Sezione 1

L'ordinamento giuridico

Le norme giuridiche destinate ai consociati, insieme a quelle istituzionali ed organizzative dello Stato, ordinate sistematicamente, costituiscono **l'ordinamento giuridico**, un insieme di individui senza regole sarebbe un'orda in preda agli istinti. Inoltre, un popolo avente un insieme di regole in comune si sentirà più unito.
L'Italia è uno "**Stato di diritto**", ovvero soggiace alle stesse regole che ha emanato. Esiste un diritto primordiale, detto **diritto naturale**, che è quello che ci fa rispettare le regole senza sentirci obbligati. Senza di esso, ci sentiremmo obbligati a sottostare alle norme giuridiche. Inoltre, il sistema giuridico si è evoluto negli anni. Basti pensare che prima dell'invenzione della carta non si sentiva il bisogno di preservare i dati delle persone. Ricordiamo inoltre che lo Stato Italiano è laico, non obbliga quindi nessuno a rispettare od onorare una religione.

Le fonti del diritto

In Italia abbiamo un organo predisposto alla creazione di norme giuridiche, il **Parlamento**. Esso è composto dalla **Camera dei Deputati** e dal **Senato della Repubblica**. Il Parlamento ha potere **legislativo**, ovvero il potere di creare, modificare o eliminare una legge.
Distinguiamo due tipi di fonti, le **fonti atti** e le **fonti fatti**. Le prime sono manifestazioni espresse da un componente dello Stato e scritte, le seconde sono invece ciò che la comunità crede giuridicamente obbligatorie, le cosiddette "consuetudini" e modi di fare.
Esiste una **Gerarchia delle fonti**, ovvero una gerarchia di importanza delle norme. Al primo posto troviamo la **Costituzione Italiana** e le leggi Costituzionali. Nella Costituzione troviamo tutte le norme che finalizzano lo scopo dell'Italia, ovvero i suoi obiettivi e le finalità che la nazione intende percorrere. Sotto la Costituzione troviamo le **Norme comunitarie e di diritto internazionale**, ovvero le norme istituite da un insieme di Stati come l'Unione Europea che servono a salvaguardare obiettivi più grandi, come ad esempio l'uso dello spazio aereo, dei mari, l'ambiente ecc. Per quanto importanti, però, non possono andare incontro alle regole Costituzionali.
Al terzo posto troviamo le **Leggi ordinarie dello Stato**, ovvero le leggi che provengono dal Parlamento Italiano. Esse vengono fornite dal Parlamento, passando per entrambe le Camere e infine passando dal Capo dello Stato.
La funzione legislativa non è esclusiva del Parlamento, bensì è possibile applicarla con il Governo in **due casi specifici**: il primo caso è quando vi sono situazioni di particolare urgenza e quindi non è possibile aspettare il normale iter legislativo del Parlamento. In questo caso la norma prende nome di **Decreto-Legge**, che entra in vigore fin da subito, ma deve essere convertito in Legge del Parlamento entro sessanta giorni, altrimenti perde i suoi effetti.
Nel secondo caso, il Governo emana norme giuridiche avendo ricevuto una delega da parte del Parlamento e prende il nome di Legge delegante, mentre la legge si chiama **Decreto legislativo**. Come fonti normative abbiamo anche i Regolamenti, che sono atti di natura amministrativa ma che innovano l'ordinamento giuridico. Essi possono assumere le forme di **Decreto del Presidente del Consiglio dei Ministri (DPCM)**, del **Decreto Ministeriale (DM)** o del **Decreto del Presidente della Repubblica (DPR)**. Le leggi regionali assumono la forma di Legge Ordinaria se regolano le materie che l'art 117 della Costituzione non riserva al Parlamento, altrimenti esse assumono la penultima posizione della Gerarchia delle fonti e prendono nome di "**Leggi e regolamenti regionali**", insieme a quelli provinciali e comunali. All'ultimo posto, infine, abbiamo ciò che chiamiamo "usi" o "consuetudini"; si tratta per l'appunto di una fonte non scritta e consiste nella pratica uniforme e costante di dati comportamenti, accompagnata dalla convinzione che essi siano giuridicamente obbligatori.
Lo Stato Italiano ha suddiviso i suoi poteri in tre parti, ovvero il potere legislativo al Parlamento (creazione delle leggi), il potere esecutivo al Governo (emanarle) e quello giudiziario ai giudici (farle rispettare).

Il diritto pubblico e privato

Il diritto si divide in tante sottoclassi, ma noi distinguiamo due macroaree: il **diritto pubblico** e il **diritto privato**. Il diritto pubblico si occupa di fissare i diritti fondamentali degli italiani e si divide in:

- **Diritto Costituzionale**: disciplina gli enti dello Stato e la loro organizzazione.
- **Diritto Amministrativo**: regola l'azione degli enti pubblici.
- **Diritto Tributario**: regola la finanza pubblica.
- **Diritto Penale**: regola i reati e i loro sanzionamenti

Il diritto privato si occupa invece di disciplinare i rapporti tra i privati, ad esempio il **Diritto Civile** si occupa della famiglia, le successioni, servitù, diritti assoluti e diritti relativi. Il diritto penale serve per assicurare il rispetto delle regole imposte e salvaguardare i beni essenziali e la convivenza tra i consociati. I valori a cui l'ordinamento assegna una rilevanza assoluta sono: la vita, la salute, il patrimonio, la riservatezza, l'ordine pubblico. Tenere presente che l'imputato che viola una di queste è considerato innocente per tutta la durata dell'udienza fino al momento della sentenza finale.
Lo Stato conosce **tre gradi** di giudizio: il primo grado e il secondo grado (detto anche "giudizio di appello") sono detti "di merito" e consentono al giudice di conoscere al meglio il caso in questione. Il terzo grado, di "legittimità" è riservato alla **Suprema Corte di Cassazione** con sede a Roma che si occupa alla valutazione e al giudizio finale. Alcuni giudici danno il loro giudizio individualmente (giudici monocratici), altri giudici sono composti da magistrati che scelgono insieme il giudizio da dare. La **Corte Costituzionale** è un giudice che si occupa della legittimità delle leggi emanate e, in caso di contrato con la Costituzione, vengono cessate immediatamente. La **Corte dei Conti** effettua il controllo sulla gestione del bilancio dello Stato ed è competente a giudicare sui giudizi contabili dello Stato e degli altri enti pubblici. Data la complessità delle norme processuali, i privati non possono stare in giudizio, bensì devono assumere un tecnico del diritto (avvocato, o procuratore) per rappresentarli.

