. Tuttavia, alla luce degli interventi giurisprudenziali sulla soggettività giuridica del nascituro e sulla sua titolarità di specifici diritti, non sarebbe ingiustificabile un'estensione della tutela in materia di protezione dei dati personali anche nei confronti del concepito.

L'indirizzo IP (Internet Protocol Address) è un dato personale?

Il GDPR afferma che l'indirizzo IP (statico) debba essere **considerato come un dato personale** in quanto ricadrebbe **nell'ambito degli identificativi online** come peraltro i cookies. Questo perché gli indirizzi IP sono registrati dagli internet service providers, i quali sono a conoscenza degli utenti ai quali gli indirizzi sono assegnati. Il gestore di una pagina web registra gli indirizzi IP che accedono ad una determinata pagina. Se le due informazioni venissero combinate permetterebbero l'identificazione di un utente associato ad un IP.

I Location data sono dati personali? (posizione)

Il GDPR non è chiaro a riguardo e non fornisce una definizione né indicazioni circa la loro gestione.

Dipende dalle circostanze.

Esempio:

- i dati che identificano gli autoveicoli di una flotta non sono dati personali.
- i dati che localizzano un individuo al momento di un pagamento in un centro commerciale costituiscono dati personali;
- i dati che localizzano un individuo in un ospedale o le frequenti visite in un luogo di culto o sindacato sono dati personali e potrebbero rientrare in dati sensibili in quanto identificherebbero dati relativi a stato di salute, orientamento religioso e/o politico ecc.

Titolare del trattamento

È la persona fisica o giuridica, ente o autorità pubblica che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento dei dati personali**.

Responsabile del trattamento

È la persona fisica o giuridica, ente o autorità pubblica che **tratta dati personali per conto del titolare del trattamento**.

I trattamenti da parte di un responsabile del trattamento sono **disciplinati da un contratto o da altro atto giuridico**.

Incaricato

Non più espressamente previsto, ma il responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento che abbia accesso a dati personali **non può trattare tali dati se non è istruito** dal titolare del trattamento.

Interessato

È la persona fisica identificata o identificabile cui si riferiscono i dati personali. È il baricentro della normativa che deve essere interpretata sempre a sua tutela.

All'interessato si ricollegano principalmente i **diritti** mentre agli altri i doveri.

- La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un **diritto fondamentale**.
- Il trattamento dei dati personali dovrebbe essere **al servizio dell'uomo**; il diritto alla protezione dei dati di carattere personale **non è prerogativa assoluta**, ma **va temperato con altri diritti fondamentali**.

Diritti dell'Interessato

- Conoscitivi
 - Diritto a ricevere l'informativa
 - Diritto di richiedere ed ottenere informazioni (accesso)
 - Diritto a ricevere informazioni in caso di violazioni (comunicazione data breach)
- Di controllo sul trattamento
 - Diritto al consenso e autorizzazione al trattamento
 - Diritto a revoca del consenso ed opposizione
 - Diritto alla limitazione del trattamento
- Di Intervento sui dati
 - Portabilità rettifica ed integrazione (modifica)
 - Cancellazione ed oblio (eliminazione)
- Di non essere sottoposto a decisione basata unicamente sul trattamento automatizzato, compresa la profilazione che produca effetti giuridici che lo riguardano.
Significa che, se il trattamento dei dati porta a qualcosa di giuridico, serve anche l'intervento umano. (Mutuo banca)

Responsabile della protezione dei dati (DPO)

Verifica e vigila (sia come figura interna che esterna) che il trattamento dei dati rispetti le normative ed i diritti; informa e consiglia sulle modalità; è il punto di contatto con le autorità di controllo.

È obbligatorio in 3 casi:

- Autorità pubblica o organismo pubblico (tutti gli enti pubblici devono farlo);
- Controllo regolare e sistematico degli interessati su larga scala;
- Trattamento, su larga scala, di categorie particolari di dati.

Un gruppo di imprese può nominare un unico DPO.

È coinvolto in tutte le questioni relative al trattamento dati.

Non deve ricevere istruzioni e non dev'essere in conflitto di interessi.

Autorità di Controllo (Garante Privacy)

Ogni stato membro del GDPR dispone di un'Autorità per la Protezione dei Dati. Le Autorità sono riunite nel Comitato Europeo.

Si tratta di **Autorità Amministrative Indipendenti** (Authority) che, quindi, non rispondono direttamente all'autorità statale ma a quella europea.

In Italia: Autorità Garante Privacy.

L'Autorità Garante ha funzioni di **controllo normativo** sulle materie di competenza nazionale.

Sono quattro membri eletti ogni 7 anni dal parlamento.

L'attività ispettiva del Garante è svolta dai Funzionari e dalla Guardia di Finanza Nucleo Privacy.

Liceità del Trattamento

Il titolare del trattamento adotta misure adeguate a fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare per informazioni destinate ai minori. Le informazioni sono presentate **per iscritto** o con altri strumenti elettronici.

Può anche essere esposta oralmente purché comprovata con altri mezzi l'identità dell'intestatario.

In caso di raccolta di dati dell'interessato, il titolare fornisce le seguenti informazioni:

- **Identità** e i **dati di contatto del titolare** del trattamento;
- I **dati di contatto del responsabile** dei dati;
- Le **finalità del trattamento** cui sono destinati i dati personali nonché la base giuridica del trattamento;
- Gli eventuali **destinatari** o le eventuali **categorie di destinatari**;
- L'**intenzione** del titolare del trattamento di **trasferire dati personali** ad un paese terzo o a un'organizzazione internazionale;
- Il **periodo di conservazione** dei dati personali o, se non possibile, i **criteri utilizzati** per determinare tale periodo;
- L'esistenza del **diritto dell'interessato** di chiedere al titolare del trattamento **l'accesso ai dati personali**, la **rettifica**, l'**eliminazione** o la **limitazione**;
- Il **diritto ad opporsi** al trattamento oltre al diritto di portabilità dei dati;
- Il **diritto di revocare il consenso in qualsiasi momento**
- L'esistenza di un **processo decisionale automatizzato** di proliferazione e, nel tal caso, informazioni sulla logica utilizzata, nonché l'importanza e le conseguenze.

Il trattamento è **lecito** solo se ricorre almeno una delle seguenti condizioni:

- L'interessato ha espresso il **consenso** al trattamento;
- Il trattamento è **necessario all'esecuzione di un contratto**;
- Il trattamento è **necessario per adempiere un obbligo legale** al quale è soggetto il titolare;
- Il trattamento è **necessario per la salvaguardia degli interessi vitali** dell'individuo o di un terzo;
- Il trattamento è necessario per l'**esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri**;
- Il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento** o di terzi a patto che non violino i diritti precedenti.

Il **consenso dell'interessato** deve essere espresso mediante un **atto positivo inequivocabile** con il quale l'interessato manifesta l'intenzione al trattamento. (No silenzio, inattività o preselezione di caselle).

- Se il trattamento ha **più finalità** il consenso deve essere **prestato per ognuna di queste**.
- Se il trattamento è basato sul consenso, il titolare deve essere in grado di **dimostrare che l'interessato ha dato il proprio consenso**.
- Se il consenso è scritto deve essere **facilmente comprensibile** ed accessibile.
- L'interessato ha il diritto di **revocare** il proprio consenso in qualsiasi momento.
- Il **consenso deve essere libero**, non ci possono essere condizioni contrattuali che ti vincolano ad accettare.

Data Breach

VIOLAZIONE DELLA SICUREZZA CHE COMPORTA ACCIDENTALMENTE O IN MODO ILLECITO LA DISTRUZIONE, LA PERDITA O MODIFICA, LA DIVULGAZIONE NON AUTORIZZATA O ACCESSO AI DATI PERSONALI TRASMESSI, CONSERVATI O COMUNQUE TRATTATI.

- **Confidentiality breach:** in caso di divulgazione o accesso non autorizzato o accidentale a dati personali
- **Availability breach:** in caso di cancellazione / distruzione non autorizzata o accidentale di dati personali
- **Integrity Breach:** in caso di modifica non autorizzata o accidentale di dati personali

Notifica di una violazione di dati

Il titolare del trattamento notifica la violazione all'Autorità di Controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche.