Nel nostro ordinamento è possibile risolvere le questioni di diritto civile in un altro modo, ovvero con un "**Arbitro**" o un collegio arbitrale. Essi non sono soggetti al rispetto delle regole processuali, ma sono obbligati ad ascoltare entrambe le parti, essere imparziale e dare tutte le possibilità di dimostrare la propria ragione a entrambe le parti. L'atto si conclude con il "**lodo**", ovvero il momento in cui l'arbitro (o il collegio arbitrale) danno il loro riscontro davanti al giudice di secondo grado. Il **precedente giurisdizionale** è una decisione già assunta da un giudice su un fatto analogo che un altro giudice è chiamato a conoscere. Il "precedente", però, viene trattato in maniera diversa a seconda che si tratti di **civil law** o **common law**. Nella prima, i giudici usano il "precedente" come un aiuto per il giudizio finale, che però si basa esclusivamente sulle norme scritte, facendo valere di più i diritti civili. Nel secondo, invece, i giudici si basano pochissimo sulle norme e usano di più il loro giudizio soggettivo, che nella maggior parte delle volte equivale allo stesso giudizio dato dal "precedente". Quando una fattispecie non è disciplinata dall'ordinamento giuridico, nei paesi di common law, i giudici, nel risolvere le questioni portate alla loro conoscenza, **creano una nuova regola** di diritto che colma immediatamente la lacuna; invece, nei paesi di civil law, i giudici devono attendere la disciplina dettata dal legislatore per poi applicare la regola al caso concreto; nell'attesa i giudici, nei sistemi di civil law, cercano di adattare le regole degli istituti simili. Il **diritto soggettivo** è una situazione giuridica riconosciuta ad un soggetto al quale la norma assicura la possibilità di soddisfare un certo interesse economico o morale. Al diritto di un soggetto corrisponde il **dovere giuridico** di un altro soggetto di riconoscergli quella situazione di vantaggio. Esempio: ciascuno di noi ha il diritto di esprimere un'opinione e gli altri hanno il dovere giuridico di lasciarcelo fare.

Sezione 2

I sistemi informativi

Tra le applicazioni più rilevanti di Informatica giuridica troviamo i sistemi informativi, ossia quei sistemi informatici che hanno lo scopo di immagazzinare dati ed aiutare l'utente a reperire quelli di suo specifico interesse. Il "**documento**" è l'oggetto centrale delle discipline che si occupano di documentazione. Con tale termine si individua qualsiasi oggetto portatore di informazioni. **L'archivio** di documenti è un insieme di documenti, dello stesso tipo o di tipi diversi, che, per esigenze specifiche informative, costituisce una raccolta logicamente omogenea. Le dimensioni dell'archivio possono far sì che la sua gestione con sistemi manuali si riveli complicata o financo impossibile e l'utente non possa essere in grado di consultare la raccolta nella sua interezza in un tempo accettabile.
Con l'espressione "**base di dati**" o "database" si intende una raccolta di informazioni gestite tramite elaboratore elettronico, organizzate secondo un sistema di relazioni contestuali che ne consentano il recupero. Generalmente, si usa distinguere le basi di dati in due categorie:

- **Reference data bases:** Le informazioni contenute forniscono gli elementi necessari per identificare una entità, alla quale rinviare l'utente.
- **Source data bases:** La base di dati contiene il dato informatico richiesto.

L'inserimento dei documenti in un archivio documentario avviene tradizionalmente secondo una procedura standardizzata: ciascun documento va anzitutto individuato nella sua fisicità (descrizione formale). Ciò può avvenire in vari modi: dal più semplice, attraverso un numero progressivo d'ingresso del documento nell'archivio, a sistemi più raffinati, che individuano alcuni elementi esteriori, ad esempio, per i volumi di una biblioteca, autore, titolo ecc. Ciascuno di questi elementi è individuato nell'archivio informatico con un apposito campo in cui viene articolato il **record** e può costituire **chiave di ricerca**; vale a dire che il documento può essere ricercato attraverso ciascuno di quegli elementi formali di identificazione indicati nei campi che costituiscono il record.
I dati aggiuntivi sono **metadati**, cioè sono informazioni a corredo dell'informazione principale che vanno oltre il semplice testo contenuto.
La descrizione semantica di un documento avviene, più in particolare, attraverso due diversi procedimenti: **l'indicizzazione** e **l'abstract.** La prima è un'operazione mirante a rappresentare i risultati dell'analisi di un documento con gli elementi di un linguaggio controllato al fine di individuare immediatamente gli elementi significativi. Il linguaggio controllato è un linguaggio che può essere costruito anche a prescindere dal contenuto dei documenti, partendo cioè da schemi scientifici o concettuali già organizzati e articolati, sempre relativi ad un particolare ambito disciplinare.
Il linguaggio controllato può essere espresso in:

- **linguaggio documentario**: generalmente un codice numerico o alfanumerico, che esprime un determinato concetto o un argomento.
- **linguaggio naturale**: espresso invece mediante termini, o serie di termini, usati per definire un concetto in maniera univoca e completa (descrittori) apposti dall'autore o da un documentarista esperto della materia e generalmente estratti da una lista.

A differenza delle parole-chiave (keywords), che sono parole del linguaggio naturale direttamente estratte dal documento, i **descrittori** sono il risultato di una scelta e di un'elaborazione del linguaggio connessa all'indicizzazione. I descrittori possono essere presentati semplicemente in una lista alfabetica, a cui si possono aggiungere alcuni sinonimi sotto i termini corrispondenti; ma possono anche essere organizzati in maniera da stabilire le relazioni fra i descrittori: si ha, in questo caso, una lista strutturata.
Sotto il nome di **abstract** si intende genericamente il riassunto in linguaggio libero del contenuto del documento in forma abbreviata senza interpretazione né critica, redatto dallo stesso autore o da un tecnico dell'informazione (documentarista). Il **linguaggio libero** è un linguaggio che contiene una terminologia non controllata, e quindi più semplice da comprendere. Essendo l'abstract redatto in linguaggio libero, ai fini del recupero dell'informazione, potrebbe, da un lato, restituire documenti in eccesso in risposta, fornendo risultati che niente hanno a che fare con l'esigenza informativa dell'utente e, dall'altro, non consentire il reperimento di quei documenti. È per questa ragione che le due operazioni di descrizione semantica (indicizzazione e abstract) vengono spesso adoperate insieme. Così, in molti sistemi informativi l'unità documentaria comprende sia le informazioni formali del documento sia i relativi termini in linguaggio controllato sia una sintesi in linguaggio libero.
Fra le strategie di ricerca va ricordato anzitutto l'uso degli **operatori logici**. Si tratta di tre operazioni logiche che, in termini documentari, individuano:

- la compresenza di due o più elementi (AND);
- l'alternativa fra più elementi (OR);
- l'inesistenza di uno o più elementi (NOT).

Ricordiamo inoltre l'esistenza di pagine dinamiche, ovvero pagine non reperibili tramite url, non ripetibili e composte sul momento, ovvero contenuti nel **deep web**. Altre reti oscure ospitano il **dark web** ossia una porzione più specifica del deep web non tracciabile e del tutto anonima in cui sono veicolate informazioni e sono forniti servizi che poco hanno a che vedere con i concetti di trasparenza e di legalità. Per proteggere l'utente, le reti oscure utilizzano un grande numero di server intermedi. I pacchetti vengono cifrati con chiavi diverse ad ogni passaggio, rendendo così molto complesso ricostruirne il percorso dato che ogni nodo conosce solamente l'indirizzo dei suoi due corrispondenti. Questa tecnica è comunemente nota con il nome di **onion routing**.
Per calcolare la prestazione dei sistemi informativi la scienza della documentazione usa **quattro indici**, detti 'di prestazione': **richiamo**, **precisione**, **silenzio**, **rumore**.

- **Richiamo**: È la capacità del sistema di ottenere in risposta tutti i documenti pertinenti, contenuti nell'intero archivio.
- **Precisione**: È la capacità del sistema di fornire in risposta solo documenti pertinenti.
- **Silenzio**: L'opposto del richiamo, indica i documenti pertinenti non richiamati dal sistema.
- **Rumore**: L'opposto della precisione, indica i documenti non pertinenti contenuti nella risposta.