Se ci vogliono più di 72 ore nella notifica, va allegata la motivazione del ritardo.

Nel caso di **violazioni multiple** (ovvero se, da quando nota la prima a quando la notifica, ne nota altre) il titolare può effettuare una notifica unica contenente le diverse violazioni, qualora tali violazioni **riguardino le stesse categorie di dati** e si siano verificate tramite le **stesse modalità**.

Se invece sono modalità diverse deve notificarne ognuna singolarmente.

Comunicazione di una violazione di dati

Se la violazione comporta un rischio elevato per i diritti e le libertà delle persone fisiche, la comunicazione al cliente deve essere effettuata senza ingiustificato ritardo.

La comunicazione all'interessato invece **non è richiesta se** il titolare:

- ha messo in atto misure tecniche e organizzative adeguate di protezione;
- ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato;
- detta comunicazione richiederebbe uno sforzo troppo elevato, in tal caso si fa una dichiarazione pubblica.

DIRITTO PENALE

Il nostro Codice penale (Codice Rocco) risale al 1930 ed è diviso in due blocchi principali.

La prima non tratta direttamente dei singoli reati ma in generale degli strumenti per applicare correttamente il diritto nei casi.

È un settore dell'ordinamento giuridico dello Stato ed è caratterizzato dalla natura della conseguenza giuridica che deriva dalla violazione delle sue prescrizioni, ovvero dalla pena.

In particolare, il diritto penale è l'insieme di norme giuridiche con le quali lo Stato proibisce, mediante minaccia di una pena, determinati comportamenti umani che possono consistere in azioni ed omissioni.

La **pena** è definita in generale come una **sofferenza che lo stato infigge alla persona che ha violato un dovere giudiziario** e consiste nella **privazione o diminuzione delle libertà personali o di un bene individuale** come il patrimonio.

Principio di Legalità:

nessun crimine e nessuna pena se non c'è una **legge** nelle quale rientra la casistica (non decreto-legge ma proprio legge).

- **Articolo 25 costituzione:** si può essere puniti solo per una legge che sia entrata in vigore prima del fatto commesso.
- **Articolo 1 Codice penale:** non si può essere puniti per un fatto che non sia espressamente preveduto come reato dalla legge, né con pene che non siano da essa stabilite.

Si basa su:

- **Riserva di legge:** solo il potere legislativo possiede il monopolio normativo in materia penale (non esecutivo o giudiziario);
- **Tassatività:** riguarda le tecniche di formulazione delle norme penali (devono indicare precisamente ciò che è penalmente illecito e vige il divieto per il giudice di fare ricorso ad analogie);
- **Irretroattività:** riguarda la validità nel tempo della legge penale; le leggi sfavorevoli (quindi di colpa) non sono retroattive mentre quelle di favore (decaduta, modifica di una legge penale) sono retroattive. (se vado in carcere per un reato X e poi il reato X decade, esco)

Il Reato

Si suddivide in **delitto** e **contravvenzione**.

Il soggetto attivo del reato (agente, reo) può essere SOLO la persona umana.

Sono state comunque introdotte le responsabilità di Enti ed Aziende tali che, per quanto un reato magari (come falsificazione di documenti aziendali) non sia diretto da una persona umana, il guadagno del reato va sull'azienda.

Capacità Penale:

riguarda tutti indistintamente (dal momento che sei un soggetto, sei un soggetto penale e hai la capacità di essere giudicabile).

Capacità alla pena:

presuppone l'imputabilità (se hai meno di 14 anni o se non sei capace di intendere o volere nel momento del reato, non sei legalmente imputabile).

Le norme penali sono costituite da due elementi:

- **Precetto**: il comando di tenere una certa condotta (di non compiere una determinata azione) - il più delle volte è implicito (per l'omicidio non c'è scritto "non uccidere" ma "chiunque cagiona la morte di un uomo è punito con la reclusione...");
- **Sanzione**: è la conseguenza giuridica che deve seguire l'infrazione del precetto. Fornisce un'indicazione per l'applicazione della pena (da 3 mesi a 6 anni, da 10€ a 1000€ di multa).

Norma Penale in bianco: la descrizione del precetto è destinata a fonti extra-penali, ossia a norme che provengono da altri rami dell'ordinamento (come quello amministrativo), mentre la sanzione è esplicitata.

Ad esempio, art 650 c.p. in materia di contravvenzioni che sanziona con "l'arresto fino a tre mesi o con l'ammenda fino a €206" il comportamento di "chiunque non osservi un provvedimento legalmente dato dall'Autorità per ragione di giustizia o di sicurezza pubblica, o di ordine pubblico o di igiene" formulando così un precetto in modo generico.

Viene usata in ambiti molto specifici e tecnici (esempio le sostanze stupefacenti) dove viene rimandata la costruzione del precetto ad un organo altamente specializzato ed in grado di aggiornare rapidamente le informazioni (nuove sostanze droganti che non sono attualmente in una tabella di sostanze vietate, fare tutti i passaggi dalla camera ecc. per aggiornarla è troppo lungo).

Bene Giuridico / Interesse Tutelato

Ogni norma penale tutela un determinato bene o interesse.

L'oggetto giuridico del reato è il **bene giuridico o l'interesse giuridico tutelato dalla norma** che prevede il reato (ad esempio, la norma che punisce il "furto" tutela il bene giuridico del "patrimonio").

L'individuazione dei beni protetti va fatta tenendo conto dei principi sanciti dalla Costituzione.

L'oggetto giuridico non va confuso con l'**oggetto materiale dell'azione** (nel caso di un furto d'auto il bene giuridico è rappresentato dal patrimonio, mentre l'oggetto materiale dell'azione è il veicolo in sé).

Com'è strutturato il Reato?

Si compone di svariati elementi che devono tutti essere presenti per poter ritenere realizzata la fattispecie criminale prevista dalla legge:

- **Condotta-Evento**: elemento essenziale e fondamentale – senza condotta non può esserci reato, mentre può esserci reato senza evento (tipo omissione di soccorso). La condotta può consistere sia in **azione** che in **omissione** (violazione di un dovere giuridico).
L'evento è risultato della condotta, a cui è legato per nesso causale. Non tutti i reati prevedono l'esistenza di un evento (distinguiamo **reati di evento** e **reati di pura condotta**). Si parla di **reati ad effetto differito** quando l'evento segue a distanza di tempo la condotta e di **reati a distanza** quando l'evento si verifica in un luogo diverso da dove si è svolta la condotta (es. lesioni via internet). Altra distinzione è fatta da evento **di danno** o **di pericolo**.
- **Rapporto di causalità**: per poter attribuire all'agente un fatto penalmente illecito è necessario che condotta ed evento siano tra loro legati da nesso causale (faccio una cosa e di conseguenza ne succede un'altra).
- **Caso fortuito**: fattori causali preesistenti, concomitanti o sopravvenuti che hanno reso eccezionalmente possibile il verificarsi di un evento imprevedibile; si parla di **non punibilità**.

- **Forza Maggiore:** forze naturali sopravvenute esterne all'agente; si parla di **non punibilità**.
- **Offesa-Elemento soggettivo:** storicamente c'era la responsabilità per fatto altrui (un dodicenne ammazza qualcuno, i genitori ne pagano le conseguenze) e la responsabilità oggettiva (responsabilità di un reato indipendentemente dallo stato psicofisico). Ora è stato cambiato con **responsabilità colpevole** (fatto proprio tenendo conto dello stato psichico) e **responsabilità personalizzata** (tenere conto dello stato del soggetto e non generalizzare la situazione).

La Colpevolezza

La colpevolezza si basa su 3 capisaldi:

- **Imputabilità:** avere un'età superiore ad un certo limite, la capacità di intendere e volere al momento della condotta;
- **Conoscenza / Conoscibilità del precetto penale:** la legge non ammette ignoranza, se non conosci la norma non cambia la tua responsabilità. Tuttavia, data l'enorme quantità di norme esistenti, l'ignoranza inevitabile è giustificabile (come, ad esempio, quando ci sono più norme contraddittorie o poco chiare).
- **Dolo o Colpa:**
 - **Dolo:** è rappresentazione e volontà del fatto materiale tipico e quindi di tutti gli elementi (oggettivi-positivi-negativi) della fattispecie di reato. Nel doloso rientra il volontario (investo delle persone volontariamente);
 - **Colpa:** storicamente più recente, meno grave del dolo. È un rimprovero per aver realizzato, seppur involontariamente tramite la violazione delle regole cautelari di condotta, un fatto-reato che avrebbe potuto essere evitato mediante l'osservanza esigibile di detta regola (si rompe un freno perché non l'ho fatto revisionare ed investo una persona).

La colpa si compone di: mancanza di volontà del fatto, inosservanza della regola di condotta, attribuibilità dell'inosservanza all'agente.

La Preterintenzione

Vi è la volontà di un evento minore e non volontà di un evento più grave. Esistono solo due ipotesi di reato preterintenzionale: l'omicidio e l'aborto.

- **Omicidio Preterintenzionale:** faccio una rissa, tiro un pugno e l'altra persona muore. Non c'era l'intenzione di uccidere ma l'intenzione di ferire.
- **Aborto Preterintenzionale:** percuoto una donna incinta e lei perde il bambino. L'intenzione non era perdere il bambino ma è capitato comunque quindi ne rispondo.

DIFFAMAZIONE E SOCIAL NETWORK

Ingiuria:

illecito depenalizzato (in principio era illecito penale, ora illecito civile) sotto Governo Renzi.

Elementi dell'ingiuria:

- Chiunque offende l'**onore** o il **decoro** di una persona presente.
- Anche mediante comunicazione telegrafica o telefonica, o con scritti o disegni, diretti alla persona offesa.
- Pena era aumentata se l'offesa era commessa in presenza di più persone (da valutare in sede civile)

Diffamazione:

Chiunque, comunicando con più persone (anche in momenti diversi), offende l'altrui **reputazione**, è punito con la reclusione fino a un anno o con la multa fino a euro 1032.

Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità (come i social) ovvero in atto pubblico, la pena è la reclusione dai sei mesi ai tre anni o la multa non inferiore a 516 euro (diffamazione aggravata).

Se l'offesa è recata ad un Corpo politico, amministrativo o giudiziario, le pene sono aumentate.

Se la persona non è presente, è più diffamazione che ingiuria.

- **Decoro**: complesso di valori e atteggiamenti ritenuti confacenti a una vita dignitosa, riservata, corretta.
- **Onore**: elemento personale che costituisce motivo di soddisfazione, di vanto.
- **Reputazione**: considerazione in cui si è tenuti dagli altri.

▪ Reato a forma libera:

la condotta diffamante risulta fatta ogniquale volta venga offesa la reputazione di una persona, in assenza del soggetto passivo con qualsiasi mezzo idoneo comunicando con più persone. Non è espressamente descritta la modalità nella quale viene fatto il reato (reato per omicidio non descrive tutte le modalità ma in generale l'omicidio, quindi è reato a forma libera).

▪ Reato di danno:

per la cui configurabilità è necessaria la realizzazione dell'evento inteso quale percezione e comprensione dell'offesa da parte di più persone. Ovvero non basta l'intenzione ma serve anche l'esecuzione del reato.

Libertà di Pensiero:

tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.

La stampa non può essere soggetta ad autorizzazioni o censure. Ci sono delle linee guida affinché una manifestazione di pensiero rientri nel diritto di critica e di cronaca:

- **Veridicità** – non è possibile accusare una persona sulla base di notizie false (video ritagliati ad hoc);
- **Continenza** – moderazione nel come viene manifestato il dissenso;
- **Interesse pubblico** – utilità/rilevanza per la comunità (ci deve essere un'utilità per le persone che ascoltano quel che dici).

Diffamazione e Museo Egizio

“Fortunato chi parla arabo” campagna promozionale lanciata dalla Fondazione delle Antichità Egizie di Torino (M.A.E.) per cercare di avvicinare la comunità araba alle collezioni del Museo Egizio attraverso l’ingresso 2x1. Un esponente politico pubblica sulla propria pagina Facebook un video che riporta una telefonata polemica con un centralinista del museo accompagnato da *“Al Museo Egizio ingressi gratuiti per gli arabi. E gli italiani? Pagano”*. Dopo aver espresso sul sito e sulla pagina istituzionale del museo i dubbi sull’autenticità del video, la Fondazione M.A.E. presenta un esposto alla Questura di Torino, sollecitando le indagini. Ottenuta la conferma di non autenticità del video, la Fondazione porta in giudizio l’esponente politico per sentirlo condannare al pagamento di 100mila euro e alla rimozione dei contenuti offensivi dai social.

Motivi della sentenza per diffamazione:

- Non conformità della condotta al requisito di verità;
- Mancato rispetto del requisito della continenza (termini aggressivi ad una comunità).

Truffa:

Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno.

Atti di concorrenza sleale:

- Diffusione di notizie e apprezzamenti su prodotti e sull’attività di un concorrente, idonei a determinare il discredito;
- appropriamento di pregi dei prodotti o dell’impresa di un concorrente.

Sottolineare con eccessivi punti esclamativi, maiuscolo eccessivo, dichiarare di aver fatto denuncia di un locale, contraddizioni nel commento, non chiarezza nel perché della critica ecc. sono tutte componenti che portano a definire un commento come potenzialmente diffamatorio.

In generale la pubblicazione di contenuti attraverso i social network rappresenta senza dubbio una forma di “comunicazione con più persone” e, pertanto, corrisponde perfettamente alla fattispecie delineata nella **diffamazione aggravata**.

Diffamazione e TripAdvisor

Recensore deve risarcire Iginio Massari:

“Se questa è la tua pasta di mandorle allora non sai cosa sia la realtà. La crema pasticcera è vomitevole. Sarai pure un pasticcere stellato, ma se vuoi imparare a lavorare devi assaggiare i nostri prodotti del sud Italia”.

La recensione non presenta moderazione dei termini e non esprime informazioni di utilità per la comunità.

Diffamazione e Meta:

Se offendo qualcuno attraverso WhatsApp è Ingiuria o Diffamazione?

Analisi di possibili diffamazioni:

- Pubblicare messaggi offensivi sulla reputazione della ex-fidanzata sul proprio stato di Whatsapp è diffamazione? **SI**
- Pubblicare messaggi offensivi sulla reputazione dell'ex-fidanzata sulla chat di gruppo di Whatsapp (due o più persone) in cui non è presente la ex? **SI**
- Pubblicare messaggi offensivi sulla reputazione dell'ex-fidanzata sulla chat di gruppo di Whatsapp (due o più persone) in cui è presente la ex? **Dipende: è Ingiuria** (se la persona offesa è on-line e risponde attivamente) **o Diffamazione** (quando il messaggio offensivo è già stato letto da almeno altri due partecipanti prima che venga visualizzato dalla persona offesa).

DOCUMENTI E FIRME ELETTRONICHE

Fonti Normative:

- **Codice dell'Amministrazione Digitale** noto anche come (**CAD**) [2005].
- Regolamento (UE) del Parlamento europeo del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno [2014 / 2016 - **eIDAS**].
Base normativa a livello comunitario per i servizi fiduciari degli stati membri, ossia servizi di **identificazione digitale**, **firma elettronica** nonché **servizi di recapito elettronici**.

Tipi di Documenti:

Documento Elettronico: qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (ANCHE i documenti vuoti, qualunque documento di base).

Documento Informatico: il documento elettronico che contiene la **rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti** (ovvero che abbia effetti sulla sfera giuridica del soggetto, es. responsabilità, diritti, obblighi...).

Documento Analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Firme Elettroniche:

abbiamo 4 tipologie di firme, le prime tre sono regolamentate da UE, l'ultima da CAD.

Firma Elettronica (c.d. Semplice): insieme di *“dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare”*.

Tre categorie, a seconda che il meccanismo si basi:

- Sulle conoscenze dell'utente (conoscenza di una parola chiave);
- Sulle caratteristiche fisiche dell'utente (impronta digitale o retina);
- Sul possesso di un oggetto da parte dell'utente (tessera magnetica).

Firma Elettronica Avanzata: si possono firmare tutti gli atti ad esclusione dei contratti relativi a beni immobili.