Uno strumento tipico dei sistemi documentari è costituito dai **thesauri**. I thesauri sono dei vocabolari di un linguaggio di indicizzazione controllato, in modo che le relazioni tra i concetti siano rese esplicite. Il loro ruolo è il controllo applicato sia ai fini dell'indicizzazione, sia ai fini di recupero dell'informazione e sia a fini di consultazione. La caratteristica che distingue un thesaurus da una semplice lista di descrittori controllata è il fatto che tutti i termini presenti nel thesaurus sono organizzati in una struttura semantica, cioè le relazioni tra loro sono compiutamente esplicitate. Tali relazioni possono essere di vario genere:

- **Relazione di preferenza**: indicata con operatore ***us*** (use) e col suo reciproco ***uf*** (used for) o con il simbolo internazionale "=" serve per risolvere situazioni di sinonimia (case=abitazioni), quasi sinonimia (ville=abitazioni) o antinomia (comunismo *contrario di* anticomunismo).
- **Relazione di gerarchia**: Indicata con l'operatore ***bt*** (termine più ampio) e con ***nt*** (termine più ristretto) oppure con i simboli internazionali "<" e ">" per evidenziare i rapporti di sovra-ordinazione o sub-ordinazione tra genere e specie.
- **Relazione di associazione o affinità**: Indicata con l'operatore ***rt*** (termine associato) o con il simbolo internazionale "-", evidenzia i rapporti di correlazione o equivalenza d'idee tra descrittori.

Disponiamo, inoltre, di **ontologie**, ovvero descrizioni che indicano in modo formale il significato ed i legami tra i termini, costituendo ottime basi di conoscenza, soprattutto per i sistemi di intelligenza artificiale. La disponibilità di un'ontologia formale consente di raffinare anche la ricerca documentale, infatti è possibile individuare con precisione il concetto che ci interessa anche con un **termine simile** a ciò che stiamo cercando.

I sistemi cognitivi

I **sistemi cognitivi** sono sistemi **eteromorfi** (output diverso da input) in cui si dispone di un'intelligenza artificiale che serve per riprodurre, tramite calcoli complessi, il ragionamento dell'uomo. È quindi un sistema che, sulla base di un'elaborazione complessa sui dati forniti all'elaboratore, tenta di riprodurre il ragionamento della mente umana per risolvere un problema, riconoscere la realtà, comprendere un messaggio, proporre una risposta/soluzione ad un quesito/problema. Negli anni '70 si svilupparono due diverse teorie sulle intelligenze artificiali: quella **forte** e quella **debole**.
Quella forte sostiene che il computer potrebbe essere davvero dotato di una intelligenza non distinguibile in alcun modo da quella della mente umana, anzi l'intelligenza artificiale sarebbe in grado di valutare la correttezza dei processi mentali umani, producendo da sé modelli di ragionamento.
Quella debole invece sostiene che un computer non potrà mai eguagliare la mente umana, ma al massimo potrà simulare alcuni processi mentali umani senza mai riprodurli nella loro complessità. Per quanto la prima tesi sia affascinante, nel corso degli anni non ci sono stati risultati certi, anzi, tutto porta a pensare che quella più realistica sia la seconda tesi.
I sistemi cognitivi strutturalmente sono basati su due moduli fondamentali:

- Le informazioni sul settore della realtà di cui si occupano, detto anche "**base di conoscenza**"
- Le istruzioni per elaborare tali informazioni ('ragionare'), ricavandone informazioni originali, detto anche "**motore di inferenza**"

A differenza dei sistemi informativi, quelli cognitivi non vanno a ricercare i dati dalla base di conoscenza, bensì li elaborano e creano una nuova conoscenza. Per costruire un sistema cognitivo la prima operazione da fare consiste nell'individuazione della base di conoscenza, nel caso del diritto non si tratta solo delle norme, ed eventualmente delle sentenze o della dottrina, ma di tutti gli elementi, anche fattuali e di esperienza, che possono essere utili alla decisione. Il motore di inferenza utilizza la conoscenza memorizzata mettendo in atto processi di ragionamento differenti a seconda del formalismo di rappresentazione adottato: deduttivi per i formalismi procedurali; analogici per i formalismi dichiarativi. Tra le applicazioni delle tecniche di intelligenza artificiale, quella che più ha interessato i giuristi è relativa alla soluzione dei problemi giuridici (**problem solving**). Si tratta in sostanza di analizzare il processo di ragionamento attraverso cui il giurista mette a confronto una situazione fattuale che gli viene presentata con tutti i dati che ha a disposizione e giunge ad una decisione sul caso concreto. Un sistema **esperto giuridico** è appunto un sistema cognitivo composto da una base di conoscenza giuridica, rappresentata in maniera formalizzata, e da un motore inferenziale che, sulla base di una logica produce una soluzione al caso proposto. In altre parole, un sistema esperto non fornisce all'utente gli strumenti per costruire un ragionamento giuridico, come avviene nei sistemi informativi, ma sulla base di questi stessi strumenti enuncia una soluzione del caso. Per quanti elementi si potranno fornire al computer, sia con riferimento al caso concreto sia destinati a costituire la base di conoscenza, difficilmente si riuscirà a rappresentare tutti gli elementi di senso comune, di esperienza, di originalità e di intuito che caratterizzano i processi della mente umana. È per questo che si preferisce parlare di sistemi di **aiuto alla decisione**, a voler sottolineare che si tratta di fornire a colui che deve prendere una decisione elementi certamente utili, ma non certo definitivi, giacché sarà la mente e la volontà dell'uomo a prendere, ancora per qualche tempo, la decisione ultima.

Open Data e Big Data

Con l'espressione **open data** si indica il formato 'aperto' con cui i dati digitali possono essere distribuiti nel web per essere accessibili, riusabili ed integrabili. In senso lato, il fenomeno degli open data costituisce una delle novità più rilevanti nella realtà di Internet, in quanto, consentendo di trattare e rielaborare l'immensa conoscenza disponibile contenuta nella rete, apre un panorama illimitato di applicazioni.
Art. 50: principio di "disponibilità dei dati pubblici" che consiste nella possibilità, per soggetti pubblici e privati, "di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge".
Art. 52: precisa che i dati e i documenti pubblicati dalle pubbliche amministrazioni si intendono rilasciati in formato aperto, fatti salvi i riferimenti ai dati personali.
Gli open data sono stati classificati in cinque livelli di completezza, dai più strutturati a quelli meno strutturati. Quelli più importanti, di livello cinque, comprende quelli che vengono chiamati "**linked open data**". Sono dati aperti che, dal punto di vista del formato, oltre a rispondere alle caratteristiche indicate ai livelli precedenti, sono strutturati in modo da potersi agganciare ad altri dati, formando **dataset** in collegamento tra di loro. L'espressione **big data** identifica ampi volumi di informazioni digitali raggruppati e immagazzinati al fine di effettuare analisi automatiche. Le caratteristiche fondamentali sono: il volume, cioè che il sistema interessa vasti bacini di raccolta di dati; la velocità, vale a dire che i dati hanno una rapidità di crescita esponenziale; la varietà, cioè che le informazioni sono raccolte in qualsiasi tipo di formato.