Deve rispettare alcuni requisiti:

- Connessa unicamente al firmatario;
- Idonea a identificare il firmatario;
- Creata mediante dati per la creazione di firma elettronica che esclusivamente il firmatario può utilizzare;
- Collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Firma Elettronica 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 verificata da soggetti pubblici o privati che sotto la vigilanza di agID emettono **certificati** qualificati.

N.B: il concetto di certificato non è menzionato nella definizione di firma elettronica avanzata.

Firma Digitale: “un particolare tipo di firma qualificata basata su un **sistema di chiavi crittografate**, una pubblica ed una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la **provenienza** e l'**integrità** di un documento informatico o di un insieme di documenti informatici”. Viene scelta una crittografia a chiavi asimmetriche che garantisce un livello di sicurezza molto elevato.

Come funziona la firma Digitale (CADES):

1. L'applicativo di firma calcola l'impronta (evidenza informatica) del file attraverso un algoritmo di Hash che deve essere unico per ogni file;
2. L'app di firma cifra l'impronta (digiset) usando la chiave privata memorizzata sul certificato di firma che deve avere determinati requisiti di robustezza;
3. La sottoscrizione così generata da un determinato file è sempre identica, indipendentemente dal programma che la genera.
4. Il documento sottoscritto, l'impronta cifrata ed il certificato dell'ente certificatore sono inseriti in una busta unica (.p7m).

Come avviene poi la certifica? Quando ricevo la busta, la apro, tiro fuori il certificato dell'ente certificatore, tiro fuori l'impronta (hash) cifrata con la mia firma privata (del firmatario), ho poi ancora il file originale (in chiaro). A questo punto con la funzione di hash ricalcolo l'impronta dal file originale e decifro con la mia chiave pubblica l'evidenza che avevo cifrato.

Se le due impronte coincidono allora il file non è stato modificato.

Legalmente: l'utilizzo del dispositivo di firma qualificata o digitale si presuppone riconducibile al titolare, salvo che questi dia prova contraria. Inoltre, il titolare della firma è tenuto ad assicurare la custodia del dispositivo di firma ed è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

Un documento informatico soddisfa il *requisito di forma scritta* e ha l'*efficacia prevista* quando vi è apposta:

- una firma digitale;
- un altro tipo di firma elettronica qualificata;
- una firma elettronica avanzata;
- è formato, previa identificazione informatica del suo autore mediante processi fissati dall'AgID, con modalità tali da garantire sicurezza, integrità e immodificabilità del documento e, in maniera inequivoca, la sua riconducibilità all'autore (SPID / Carta Identità Elettronica).

In tutti gli altri casi (firma semplice o non sottoscritto) l'idoneità del documento informatico è liberamente valutabile in giudizio (quindi dal giudice) tenendo conto delle relazioni di sicurezza, integrità e immodificabilità.

POSTA ELETTRONICA CERTIFICATA (PEC)

È un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con piena valenza legale, attestante l'invio e la consegna di documenti informatici. È la versione digitale della Raccomandata.

Sono soggetti del servizio di posta elettronica certificata:

- il **mittente**, cioè chi si avvale del servizio per la trasmissione di documenti prodotti mediante strumenti informatici;
- il **destinatario**, cioè chi si avvale del servizio per la ricezione dei documenti;
- il **gestore del servizio**, cioè il soggetto pubblico o privato che eroga il servizio di posta elettronica certificata e che gestisce domini di posta elettronica certificata.

Trasmissione del documento informatico:

Il documento informatico trasmesso per via telematica si intende **spedito dal mittente** se inviato al proprio gestore, e si intende **consegnato al destinatario** se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione del gestore.

NOTA BENE che non implica la presa in lettura ma solo la consegna: una volta consegnato è legalmente valido.

Viene fornito al mittente:

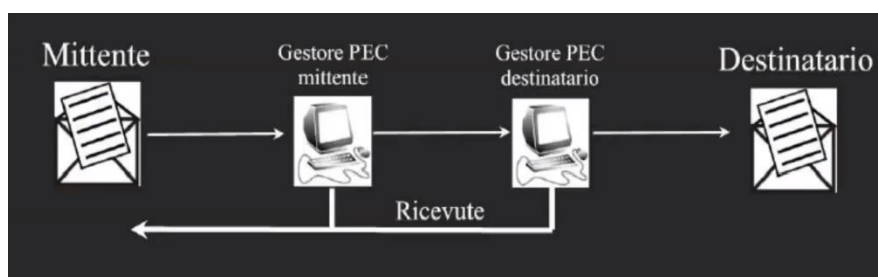
- **Ricevuta di accettazione** nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione di un messaggio di posta elettronica certificata. (Certifica INVIO)
- **Ricevuta di avvenuta consegna** nella quale certifica il momento della consegna e la resa disponibile nella casella di posta indipendentemente dalla lettura. (Certifica CONSEGNA)

Se il messaggio non risulta consegnabile, entro 24 ore, il gestore lo comunica al mittente tramite un avviso.

Le **ricevute** rilasciate dai gestori di posta sono **sottoscritte dal gestore** mediante la firma elettronica avanzata generata automaticamente dal sistema di posta elettronica.

Il gestore del mittente, prima di consegnare, deve verificare l'assenza di virus informatici a scopo dannoso e, nel caso ci fossero, è tenuto a non accettare i documenti informando tempestivamente il mittente dell'impossibilità di trasmissione; in tal caso il gestore conserva i messaggi per 30 mesi.

Allo stesso modo, qualora il gestore del destinatario riceva messaggi con virus informatici, è tenuto a non inoltrarli al destinatario, informando il gestore del mittente; anche in questo caso i messaggi vengono conservati per 30 mesi.



COME FUNZIONA UN PROCESSO PENALE

Indagato: colui che è sotto indagine

Imputato: quando il PM (pubblico ministero) rinvia a giudizio e formula un'imputazione

Notizia di reato: fatto di cui viene a conoscenza PM/organi di polizia e che comporta un possibile reato

Giudice preliminare: verifica che il PM abbia lavorato correttamente verifica i dati esposti e valuta quali sono necessari al fine del procedimento, per le prove preliminari che rischiano di deteriorare o di non essere + accessibili interviene con anticipo (quindi tipo interrogatorio di una persona che potrebbe decedere)

Misure preliminari: atti preventivi al fine dell'indagine che servono ad evitare qualche atto dei colpevoli (firme, domiciliari, carcere preventivo...)

Intercettazioni telefoniche ed informatiche: al fine delle indagini possono essere necessarie intercettazioni, nel limite del consentito, per eventi di pericolo pubblico

Sequestri e perquisizioni: fanno parte (tendenzialmente) di componenti preliminari del processo. Si tratta di elementi non ripetibili (una volta che ho sequestrato X, lo ho durante il processo. Non deve avvenire un secondo sequestro)

Il PM in Italia, a differenza dell'America ad esempio, non ha la facoltà di scegliere quali processi penali seguire e quali non. Ha il vincolo di Obbligatorietà, ovvero obbligo di intervento sempre. Chiaramente in condizioni nelle quali un singolo PM deve dedicarsi a tre omicidi ed una rapina, gli omicidi hanno la priorità.

Quando un PM ha raccolto sufficienti prove da ritenere possibile un procedimento giuridico, deposita gli atti ed il difensore dell'imputato viene a conoscenza di quali sono gli atti compiuti dal PM.

A questo punto il giudice preliminare, in presenza di avvocati difensori, PM e avvocati civili, qualora ci fossero, si esprime rispetto al rinvio a giudizio dell'imputato o rispetto al fatto che a suo parere questo procedimento non porterà ad una colpevolezza dell'imputato.

L'imputato può scegliere delle vie più rapide per la conclusione del processo come, ad esempio, il patteggiamento, tale per cui PM ed imputato (avvocati) concordano rispetto ad una pena da proporre al giudice. Chiaramente la pena deve rispettare le normative di legge ed essere accettata. Mediante il patteggiamento, l'imputato guadagna la non responsabilità civile (quindi il risarcimento dei danni monetari) ma prende comunque in carico le spese processuali.