Web Semantico

Il web sta evolvendo e si sta concretizzando la possibilità di relazionare automaticamente, sotto il profilo logico-concettuale, le informazioni in esso contenute. In altri termini, la struttura dei dati pubblicati e le tecnologie di intelligenza artificiale sono sempre più in grado di collegare in rapporti di significato le diverse parole e i vari documenti presenti in rete al di là dell'intervento dell'uomo.
Gli **obiettivi** del web semantico sono:

- realizzare la catalogazione dei contenuti delle singole pagine web e le relazioni tra di essi;
- riunire dinamicamente in un unico documento logico-concettuale collezioni di pagine web semanticamente correlate anche se distribuite in più siti;
- migliorare la precisione e l'efficienza dei motori di ricerca;
- aumentare il livello di fiducia degli utenti sulla qualità dei servizi pubblici e privati offerti nel web;
- semplificare ed aumentare la sicurezza per l'automazione di transazioni di tipo commerciale;
- favorire la condivisione, lo scambio e l'interpretazione di informazioni tra operatori umani e sistemi intelligenti.

I tre pilastri sui quali poggia il web semantico sono:

- L' **XML**: è un metalinguaggio di marcatura del testo utilizzato per caratterizzare le informazioni contenute in un documento; è estensibile, implementabile cioè in ragione di esigenze specifiche di descrizione del contenuto con la possibilità di creare nuovi tags; consente di attribuire ai dati elementi di significato; favorisce lo scambio documentale tra applicativi informatici che cooperano; offre, ancora, la possibilità di controllare la correttezza sintattica e strutturale definita per un determinato tipo di documento.
- L'**rdf** è una sorta di vocabolario o thesaurus per il riconoscimento dei tags xml. Consente alla macchina di comprendere la sintassi delle informazioni contenute nelle pagine web per come sono descritte in xml.
- Le **ontologie**.

Sezione 3

Quadro normativo

Il processo di informatizzazione nella pubblica amministrazione si può dire che abbia avuto inizio negli anni Novanta.
Legge n. 241/1990, intitolata "**Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi**", ha introdotto rilevanti innovazioni nel modo di organizzare il procedimento amministrativo, definendone sia i termini di durata sia la struttura sequenziale. Inoltre, con la stessa legge, è stato previsto **l'utilizzo dell'informatica** nel settore pubblico per la redazione dei documenti amministrativi.
Decreto Legislativo n. 29/1993 ha operato una vera e propria rivoluzione per l'amministrazione pubblica disciplinando nuovi criteri di gestione e di valutazione dei risultati dell'agire amministrativo. Con esso è stata istituita l'Autorità per l'informatica nella pubblica amministrazione (**AIPA**), un'autorità indipendente dal controllo del Governo alla quale è stato affidato il compito di armonizzare il processo di informatizzazione nella PA per evitare il prevalere di interessi privati e abusi di potere da parte degli stessi amministratori. Nel 2001, è stato istituito il **Ministero per l'Innovazione e le Tecnologi**e che ha assunto buona parte delle funzioni che in precedenza erano state delegate all'AIPA.

Nel 1995 è stata creata la **Rete Unitaria della Pubblica Amministrazione (RUPA)** con lo scopo di garantire ed assicurare l'interoperabilità e la cooperazione delle infrastrutture informatiche e telematiche delle pubbliche amministrazioni. In tal modo, tramite la rete dedicata, è stato possibile connettere qualsiasi terminale pubblico ad un qualsiasi altro computer collegato alla medesima rete. Dalla RUPA, nel 2005, si è passati al Sistema pubblico di connettività (**SPC**), disciplinato compiutamente dal Codice dell'amministrazione digitale (**CAD**).

Documento amministrativo elettronico

Il **documento amministrativo elettronico** è il primo strumento significativo nel processo di dematerializzazione della PA. La legge n. 241/90 definisce il documento amministrativo come "ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti anche interni formati dalle pubbliche amministrazioni o comunque utilizzati ai fini dell'attività amministrativa". Tale nozione, se da un lato sancisce il principio della libertà delle forme che l'atto può assumere in quanto oggettivazione dell'attività amministrativa, dall'altro acclara la piena ammissibilità nel sistema giuridico-amministrativo della tecnica elettronica.
La legge Bassanini 1, in parte, stabilì che "gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti ad ogni effetto di legge". Il successivo regolamento ha poi fissato i **criteri giuridici** oggettivi ai quali dovranno sottostare i documenti informatici e le modalità con cui i contratti dovranno essere realizzati.

Le firme elettroniche

La **sottoscrizione** è la scrittura del proprio nome e cognome di proprio pugno in calce ad un documento. Nel codice di procedura penale all'art. 110 troviamo: "Non è valida la sottoscrizione apposta con mezzi meccanici o con **segni diversi dalla scrittura**". In sostanza, nel caso di firma non autenticata, se un soggetto disconosce una firma su un documento attribuito a sé o ad altri, sarà suo l'onere di dare la prova della falsità della firma. Lo strumento giuridico di ordine penale per verificare la falsità dell'atto è la **querela di falso**.
Il concetto di **firma digitale** è definito come "il risultato della procedura informatica (validazione) basata su un sistema di **chiavi asimmetriche** a coppia, una pubblica e una privata, che consente al sottoscrittore 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". Il sistema garantisce quattro requisiti: provenienza, non ripudio, immodificabilità, segretezza. Il legislatore europeo ha ampliato la nozione di firma elettronica prevedendone quattro tipologie differenti: la **firma elettronica semplice**, la **firma elettronica avanzata**, la **firma elettronica qualificata**, la **firma digitale**. L'articolo 1 del CAD definisce il 'documento informatico' come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".
Il **valore probatorio** del documento informatico è determinato secondo una scala decrescente. Se è sottoscritto con firma digitale o altra firma elettronica qualificata o avanzata l'efficacia probatoria sarà più forte; se è possibile identificare un soggetto tramite una procedura informatica semplice (firma elettronica semplice) l'efficacia probatoria sarà più debole. La firma elettronica avanzata è definita come l'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la sua connessione univoca al firmatario e consente di rilevare se i dati stessi siano stati successivamente modificati.
La firma elettronica avanzata ha un campo di utilizzo minore rispetto alla firma digitale, infatti non può essere utilizzata in contratti di vendite, locazioni di immobili etc… ma solo se la richiede il venditore perché ha valenza solamente tra le due controparti, a differenza invece della chiave digitale. La **firma elettronica qualificata** è un particolare tipo di firma elettronica avanzata, basata su un **certificato qualificato**, e realizzata mediante un dispositivo sicuro per la creazione della firma. Sono presenti due elementi addizionali rispetto alle firme che abbiamo descritto finora: un certificato rilasciato da **un'autorità di certificazione**, ed un **dispositivo fisico** sicuro per la creazione della firma.
La **firma digitale** è basata su un certificato qualificato e su un sistema di chiavi crittografiche asimmetriche, una pubblica e una privata, correlate tra loro. Con il Regolamento europeo **eIDAS** sia la firma elettronica qualificata che la firma digitale hanno acquisito pieno valore in tutto il territorio dell'Unione, essendoci regole tecniche comuni in tutti gli Stati membri. In generale, la firma digitale può essere apposta tramite software di firma dedicati e si distingue in tre tipologie:

1) la firma **CAdES** produce una estensione "**p7m**" al file e sigilla in una busta digitale il contenuto del documento insieme al certificato di firma.
2) la firma **PAdES** può essere apposta ai documenti in formato "pdf", i quali conserveranno la medesima estensione. Questo formato permette, inoltre, di apportare modifiche al documento con ulteriori firme senza che venga persa la traccia del file firmato in origine.
3) la firma **XAdES** come per i pdf, non prevede la creazione di una busta, non modifica l'estensione del file e permette di accedere ai metadati contenuti all'interno del documento. Con quest'ultima tipologia di firma vi è la possibilità di sottoscrivere singole parti del documento, ad esempio, nei casi in cui il documento sia stato scritto a più mani e ciascuno debba firmare solo la propria parte.

Il timbro digitale

Il **timbro digitale** è un codice grafico bidimensionale impresso nel documento originale elettronico che permette anche dopo la stampa di conservare le garanzie di autenticità e di verificarne l'eventuale alterazione. La previsione all' Art. 23, comma 2-bis, del CAD consente, ad esempio, di emettere certificati senza la necessità di utilizzare supporti speciali, quali carta filigranata, timbri a secco, firme autografe, ecc., per garantirne l'autenticità. L'esigenza tutelata dalla previsione del CAD riguarda l'ottimizzazione della vita dei documenti prodotti in originale in formato elettronico con firma digitale.

La marca temporale

Un altro strumento disciplinato dal Regolamento europeo **eIDAS** è la **marca temporale** che è possibile applicare su un documento o su una serie di documenti. Consiste nella generazione, da parte di una terza parte fidata (CA), di una firma digitale sul documento a cui è associata l'informazione relativa ad **una data e ad un'ora certa**. La marcatura temporale consente quindi di stabilire l'esistenza di un documento informatico o di un gruppo di documenti informatici a partire da un certo istante temporale e di opporlo ai terzi. L'apposizione della marca temporale **non incide** sul contenuto del documento e non ne modifica la sua firma originaria.

La posta elettronica certificata

Il servizio di posta elettronica certificata (**PEC**) consente di spedire qualunque tipo di documento prodotto con strumenti informatici da un server ad un altro in maniera certa e sicura. La PEC, infatti, è un sistema di posta elettronica avanzato, idoneo a fornire al mittente documentazione elettronica con valenza legale attestante l'invio e la consegna di documenti informatici. Certificare l'invio e la ricezione del documento significa, da un lato, fornire al mittente da parte del proprio gestore di PEC **una ricevuta** che è prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione, dall'altro, con riferimento all'arrivo del messaggio al destinatario, fornire al mittente, da parte del gestore di PEC del destinatario e dello stesso mittente, la ricevuta di avvenuta o mancata consegna con precisa indicazione temporale. Questa possibilità è finalizzata a garantire l'utente nell'ipotesi di un contenzioso, laddove si richieda la documentazione attestante l'invio e la ricezione di un messaggio. Il destinatario di un messaggio di PEC **non può negare l'avvenuta ricezione**, posto che la ricevuta di avvenuta consegna, firmata ed inviata al mittente dal gestore di PEC scelto dal destinatario, riporti le indicazioni della data e dell'ora in cui il messaggio è stato consegnato nella casella di PEC del destinatario, certificandone l'avvenuta consegna. Alcuni provider PEC consentono di inviare mail ad indirizzi non PEC, ma ovviamente questo tipo di scambio documentale non soddisfa la previsione di cui all' Art. 48 del CAD. I gestori di questo tipo di servizio hanno l'obbligo di registrare tutte le operazioni relative alle proprie PEC nel **log** del proprio sistema. Il **registro di log** deve contenere le seguenti informazioni: il codice identificativo univoco assegnato al messaggio originale (message-id), la data e l'ora dell'evento, il mittente del messaggio originale, i destinatari del messaggio originale; l'oggetto del messaggio originale, il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.), il codice identificativo (message-id) dei messaggi correlati generati (ricevute, errori, ecc.), il gestore mittente. Il citato Regolamento eIDAS, oltre ad intervenire in materia di firme elettroniche, ha istituito il Servizio elettronico di recapito certificato (**SERC**), che costituisce un'alternativa alla PEC.

Le carte elettroniche

Già con il primo piano di azione per l'e-Government era stata prevista la diffusione di strumenti di autenticazione in rete, quali la carta d'identità elettronica (**CIE**) e la carta nazionale dei servizi (**CNS**), per l'accesso ai servizi telematici. Dal 2006 i Comuni avrebbero dovuto rilasciare la CIE ai richiedenti in sostituzione di quella cartacea, ma i costi per acquistare gli strumenti necessari per produrla e la scarsa utilità pratica della stessa ne hanno rallentato notevolmente la distribuzione. Le vicende traverse della CIE si sono sbloccate solo di recente quando sono stati implementati i servizi aggiuntivi che hanno suscitato una vera spinta all'utilizzo. I dati riportati sono firmati digitalmente dal Ministero dell'Interno. L'accesso alle impronte digitali è permesso solo a chi è in possesso di specifiche autorizzazioni. La **carta nazionale** (o regionale) **dei servizi** (CNS), che in alcune regioni coincide con la tessera sanitaria, è, invece, una smart card che non ha funzione di documento di riconoscimento 'a vista', perciò non contiene la foto del titolare ed è provvista esclusivamente di un microchip. La CNS contiene anch'essa un certificato di autenticazione. Essa contiene i dati identificativi del titolare, il codice numerico di identificazione delle carte nonché le date del suo rilascio e della sua scadenza. Essa può eventualmente contenere informazioni di carattere individuale generate, gestite e distribuite dalle pubbliche amministrazioni per attività amministrative e per l'erogazione dei servizi al cittadino, cui si può accedere tramite la carta.

Il sistema pubblico di identità digitale – SPID

Il DPCM del 24 ottobre 2014 ha novellato l'Art. 64 del CAD, prevedendo per i cittadini e le imprese il **Sistema pubblico di identità digitale** (SPID), quale strumento di accesso elettronico unico, sicuro e protetto ai servizi online quale strumento di accesso elettronico unico, sicuro e protetto ai servizi online. L'identità digitale dei soggetti richiedenti (credenziali) è rilasciata da appositi gestori (identity provider), soggetti privati accreditati presso. Esso diventa utile alla semplificazione dei servizi pubblici digitali. Il sistema prevede **tre livelli** di sicurezza: un primo, permette di accedere ai servizi online attraverso un nome utente e una password scelti dall'utente; un secondo permette l'accesso attraverso un nome utente e una password scelti dall'utente, più la generazione di un codice temporaneo di accesso. Con il terzo livello è necessario effettuare la procedura di riconoscimento utilizzando la carta nazionale dei servizi (CNS), la tessera sanitaria (sempre con CNS), la carta di identità elettronica (CIE) oppure un dispositivo di firma digitale o di firma remota.