Il giudice si riserva comunque la facoltà di ignorare (assolvendo o cambiando la pena) il patteggiamento processuale proposto.

Il giudice preliminare, quindi, valuta tutte le circostanze e decide se rimandare al vero e proprio processo (rimandare a giudizio). Nel qual caso applica all'imputato (non condanna ma applica) le pene proposte dal PM o dagli accordi sviluppati.

Giudizio a rito abbreviato:

l'imputato richiede il *procedimento a rito abbreviato* quindi il processo parte solo dal materiale raccolto dal PM nelle indagini preliminari e senza il dibattimento (udienza preliminare). Questo permette di accorciare i tempi di processo. Se l'imputato viene condannato al termine, avrà uno sconto di metà pena nel caso di contravvenzioni o di un terzo per i delitti.

Una volta rinviato al giudizio, passa alla seconda parte con il giudice dipartimentale: qui vengono ripresentate le prove e i testimoni; vengono richieste ulteriori indagini qualora necessarie.

A fine di questo processo il giudice si esprime in maniera inequivocabile e senza dubbio rispetto alla sentenza di assoluzione o di condanna (senza dubbio, quindi fintanto che ne ha il processo continua).

Una volta espresso in maniera definitiva, sia difensori che PM possono fare ricorso in cassazione se reputano la sentenza inadeguata.

Nel processo: imputato, difensori e PM devono essere presenti e direttamente rappresentati, altrimenti il processo è nullo.

La parte civile invece può decidere se prendere parte o meno al processo penale.

COMPUTER CRIME

Reato che:

- Implica l'uso di un sistema informatico (ad esempio accesso abusivo a sistema informatico);
- Coinvolge un apparato informatico quale oggetto su cui ricade l'azione commessa dal soggetto agente (ad esempio casi di diffamazione/ingiuria o truffa).

ACCESSO ABUSIVO A SISTEMI INFORMATICI O TELEMATICI

*“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 ...”.*

Questo significa che il reato scatta già solo per aver effettuato l'accesso. Non è necessario danneggiare o rubare dei dati, basta aver fatto l'accesso.

Se invece trovo un telefono senza PIN e lo sblocco per vedere il proprietario, non sto commettendo reato fintanto che il mio uso è esclusivo verso il riconoscimento del proprietario.

Se un amico mi dà il suo PIN ed accedo al suo telefono è ok, se però discutiamo entro 24 ore devo lasciare l'accesso in quanto non è più una condizione di consenso.

Quanto riportato sopra comporta aggravanti se:

- l'atteggiamento è tenuto da un **pubblico ufficiale** o pubblico servizio che esercita il proprio potere;
- il soggetto che commette il reato **usa violenza su cose o persone** o è **palesamente armato**, ovvero ad esempio se hai su una chiavetta un tool per fare brute-force di password, è considerato palesamente armato;
- dal fatto deriva la **distruzione o il danneggiamento del sistema o l'interruzione totale/parziale del suo funzionamento** ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuto.

Se non ci sono aggravanti si procede a seguito di querela, altrimenti si può procedere direttamente d'ufficio.

Procedere d'ufficio significa che, quando arriva la notizia del reato (quando la polizia giudiziaria, PM, giudice vengono a conoscenza del reato) si agisce nell'immediato con il procedimento penale.

Procedimento per querela invece avviene come nel precedente ma serve anche una denuncia o querela della persona offesa rispetto a quel reato.

La **competenza territoriale** si radica **nel luogo in cui si trova a postazione remota** (client) di chi commette l'illecito. L'atto fisico della trasmissione dei dati da parte dell'operatore, una volta avviata, non è bloccabile e determina automaticamente il superamento delle barriere informatiche di accesso e pone automaticamente il soggetto agente nella condizione di consultare le informazioni contenute nella banca dati. In tal senso **non rileva** quindi **il luogo in cui si trova il server a mezzo del client** (mezzo fisico di trasmissione).

Se invece, ad esempio, un ex dipendente di un'azienda **copia e rivende** dei dati o comunque li ridistribuisce, per quanto l'accesso al sistema informatico non sia stato violato dal rompere una password, commette comunque il reato di andare contro la volontà del titolare (implicita o meno) di non accedere a quei dati.

Anche l'accesso abusivo ad aree riservate o impedita da password comporta reato.

DANNEGGIAMENTO INFORMATICO

Il danneggiamento informatico nel caso di accesso abusivo ad un sistema *implica un aggravante al reato*, non si tratta di concorso di reati (somma di due reati) ma invece si tratta di uno unico aggravato.

REVENGE PORN

Chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito destinati a rimanere privati, senza il consenso delle persone rappresentate, è **punito con la reclusione da uno a sei anni e con la multa da 5 a 15 mila euro**.

La stessa pena si applica a chiunque, avendo ricevuto o acquisito le immagini o i video, a sua volta li invia, cede, ... senza il consenso.

La pena è aumentata se i fatti sono commessi da coniuge, anche separato o divorziato, o da persona che è stata legata da relazione affettiva alla persona offesa.

La pena è aumentata di un terzo o di metà qualora venisse recato ad una donna incinta, una persona in inferiore condizione fisica o psichica.

La pornografia virtuale con volti di persone reali è un reato in quanto lede il bene giuridico di un soggetto.

Nel caso di volti e corpi completamente generati e non esistenti invece no.

Rispetto alla pedopornografia virtuale, oltre a tutti i reati di base che comporta, nel caso fosse generata un immagine/video rappresentati minori inesistenti in attività esplicitamente sessuali, lo spiccato realismo delle immagini o il non avere dubbi che si tratti di un infante, comporta reato in quanto il bene giuridico leso è generale. Lo scopo è quello di reprimere la diffusione di pratiche che, ancorché non riguardino un minore esistente, possano fungere da stimolo per potenziali vittime a farsi strumentalizzare a scopi sessuali e possano in ogni caso far proliferare il fenomeno.

Calunnia

Chiunque denunci un comportamento che sa per certo non essere avvenuto al fine di danneggiare il denunciato.

Un'aggravante è applicata se la denuncia fasulla comportasse una pena superiore ai 10 anni o più grave.

La pena per calunnia comporta dai 4 ai 12 anni se la pena della denuncia falsa comporta più di 5 anni. Dai 6 ai 20 se la pena comporta l'ergastolo (implicherebbe invece l'ergastolo se la pena comportasse la pena di morte).

FONDAMENTI DI DIRITTO INDUSTRIALE E PROPRIETÀ INTELLETTUALE

I diritti di proprietà intellettuale si distinguono in **due categorie** accumulate dall'ingegno dell'autore:

- **Diritto di proprietà industriale**
- **Diritto d'autore**

Le opere dell'ingegno sono classificabili in tre macrocategorie:

- Opere dell'ingegno creativo – fanno riferimento al mondo dell'arte e cultura
- Segni distintivi – quali marchio, ditta, insegna, indicazione geografica, denominazione d'origine
- Innovazioni tecniche e di design – hanno per oggetto invenzioni, modelli di utilità, disegni e modelli industriali, topografie di prodotti a semiconduttori, nuove varietà vegetali

Ulteriore distinzione tra

Diritti Titolati: ossia originati dalla brevettazione o registrazione

Diritti non Titolati: sorgono in presenza di determinati presupposti

Cos'è un BREVETTO?

Distinguiamo varie tipologie di brevetto.

Brevetto di Invenzione: le invenzioni, di ogni settore della tecnica, che sono **nuove** e che implicano un'**attività inventiva** e sono atte ad avere un'**applicazione industriale**.

Ha una durata di massimo 20 anni.

NON sono invenzioni:

- Scoperte, teorie scientifiche e metodi matematici
- Piani, principi e metodi per attività intellettuali, gioco o attività commerciale ed i programmi di elaboratore
- Presentazioni di informazioni

NON sono brevettabili:

- Metodi per trattamento chirurgico (sia umano che animale)
- Metodi per diagnosi (sia umana che animale)
- Varietà vegetali (compresi OGM) e razze animali + metodologie riproduttive
- Invenzioni Biotecniche sul corpo umano
- Invenzioni contro la dignità umana, contro l'ordine pubblico ed il buon costume
- Invenzioni contro la tutela della salute, dell'ambiente e della vita delle persone ed animali

Brevetto per modello di utilità: i nuovi modelli atti a conferire **particolare efficacia o comodità di applicazione** o di impiego a macchine, o parti di essere, strumenti, utensili od oggetti di uso in genere, quali i nuovi modelli consistenti in **particolari conformazioni, disposizioni, configurazioni o combinazioni di parti**.

Ha una durata di massimo 10 anni.

Cosa deve avere un Brevetto (in generale) per essere registrabile?

- **Novità:** un'invenzione è considerata nuova se non è compresa nello **stato della tecnica**, il quale è **costituito da tutto ciò che è stato reso accessibile al pubblico** nel territorio dello Stato o all'estero prima della data della richiesta di brevetto mediante scritto/orale, utilizzo o richiesta antecedente di brevetto (NOVITA' ASSOLUTA). Se è già stato brevettato ed è decaduto, non posso rinnovarne il brevetto. Se divulghi la tua idea sui social prima di registrarla, non è brevettabile.
- **Industrialità:** possibilità che il brevetto possa essere applicato in maniera industriale.
- **Liceità:** non contrarietà all'ordine pubblico ed al buon costume.
- **Attività inventiva e principio di non banalità:** l'invenzione implica un'attività inventiva se, per un esperto del ramo di sviluppo, essa non risulta ovvia. Attualmente solo le persone fisiche possono essere inventrici.

Relazione Tecnica di presentazione

I documenti per il brevetto sono essenzialmente 4:

- Descrizione
- Rivendicazione
- Disegni
- riassunto

La relazione è completata da titolo e traduzioni richieste dagli Uffici Competenti.

II MARCHIO

Il marchio può durare per sempre, basta pagare il rinnovo ogni dieci anni.

Il marchio è un **segno distintivo** che consente di:

- **Distinguere** i prodotti o i servizi di un'impresa da quelli di altre;
- **Riconoscere** la provenienza;
- **Associare** un prodotto e/o servizio alla storia, al prestigio o alla qualità di un'azienda.

È necessario identificare quali prodotti o servizi sono contraddistinti dal marchio.

Tipologie di marchi:

PRIMA DISTINZIONE

- **Denominativi:** parole, lettere, cifre, caratteri tipografici e combinazioni.
- **Figurativi:** stilizzazione o layout non standard di caratteri, riproduzioni grafiche
- **Figurativi contenenti elementi denominativi:** combinazione dei precedenti
- **Marchi di Forma:** forme distintive tridimensionali (tipo bottiglia di coca-cola)
- **Motivi ripetuti:** insieme di elementi che si ripetono sempre nei prodotti
- **Posizione:** posizionamento di un elemento su tutti i prodotti
- **Colore, combinazioni:** colore unico (viola = Milka), combinazioni
- **Sonori:** suono o combinazioni di suoni
- **Multimediali:** immagini + suono

SECONDA DISTINZIONE

- **Individuali:** distinguono i prodotti e servizi di un'azienda da un'altra
- **Collettivi:** distinguono prodotti e servizi di un gruppo di aziende/associazione dalla concorrenza
- **Certificazione:** indicano che i prodotti e servizi sono conformi ai requisiti di certificazione (DOCG)

Quando registro un marchio devo specificare quasi esattamente per cosa andrò ad usarlo categorizzandolo (non posso dire “servizi elettronici”, devo specificare precisamente). Devo quindi identificare per quali prodotti o servizi saranno distinti dal marchio.

Requisiti di un Marchio:

generalizzo parlando di logo ma intendo tutte le forme sopra elencate. Il marchio è strutturato per difendere il consumatore più che l'azienda.

- **Capacità distintiva:** il logo dev'essere utile a distinguere esattamente il prodotto. Se ho un negozio di frutta non posso usare una mela come marchio in quanto descrive un prodotto generico che tratto e non è distintivo rispetto agli altri.
Non posso quindi usare: denominazioni generiche di prodotti o servizi, indicazioni descrittive dei prodotti (la mela per il fruttivendolo)
- **Novità** (relativa): la novità è relativa e non assoluta, a differenza del brevetto, e si compone di:
 - anche se il marchio è utilizzato da qualche parte ma non ha notorietà nel territorio dove lo utilizzerai, posso registrarlo senza problemi. I marchi noti sono pochi (Apple, Gucci, ...)
 - il marchio che registro non deve essere accumulabile ad un altro della stessa categoria di prodotti per evitare di creare confusione nel cliente (negozio di borse di pelle “renne”, negozio di vestiti di pelle “renni” non si può)
- **Liceità:** non può andare contro legge ed ordine pubblico, buon costume. Non può trarre in inganno rispetto a provenienza, qualità ecc. Violazione di altrui diritto d'autore. (Ex. Qualcun ha provato a registrare “Covid” come nome di un'arma e gliel'hanno chiaramente rifiutato)
- **Rappresentazione**

Uso del Marchio

Il marchio (in Europa) è a titolo esclusivo del titolare in relazione al segno, prodotti e servizi ed al territorio per cui è richiesta la protezione. Questo ha come condizione il dovere del titolare di **usare in modo serio e continuativo** il marchio.

L'obbligo di utilizzo inizia dopo 5 anni dalla registrazione.

Se questo non viene fatto, dopo 5 anni è contestabile da chi fa denuncia per la rimozione del marchio (decadenza).

Dove tutelo un marchio?

- Deposito Italiano (UIBM): protezione valida in tutta Italia
- Deposito comunitario (EUIPO): protezione in tutta UE
- Deposito internazionale (WIPO): in tutti i Paesi aderenti alla Convenzione internazionale
- Deposito estero: deposito in Paesi non aderenti alla Convenzione internazionale

Se all'interno di un videogioco metto una borsa marcata Gucci che vendo come esclusiva (quindi non standard del gioco), posso farlo oppure no?

Sono nati per questa esigenza gli NFT (token non fungibili) per beni virtuali e servizi virtuali.

Gli NFT sono token digitali registrati su blockchain e sono utilizzati come certificati digitali unici in relazione a qualche oggetto.

Al pari dei certificati convenzionali, gli NFT in tale forma si riferiscono a qualcosa di diverso da loro stessi, il che significa che il termine NFT in quanto tale è inefficace ai fini della classificazione senza ulteriori specificazioni in merito all'oggetto al quale gli NFT si riferiscono.

Nike e Gucci, ad esempio, hanno registrato ed aperto dei negozi di abbigliamento nella piattaforma Roblox.

Altro caso quello delle borse Hermes: un tale ha registrato MetaBirkins che riprende il nome delle borse "Birkins" di Hermes (che non erano in alcun modo registrate in NFT). Hermes contesta dicendo che stanno vendendo delle "meta borse" ispirate ad un loro prodotto, con parte del loro nome e senza il diritto di farlo. Il tribunale dà ragione al venditore e non ad Hermes in quanto "MetaBirkins" viene ricollegato dagli utenti alla cosa online e non ad Hermes direttamente. Quindi le norme sul marchio in generale non sono sufficienti per tutelare anche online.

LEGGE SUL DIRITTO D'AUTORE

Sono protette ai sensi di questa legge le **opere dell'ingegno di carattere creativo** che appartengono alla letteratura, musica, arti figurative, architettura, teatro e cinematografia, qualunque ne sia il modo o la forma di espressione. Sono anche protetti i **programmi per elaborare** come opere letterarie ed artistiche nonché banche di dati o software.

Cosa non può essere protetto?

Idee e principi che stanno alla base di qualsiasi elemento di un programma (compreso materiale preparatorio per la progettazione del programma stesso).

La tutela delle banche di dati non si estende al contenuto ma solo alla forma.

Il **carattere creativo di un'opera** (requisito richiesto per la tutela) **non implica per forza la novità assoluta** ma corrisponde alla manifestazione del modo personale dell'autore di rappresentarla.

Non esiste un livello minimo di creatività, è una valutazione del giudice.

La creatività è riferita esclusivamente ad una persona fisica quindi le opere prodotte da intelligenza artificiale non sono ritenute creative.

Come registrare il Diritto D'Autore?