Sezione 4

Diritto d'autore

Per garantire e tutelare **l'autore** (creatore) di un programma per elaboratore il diritto prevede una particolare disciplina dedicata ai beni immateriali. Il diritto per tutte le opere dell'ingegno prevede la protezione morale e patrimoniale in capo a chi ne risulti essere il creatore. Tale protezione riconosce al creatore del prodotto dell'intelletto lo sforzo sostenuto per la sua realizzazione, oltre che in termini di ingegno, anche in termini economici e di tempo. In Italia, soltanto nel dicembre 1992 con il D.Lgs. n. 518 è stata attuata la tutela penale per le violazioni riguardanti i programmi per elaboratore. il Pretore di Torino nel 1982 risolse una questione che gli era stata sottoposta dalla Atari Inc. (società statunitense che produceva videogames) contro la Sidam Srl (altra società produttrice di videogiochi). La questione sottoposta al giudice verteva sulla copia di tre videogiochi che la Sidam aveva riprodotto dalle versioni originali della Atari per commercializzarle in Italia ad un prezzo sensibilmente inferiore rispetto a quello praticato dalla Atari. In quell'occasione il Pretore non riconobbe in quei prodotti la creatività e l'originalità proprie delle opere tutelabili con le norme sul diritto d'autore e riscontrò invece potersi applicare un particolare tipo di norma del Codice civile che vieta la c.d. '**concorrenza parassitaria**', quella cioè che vieta di sfruttare le risorse impiegate dalla società concorrente per trarne un profitto consistente nel risparmio di spesa da parte della società parassitaria. In questo caso furono adottate le sanzioni civili previste dal codice per quella materia: l'inibitoria, cioè il divieto per la società concorrente (sleale) di continuare a servirsi del prodotto 'copiato'; il ripristino della situazione precedente l'abuso; il risarcimento del danno quantificato dal giudice in favore della Atari. All'interno del Codice civile troviamo la disciplina dedicata ai diritti sulle opere dell'ingegno. In particolare, all'articolo 2575 è disposto: "Formano oggetto del diritto di autore le opere dell'ingegno di carattere creativo che appartengono alle scienze, alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia, qualunque ne sia il modo o la forma di espressione".

Disciplina

Il diritto lascia la massima libertà alla '**forma**' di espressione del software che quindi può essere la più varia. Ciò significa che sono protetti i programmi, in qualsiasi 'forma' espressi, purché originali, quale risultato di una creazione intellettuale dell'autore. Pertanto, il diritto tutela la 'forma' in cui è realizzata l'opera software, non l'idea ed i contenuti che possono essere utilizzati liberamente da altri che non si limitino al mero plagio. In sostanza, chiunque liberamente può elaborare una nuova applicazione di editing testuale e può godere della protezione giuridica sulla propria opera, a condizione che non si limiti a dare colori diversi agli stessi bottoni o che non cambi semplicemente il font dei menu di un altro programma, perché in tal caso si avrebbe, come detto sopra, il plagio.
Il diritto d'autore tecnicamente si esprime in due forme:

- **Diritto morale**, ossia il diritto alla paternità dell'opera frutto della propria creatività e consiste a sua volta nel diritto:
    1. Ad essere riconosciuto come autore.
    2. Di non pubblicare l'opera
    3. Di opporsi alle pubblicazioni che possano recare pregiudizio alla sua reputazione
    4. di ritirare l'opera dal commercio qualora concorrano gravi ragioni morali, salvo l'indennizzo di chi abbia acquistato il diritto alla utilizzazione commerciale dell'opera

  Tale diritto morale d'autore è **imprescrittibile** (cioè non si estingue con il trascorrere del tempo), è **irrinunciabile** (l'autore non può ripudiare sé stesso), è **intrasferibile** (l'opera sarà per sempre attribuita al suo creatore e questi non potrà cedere o trasmettere tale titolo a nessun altro

- **Diritto patrimoniale**: il diritto alla utilizzazione esclusiva dell'opera d'ingegno compiuta, quando questa non è oggetto di un contratto di lavoro subordinato. Il diritto patrimoniale, dunque, è trasferibile ed ha durata di 70 anni dalla morte dell'autore o 70 anni dalla pubblicazione dell'opera, se postuma.

A partire dal momento in cui l'opera viene ad esistenza **scaturiscono automaticamente** i diritti morale e patrimoniale d'autore. Sempre più spesso, per via della complessità dei prodotti da realizzare, accade che più individui collaborino per la realizzazione di software, pertanto, si parla di "contitolarità" dell'opera in due modi:

1. **Opera in "comunione"**: creata con l'apporto indistinguibile ed indivisibile di più soggetti. Tutti i soggetti sono titolari in egual modo
2. **Opera "collettiva"**: creata con l'apporto di più soggetti in cui ogni contributo è individuabile, quindi ai singoli partecipanti è riconosciuta la propria percentuale.

Tipologie di software

A titolo meramente indicativo, le tipologie di software sono classificate e regolate sotto il profilo della tutela giuridica secondo le seguenti caratteristiche:

1. Software "**commerciale**": è concesso in licenza ad altri, tipicamente dietro pagamento di un corrispettivo. In questo caso il codice sorgente rimane nella esclusiva disponibilità dell'autore o di chi ne esercita il diritto patrimoniale e viene concesso in licenza il software compilato, cioè il solo codice oggetto.
2. Software "**open source**": sottintende la logica dell'intelligenza collettiva e se è vero che tutti possono contribuire allo sviluppo di un software di questo tipo perché distribuito con il codice sorgente aperto è altrettanto vero che chiunque voglia collaborare potrebbe essere obbligato a rispettare dei vincoli nei confronti dell'autore originario. Il movimento open source nasce con la licenza di tipo GNU-GPL, fondata da Stallman negli anni 80. L'autore potrà tutelarsi con questa licenza qualora una persona abbia modificato e immesso nel mercato un applicativo originariamente nato open source.
3. Software **freeware**: un software dall'eseguibile gratuito, ma con codice sorgente nascosto o a pagamento.
4. Software **shareware** o trial: quei software che hanno un periodo di prova con usi limitati del software.
5. Software **libero**: l'unico software libero dal suo utilizzo al suo codice sorgente, libero da vincoli giuridici.

Forme di tutela

Esistono alcuni diritti inderogabili che non possono essere negati al legittimo acquirente della licenza d'uso di un software:

- Possibilità di back-up per scongiurare il pericolo di perdere il contenuto acquistato o la piena funzionalità del software.
- Decompilazione, ovvero rendere interoperabile il prodotto con altri programmi in uso.
- Vietata la riproduzione contemporanea dello stesso software su più macchine, tranne se il prodotto è progettato per la multiutenza. Ecco perché è severamente vietato installare il software su un server per renderlo operabile da qualsiasi macchina si connetta. In caso di violazione, si va incontro all'inibitoria del software, sequestro delle copie o al risarcimento dei danni.

I gestori del diritto

La tutela del diritto patrimoniale d'autore in Italia è stata affidata alla Società degli autori e degli editori (**SIAE**), un ente di diritto pubblico economico su base associativa. Assolve ai compiti di certificazione preventiva mediante l'apposizione del contrassegno su ogni supporto contenente programmi per elaboratore destinati al commercio o ceduti in uso a fine di lucro. In altri termini, l'editore dimostra di aver assolto ai diritti d'autore apponendo il contrassegno SIAE sul supporto. Il contrassegno ha assunto negli anni caratteristiche tecniche avanzate anticontraffazione: è irriproducibile, è metallizzato, ha un inchiostro fotocromatico che a 37/38 gradi scompare e riappare. È stato istituito un registro speciale per programmi per elaboratori presso la SIAE, sul quale iscrivere ogni nuovo programma destinato al commercio; l'iscrizione prevede l'indicazione di tutti i soggetti autori del software ai fini dell'attribuzione dei diritti ad esso connessi. È bene tenere presente, comunque, che il software è protetto anche se non è iscritto al registro di cui sopra, infatti, l'iscrizione non ha natura costitutiva, ma facoltativa ed ha carattere oneroso e valore probatorio. Ove accada che qualcuno diverso dall'autore di un programma iscriva nel registro lo stesso programma prima dell'autore, avrà acquisito una prova sulla titolarità dell'opera, e sarà l'autore che avrà l'onere di dimostrare al giudice che è lui il vero autore del programma.
I dati raccolti nelle banche dati, in base alla loro disposizione, possono essere coperti da diritto di autore. Ovvero, in base alla disposizione dei documenti, trattamento di dati, o qualsiasi cosa che li contraddistingue, li rende tali da assumere la dignità di opere di ingegno, e quindi soggette alla proprietà intellettuale. Per le banche dati, a parte la selezione e la disposizione dei materiali, un cenno deve farsi anche sul **software di organizzazione**, di visualizzazione e di ricerca che su quei dati opera, che assume di per sé la dignità di opera dell'ingegno. Detto in altri termini, una cosa è la struttura dei dati, altro è la modalità attraverso la quale essi vengono classificati, estratti dal database, aggregati, presentati e visualizzati dall'utente. Quindi, nello strato base di una banca dati sono presenti diversi elementi, tra cui il software di gestione e il software di ricerca, che hanno algoritmi propri e che quindi vanno distinti dai documenti o dai dati, anche in termini di protezione del diritto d'autore.
La legge riconosce una tutela affievolita anche a beneficio di coloro che hanno semplicemente aggregato o raccolto dati, producendo un'opera del tutto priva di carattere di originalità. Questi che, come accennato sopra, prende il nome di **costitutore**. Per il solo fatto che ha investito tempo e danaro nella realizzazione della stessa, gode della protezione da parte dell'ordinamento sulla sua opera.
Inoltre, ci sono due ipotesi per il libero utilizzo della banca dati:

1. Non è possibile limitare l'accesso o la consultazione della banca dati quando tali attività abbiano esclusivamente finalità didattiche o di ricerca scientifica.
2. Non è possibile limitare l'impiego della banca dati per fini di sicurezza pubblica o per effetto di una procedura amministrativa o giurisdizionale.

Le Creative Commons

Autori e fruitori della conoscenza hanno in comune un macro-scopo fondamentale che è proprio quello dell'incremento e della diffusione del sapere nell'ecosistema digitale. Il movimento **open data** è espressione di questo pensiero ed è in assoluta contrapposizione con le logiche tradizionali di proprietà dei dati. La filosofia della libera circolazione del pensiero, dei dati e dei prodotti tramite il web è rappresentata dalle note 'Creative Commons Public Licence' (**CCPL**), redatte e distribuite da una organizzazione no-profit statunitense (la **Creative Commons** – CC) dal 2002. Gli autori di pubblicazioni digitali hanno la possibilità di conservare alcuni diritti sulle proprie opere, concedendo agli utenti della rete la libertà di riproduzione e di utilizzo a determinate condizioni. Dette licenze, sono denominate:

- **Attribution** (BY): consente che altri copino, distribuiscano, mostrino ed eseguano copie dell'opera e dei lavori derivati da questa a patto che venga indicato l'autore dell'opera.
- **Non Commercial** (NC): consente che altri copino, distribuiscano, mostrino ed eseguano copie dell'opera e dei lavori derivati da essa o sue rielaborazioni, solo per scopi non commerciali;
- **No Derivatives** (ND): consente che altri copino, distribuiscano, mostrino ed eseguano soltanto copie identiche dell'opera e non sono ammesse opere derivate o rielaborazioni.
- **Share Alike** (SA): consente che altri distribuiscano lavori derivati dall'opera solo con una licenza identica a quella concessa con l'opera originale.

Le dette licenze possono essere combinate tra loro fino a sei soluzioni possibili e utilizzate da tutti liberamente e gratuitamente. Ulteriore caratteristica delle CCPL è quella di essere '**human and machine readable**'; ciò consente anche di sviluppare applicativi robot o semi automatici che navigando il web distinguono tali licenze, nelle diverse combinazioni e, operando come se le comprendessero, raccolgono e utilizzano le informazioni e i dati disponibili nel rispetto e nei limiti dei diritti riservati.

I sistemi di Digital Right Management (DRM)

Sono definiti **Digital Right Management** (DRM) quei sistemi tecnologici utilizzati per la gestione dei diritti sulle opere digitali sotto il profilo, appunto, 'logico'. Si tratta, più segnatamente, di accorgimenti tecnici che i produttori possono inserire nelle opere digitali. Un esempio il ***product key*** (per sbloccare le funzionalità del prodotto), il ***bitstream watermarking*** (per limitare il numero di volte l'esecuzione del file e i dispositivi) e il ***fingerprint*** per identificare l'utente.

La proprietà industriale

L'art. 2585 del cc tutela le nuove invenzioni atte ad avere un'applicazione industriale. Per ottenere la protezione giuridica è necessario che l'invenzione sia brevettata. Il **brevetto** è il mezzo per rendere pubblica l'invenzione e per permettere all'inventore lo sfruttamento esclusivo della stessa. Oltre che per le invenzioni, il brevetto è previsto anche per i "modelli di utilità" cioè per quei prodotti che permettono di usare in maniera migliore rispetto al passato beni che già esistono, come ad esempio un mouse di una nuova forma che può essere utilizzato indifferentemente con la mano destra con la sinistra. Per ottenere il brevetto in Italia è necessario che l'invenzione sia nuova, cioè non sia ancora conosciuta secondo la tecnologia esistente; inoltre, è necessario che sia un'opera creativa e non una ovvia applicazione della tecnologia esistente; deve, ancora, possedere la caratteristica della liceità, ossia non deve essere contrario ordine pubblico o al buon costume e, in generale, non deve essere in contrasto con la legge dello Stato; infine, deve essere idonea ad avere un applicazione industriale. Ottenuto il brevetto all'inventore è riconosciuta la priorità dell'invenzione e il conseguente diritto ad utilizzare economicamente l'invenzione ed evitare che altri utilizzino l'invenzione brevettata senza averne titolo. La durata del diritto di sfruttamento esclusivo dell'invenzione è limitata a 20 anni per le invenzioni industriali e 10 anni per i modelli di utilità.

Sezione 5

Premesse normative e principio di legalità

Il diritto penale in Italia è governato dal '**principio di legalità**' che a sua volta si declina su quattro direttive:

1. **Riserva di legge**: lo Stato riserva la potestà normativa in materia penale al legislatore ordinario, cioè al Parlamento che rappresenta la volontà del popolo.
2. **Tassatività**: Il legislatore deve individuare con un certo grado di precisione qual è il comportamento penalmente sanzionato. Il consociato deve sapere con esattezza quale condotta non può tenere e cosa gli è invece consentito fare, qual è il confine tra il lecito e l'illecito.
3. **Irretroattività della legge**: Consiste nel divieto di applicare la legge penale a fatti commessi prima della sua entrata in vigore. Il principio è in effetti valido per tutte le leggi dello Stato. Esiste però un'eccezione. Nel caso in cui una nuova legge depenalizzi un comportamento fino ad allora considerato reato, chiunque sia incorso in quella fattispecie non sarà più punito con quella legge ma verrà applicata la nuova legge a colui che ha commesso l'illecito. Basti pensare che non è giusto infliggere una pena ad un soggetto per un fatto che non è più un reato.
4. **Divieto di analogia in materia penale**: L'analogia è un processo di integrazione dell'ordinamento che consente al giudice, in assenza di una norma specifica che regoli la fattispecie su cui è chiamato a decidere, di applicarne una che regoli casi o materie analoghe. L'analogia non opera in ambito penale perché sarebbe in contrasto con la tassatività descritta sopra.