Generalmente non va esplicitamente registrato in quanto scatta dal momento in cui hai creato l'opera. Non bisogna fare nessun iter burocratico per registrare il diritto d'autore. Fintanto che puoi attestarne l'inizio della creazione, il diritto scatta.

Chiaramente per attestare l'inizio ci si può anche affidare ad enti come la SIAE.

- **Diritti Morali:** (inalienabili, gli eredi possono far valere i diritti senza limiti di tempo, non hanno scadenza)
 - diritto di rivendicare la paternità dell'opera
 - diritto di opporsi a qualsiasi deformazione, mutilazione, modifica o atto dannoso all'opera stessa che possano lederne la reputazione
 - diritto al ripensamento – se do in concessione la mia opera a terzi e poi me ne stufo, posso volere che venga rimossa dal mercato (probabilmente a fronte di un risarcimento danni)
- **Diritti Patrimoniali:** l'autore ha diritto esclusivo di pubblicare l'opera, utilizzarla economicamente in ogni forma e modo, riprodurla, trascriverla, eseguire, rappresentare o recitare in pubblico, ottenere un compenso da essa, comunicarla al pubblico, distribuirla, tradurla, noleggiarla (licenza d'uso).
Questi diritti sono alienabili e cedibili a terzi, durano per tutta la vita dell'autore fino a 70 anni dopo la sua morte e sono trasmissibili per eredità.

Diritto esclusivo di comunicazione al pubblico:

solo l'autore ha il diritto di distribuzione fintanto che non è morto da più di 70 anni. Quindi non posso ridistribuire un libro di qualcuno ancora in vita solo perché lui non lo fa da decenni.

Non sono nemmeno permesse pubblicazioni con piccole modifiche dell'opera o l'esposizione temporanea.

La **pirateria audiovisiva** è la ritrasmissione online senza diritto d'autore ed è imputabile. Dopo denuncia il fornitore del servizio si hanno 30 minuti per chiudere tutto quello che è collegato.

Anche scaricare musica online è illegale e sanzionabile (sia provider che utente).

Se un'intelligenza artificiale aiuta nella creazione di un'opera, il diritto di chi è?

Dipende da Stato a Stato, generalmente non si riconosce alle intelligenze artificiali il patrocinio delle opere in quanto devono essere per persone fisiche. Unico caso discostante è in Sud Africa.

C'è stato un caso di riconoscimento di diritto d'autore ad un'opera di AI in Cina ma in altri Stati non prende valore. Di base varia moltissimo da posto a posto, non c'è ancora nessuna linea esatta.

In definitiva: per esercitare i diritti d'autore, l'inventore deve avere una personalità giuridica di cui i sistemi o le macchine AI non godono.

I CONTRATTI

Il contratto è l'accordo di due o più parti per costruire, regolare o estinguere tra loro un rapporto giuridico patrimoniale.

Requisiti del contratto:

- **Accordo delle parti:** due o più persone manifestano reciprocamente le proprie volontà, e queste sono dirette allo stesso scopo. Si manifesta in due modi:
 - Tacito: l'intenzione al contratto è manifestata dal comportamento delle due parti;
 - Espresso: consiste in una dichiarazione specifica, scritta o orale, che contiene le volontà di concludere il contratto.
- **Causa:** è il riferimento alla funzione (strutturale) economica (in senso ampio) che le parti intendono realizzare con quel contratto (in un contratto di compravendita, la causa è scambio di "cosa" contro prezzo). Il motivo è soggettivo, non è parte del contratto (vendo la casa perché ho bisogno di soldi, non è parte del contratto). La causa dev'essere legalmente e moralmente valida (non puoi fare un contratto per andare a zozze). Le obbligazioni naturali sono quelle che trovano la propria fonte nei doveri morali e sociali che, pur non essendo giuridici, non sono indifferenti per l'ordinamento (morale).
- **Oggetto:** l'oggetto del contratto deve essere:
 - Possibile (non posso venderti la luna)
 - Lecito (non posso venderti droga)
 - Determinato o determinabile (non posso venderti "un po'" del mio terreno)
 - "Aleatorio" (ti vendo tutto quello che quell'albero produrrà, è determinabile seppur non ancora determinato)
- **Forma** (quando richiesta **ad Substantiam**):
 - Forma espressa / tacita
 - Forma scritta / orale
 - Contratti formali (Atto pubblico e scrittura privata) / contratti a forma libera (tipo comprare un giornale)
 - Forma ad substantiam (tipo gli atti notarili necessitano di essere scritti) / forma **ad probationem** (magari non è indispensabile che siano scritti ma meglio che lo siano per poterlo provare)

CONTRATTI TELEMATICI

Contratti stipulati per via elettronica, mediante l'uso di un computer.

Si distinguono in

- **Diretti**: avviene tutto online (compro una canzone online e la ho disponibile online)
- **Indiretti**: il contratto si conclude online e l'esecuzione no (compro delle scarpe online e poi me le spediscono)

Possono essere verso un pubblico indeterminato (ho un sito di vendita di prodotti) o tra parti determinate (scambio di e-mail per la creazione di un contratto).

Distinzione importante:

- Business (imprenditore/professionista) – colui che agisce al fine aziendale di compravendita, ha conoscenze maggiori alla media comune su uno specifico ambiente.
- Consumer (consumatore) – chi acquista per sé stesso e non per fine aziendale (posso anche essere un Padrone di fiat ma se compro una padella non per cose aziendali, sono Customer)

Business to business (B to B)

Business to consumer (B to C) tramite siti

- Ha delle norme inderogabili indipendenti dal contratto ed assolute a tutto (come il diritto di recesso di 14 giorni, è il diritto a cambiare idea).
- Ha una legislazione speciale a tutela dei consumatori.

Il Diritto Di Recesso

Secondo il Codice civile, un contratto stipulato non può essere sciolto se non per mutuo consenso o per cause ammesse dalla legge.

Una di tali cause è il **recesso unilaterale**: il consumatore può esercitare la facoltà di recedere dal contratto se questa è prevista dal contratto stesso e finché il contratto non abbia avuto un principio di esecuzione.

È garantito per tutti i contratti BtoC stipulati a distanza o negoziati fuori dai locali commerciali, garantisce di non dover sostenere costi supplementari e di restituzione (eventuale spedizione), ha valenza di 14 giorni.

Eccezioni:

- contratti di servizi la cui esecuzione è iniziata con l'accordo espresso dal consumatore e con l'accettazione della perdita del diritto di recesso a seguito della piena esecuzione del contratto da parte del professionista;
- fornitura di beni su misura e chiaramente personalizzati;
- fornitura di beni che rischiano di deteriorarsi o scadere;
- fornitura di beni sigillati che non si prestano ad essere restituiti per motivi igienici o connessi alla salute;
- fornitura di bevande alcoliche e beni il cui valore è legato a fluttuazioni di prezzo che il professionista non può controllare;
- il consumatore ha richiesto una visita da parte di un professionista per lavori urgenti di riparazione o manutenzione;
- fornitura di registrazioni audio o video sigillate o di software informatici sigillati che sono stati aperti dopo la consegna;
- fornitura di contenuto digitale mediante supporto non materiale se l'esecuzione è iniziata.

Diritto per richiedere la garanzia per il bene difettoso:

è previsto il diritto per l'acquirente di pretendere una garanzia generale quando la cosa venduta è rotta o il suo valore è nettamente diminuito a causa di difetti. Il compratore deve denunciare al venditore entro 8 giorni dalla scoperta il malfunzionamento e l'azione si prescrive entro un anno dalla consegna del bene.

Quando il venditore è un professionista e il compratore è un consumatore, il venditore è responsabile per qualsiasi difetto di conformità al momento della consegna del bene. In questo caso il consumatore deve denunciare i difetti entro due mesi dalla loro scoperta e l'azione si prescrive entro ventisei mesi dalla consegna.

A prescindere, esiste la garanzia di conformità: se compro un cellulare rosso e me ne arriva uno nero, posso renderlo indietro.

Clausole Vessatorie

Sono clausole inserite all'interno di un regolamento contrattuale che per loro contenuto comportano uno squilibrio di diritti ed obblighi a danno di una parte e a favore dell'altra.

Per quanto esistano, sono da esplicitare MOLTO bene e spesso vengono posti a fondo contratto per essere notabili.

Modalità di Conclusione del Contratto

Ci sono tre modalità di conclusione del contratto

1. **Scambio di proposta ed accettazione:** Parte A propone via mail, B accetta; quando A ne viene a conoscenza (la mail arriva al server del compratore) allora il contratto è chiuso.

Nei contratti telematici si ha la "presunzione di conoscibilità", ovvero non è indispensabile che sia stato letto l'aggiornamento, basta la resa disponibile effettiva della mail. ★

2. **Offerta al pubblico:** quando un offerente rivolge una proposta contrattuale a un'ampia cerchia di persone, chiamate destinatari. L'offerta viene resa pubblica ad esempio mediante sito web, pubblicità o comunicazioni di massa.
3. **Comportamento concludente** (non conclusivo, concludente): effettuare il bonifico per il prodotto.

★ **Trasmissione del documento informatico: concetto di Spedizione e Consegna**

Il documento informatico trasmesso per via telematica **si intende spedito** dal mittente **se inviato al proprio gestore**, e **si intende consegnato** al destinatario **se reso disponibile** all'indirizzo di posta elettronica da questi dichiarato.

RESPONSABILITA' INTERNET SERVICE PROVIDERS (ISP)

Si tratta di una direttiva Europea, non leggi vere e proprie ma direttive su come costituire localmente le proprie legislazioni.

Direttiva 8 giugno 2000: si pone come obiettivo quello di contribuire al buon funzionamento del mercato comune, garantendo la libera circolazione dei servizi della società dell'informazione tra gli Stati membri.

Decreto Legislativo 9 aprile 2003: è volto ad assicurare la libera prestazione dei servizi on-line nell'insieme della Comunità, creando regole uniformi per il commercio elettronico, che per sua stessa natura è senza frontiere.

Regolamento UE – Digital Markets Act

Entrerà in vigore a maggio 2023

Digital Service Act (DSA) – Responsabilità dei prestatori di servizi intermediari

- **Assenza di obblighi generali di sorveglianza o di accertamento attivo** dei fatti: i prestatori di servizi non sono i poliziotti del web, non devono sorvegliare le azioni degli utenti.
- **Semplice trasporto:** nella prestazione di un servizio consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario o nel fornire un accesso alla rete di comunicazione, il prestatore non è responsabile delle informazioni trasmesse a condizione che:
 - non dia origine alla trasmissione (non sono io entità a pubblicare qualcosa);
 - non selezioni il destinatario della trasmissione (non sono io a decidere a chi arriva);
 - non selezioni né modifichi le informazioni trasmesse;
 - non trattenga le informazioni per un tempo maggiore a quello necessario alla trasmissione.

Resta impregiudicata la possibilità che un organo giurisprudenziale o un'autorità amministrativa esiga al prestatore del servizio di impedire o porre fine ad una violazione.

- **Memorizzazione temporanea (caching):** nella prestazione di un servizio consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio (utente), il presentatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficiente il successivo inoltra delle informazioni ad altri destinatari su loro richiesta a condizione che:
 - Non modifichi le informazioni
 - Si conformi alle condizioni di accesso alle informazioni
 - Si conformi alle norme sull'aggiornamento delle informazioni
 - Non interferisca con l'uso lecito di tecnologia
 - Agisca prontamente per rimuovere le informazioni memorizzate, per disabilitarne l'accesso non appena venga informato dall'utente di questo desiderio.
- **Hosting:** memorizzazione continuativa dei dati, non per un lasso breve di tempo. Il fornitore del servizio **non** è responsabile delle informazioni salvate su richiesta del destinatario se:
 - Non è effettivamente a conoscenza delle attività o contenuti illeciti
 - Non è a conoscenza dei fatti in caso di fatti o circostanze che rendono manifesta l'illegalità dell'attività o dei contenuti;
 - Non appena viene a conoscenza di tali attività o contenuti provvede immediatamente alla rimozione

Indagini volontarie promosse di propria iniziativa e rispetto a degli obblighi normativi

I prestatori di servizi intermediari **non** sono considerati inammissibili all'esenzione della responsabilità per il solo fatto di svolgere indagini volontarie o altre attività di propria iniziativa volte ad individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi.

Ovvero, se vengono eseguite azioni di controllo, a patto che, qualora venisse trovato qualcosa di illecito, venga immediatamente rimosso, il proprietario del servizio non è comunque responsabile di quel che viene pubblicato.

Una volta che partecipi ad un gruppo di regole internazionali, non puoi rifiutarti di rispettare una delle norme anche se va in contrasto con una legge locale.

Punti di Contatto (supporto e contatti)

- I prestatori di servizi intermediari istituiscono un **punto di contatto unico** che consenta la **comunicazione diretta** per via elettronica con le autorità degli Stati membri.
- I prestatori dei servizi **rendono pubbliche** le informazioni necessarie per identificare e comunicare agevolmente con i loro punti di contatto.
- I prestatori di servizi specificano nelle informazioni **la lingua o le lingue ufficiali dell'Unione che possono essere utilizzate per comunicare i loro punti di contatto**.

Anche un'istituzione legale reale può essere il punto di contatto qualora fuori dai trattati.

Rappresentanti legali

I prestatori di servizi intermediari che **non sono stabiliti nell'Unione** ma che offrono servizi nell'Unione **designano per iscritto una persona fisica o giuridica quale loro rappresentante legale** in uno degli Stati membri in cui offrono i propri servizi.

I prestatori di servizi intermediari incaricano i loro rappresentanti legali di fungere da **punto di riferimento**.

Il rappresentante legale detiene i poteri e le risorse necessari per cooperare con le autorità degli Stati membri, la Commissione e il comitato.

Ordine di Fornire informazioni

Nel momento in cui viene chiesto di fornire informazioni dalle autorità giudiziarie o amministrative nazionali competenti sulla base del diritto dell'Unione o nazione, **i prestatori di servizi intermediari informano senza indebito ritardo chi ha fatto richiesta**.

Ovvero, quando gli sbirri chiamano devono rispondere.

Questo a patto che:

- Gli ordini contengono una **motivazione dell'obiettivo perseguito e delle ragioni per le quali la trasmissione dei dati è indispensabile ai fini di indagine** (in linea con le norme dell'unione o nazionali), a meno che la motivazione non possa essere fornita per motivi preventivi, accertamento e perseguimento di reati.
- **Informazioni sui mezzi di ricorso** a disposizione del presentatore e destinatario del servizio
- L'ordine impone al prestatore unicamente di **fornire informazioni già raccolte**
- L'ordine è **redatto nella lingua dichiarata dal prestatore** ed è inviato al punto di contatto

Ordine di contratto di contenuti Illegali

Appena ricevuto l'ordine di contrastare specifici contenuti illegali, emesso dalle autorità giudiziarie o amministrative nazionali competenti in base al diritto dell'Unione o del diritto nazionale, **i prestatori di servizi intermediari informano subito l'autorità che ha emesso l'ordine specificando le misure adottate e il momento in cui sono state attuate.**

Gli ordini sono composti di:

- **Motivazione** per la quale va contrastato un contenuto
- **Uno o più URL esatti** per l'identificazione dei contenuti
- **Informazioni sui mezzi di ricorso**

Devono soddisfare le seguenti condizioni:

- **L'ambito di applicazione territoriale dell'ordine** non va al di là di quanto strettamente necessario per arrivare all'obiettivo
- L'ordine è **redatto nella lingua dichiarata dal prestatore** ed è inviato al punto di contatto

Condizioni Generali

- 1) I prestatori di servizi intermediari **includono nelle loro condizioni generali informazioni sulle restrizioni che impongono in relazione all'uso dei loro servizi per quanto riguarda le informazioni fornite dai destinatari del servizio.**

Tali informazioni riguardano le **politiche**, le **procedure**, le **misure** e gli **strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana.**

Devono essere scritti in forma chiara, comprensibile e comodamente accessibile all'utenza.

- 2) I prestatori di servizi intermediari agiscono in modo diligente, obiettivo e proporzionato nell'applicare e far rispettare le restrizioni di cui al paragrafo 1, tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, compresi i diritti fondamentali applicabili dei destinatari del servizio sanciti dalla Carta