Costituisce un **illecito** qualunque comportamento antigiuridico, sia di diritto pubblico che di diritto privato. L'illecito penale è rappresentato da una fattispecie di reato, cioè da un fatto che dipende dall'operato dell'uomo, anche di natura omissiva, al quale l'ordinamento giuridico ricollega una sanzione penale. La responsabilità penale è personale, cioè non è trasmissibile a nessun altro. In altri termini, l'ordinamento penale può comminare pene soltanto all'autore del reato, salvo il caso della responsabilità oggettiva. In **qualunque caso**, l'ordinamento italiano garantisce al soggetto incriminato il **diritto di difesa** in ogni ordine e grado di giudizio. La difesa è un diritto inviolabile sancito dalla Costituzione e prevede che chiunque possa difendersi in giudizio per tutelare la propria posizione giuridica in merito ad un fatto illecito. L'azione penale ed il processo scaturiscono solo se viene sporta la querela da parte di chi ha subito le conseguenze del fatto delittuoso. Alcuni comportamenti criminosi possono essere compiuti da chiunque: si pensi all'omicidio, al furto, all'omissione di soccorso. Essi sono detti **reati comuni**, mentre altri possono essere commessi soltanto da determinati individui, come un poliziotto che riceve denaro per corruzione. Questi invece sono detti **reati propri** e sono puniti più severamente. In tutti i casi, la pena a chiunque comminata, nell'ordinamento italiano, deve tendere alla rieducazione del condannato, in una visione di recupero e valorizzazione della persona umana e non di umiliazione e abbandono.
Alcune fattispecie di reato prevedono una soglia di punibilità molto bassa; si tratta dei "**reati di pericolo**", per i quali la condotta criminosa si perfeziona con la semplice messa in pericolo o lesione potenziale del bene oggetto della tutela penale; si pensi ad un soggetto che detenga illegalmente armi. Nella maggior parte dei casi, invece, il perfezionamento della fattispecie di reato avviene con la lesione effettiva del bene protetto. Essi sono i "**reati di evento**", basti pensare al sequestro di persona.
Ai fini del perfezionamento del reato, in generale, è necessario valutare l'elemento psicologico del soggetto agente. Infatti, la fattispecie criminosa prevede, nella maggior parte dei casi, che la condotta da parte del soggetto agente sia compiuta **intenzionalmente**. Il **dolo** è l'elemento psicologico che il giudice deve ricercare nel soggetto incriminato per poter infliggere la pena. Il dolo si configura, dunque, allorquando il soggetto agente con la sua condotta criminosa ha preveduto e voluto il verificarsi dell'evento dannoso o pericoloso a danno del bene protetto. In altri casi, quando è espressamente previsto dalla norma di diritto penale, l'agente risponde anche quando con la sua condotta, pur potendolo prevedere, non ha voluto il verificarsi dell'evento dannoso che si verifica a causa di negligenza, imprudenza, imperizia, per inosservanza delle leggi, ordini o discipline. È il caso della **responsabilità per colpa**. Ciascuna fattispecie di reato può verificarsi arricchita da elementi particolari. Si tratta delle "**circostanze del reato**" che possono causare l'aumento o la diminuzione della pena. Per l'aumento si parla di "**circostanze aggravanti**", come la commissione del reato per celarne un altro già commesso, la commissione del reato ai danni di un minore, la particolare efferatezza nella commissione dell'omicidio, la recidiva, cioè la ripetizione di una condotta criminosa per la quale si era già subito un processo. Per la diminuzione si parla di "**circostanze attenuanti**", esempio quando il soggetto agente ripara il danno prodotto prima del giudizio. Infine, ci sono le "**circostanze scriminanti**" (o di giustificazione), in presenza delle quali la condotta, che in astratto configura un reato, in concreto non è ritenuta antigiuridica. Le esimenti sono lo 'stato di necessità', l''esercizio di un diritto o l'adempimento di un dovere', la '**legittima difesa**'.

Crimini informatici

Sotto quest'ultima denominazione, gli studiosi a livello concettuale distinguono i reati commessi per mezzo dell'elaboratore elettronico e dei programmi in esso installati.
Le prime fattispecie di reati informatici che analizzeremo sono previste nella legge n. 633 del 1941, che si occupa di protezione del diritto d'autore.
All'art. 171-bis sono previste tre fattispecie di reato punite con la reclusione e con la multa:

1. nei casi di **duplicazione** (…) abusiva di programmi per elaboratori protetti al fine di trarne profitto;
2. nei casi di **predisposizione** o utilizzo di qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma;
3. nei casi di **riproduzione** (…), su supporti non contrassegnati SIAE, del **contenuto** di una banca di dati al fine di trarne profitto.

Passando alle fattispecie di reato inserite nel Codice penale:

Art 635-bis, '**Danneggiamento di informazioni, dati e programmi informatici**': La norma prevede che "Chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione …". La disposizione è posta a tutela dei beni informatici e configura un reato di danno rivolto a chi lo commette con dolo, cioè agendo consapevolmente con l'intenzione di distruggere, deteriorare, cancellare, alterare o sopprimere i detti beni ottiene il suo scopo. Il reato è perseguibile soltanto in presenza della querela della persona offesa.
Art 635-ter, '**Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità**': "Chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni".
Art 635-quater, '**Danneggiamento di sistemi informatici o telematici**': punisce con la reclusione "Chiunque, mediante le condotte di cui all'articolo 635-bis, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento…". Nella fattispecie il bene protetto è il sistema informatico nel suo complesso e non i dati e le informazioni.

Il **domicilio informatico** è inteso quale proiezione o trasposizione virtuale del domicilio fisico; è il luogo dove si esplica la personalità del soggetto, dove è riposta parte della memoria con i documenti, i pensieri personali, le fotografie, i video, le registrazioni vocali, dove si svolgono conversazioni, dove si trascorre parte sempre più cospicua del proprio tempo.

Art. 495-bis, '**Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri**': "Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione".
Art. 615-ter, '**Accesso abusivo ad un sistema informatico o telematico**': prevede che "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 …".
Art. 615-quater, '**Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici**': "Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione e con la multa".
Art. 615-quinquies, '**Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico**': punisce con la reclusione e con la multa "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici …". È il caso dei **virus informatici** intesi in forma ampia. Da notare in tale fattispecie che il soggetto agente è punibile **solo se viene accertato che abbia agito con dolo** e, si noti, che la soglia di punibilità è anticipata, solo per gli effetti potenziali che il virus può causare, dato che il reato si perfeziona con la messa in pericolo del bene protetto, ovvero più il bene è messo in pericolo (potenziale del virus) più è grave.

Il Codice penale si occupa anche di reati cosiddetti di **social engineering**. Dallo studio dei comportamenti individuali si è ricavato che le persone hanno una propensione a rispondere a domande dirette e impreviste o ad aiutare qualcuno che sembra in difficoltà. Tali comportamenti, se vogliamo umani e solidali, sono oggetto di attenzione anche da parte dei criminali con lo scopo di sviluppare **truffe** a livello informatico.
Parliamo, quindi, anche di "**Frode informatica**".

Art. 640-ter: è disposto che "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 e con la multa".
Art. 640-quinquies, '**Frode informatica del soggetto che presta servizi di certificazione di firma elettronica**': Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione e con la multa".
Nel codice tra i '**delitti contro la persona**', e più nello specifico tra le norme a tutela delle conversazioni e delle comunicazioni, il legislatore ha predisposto un articolo, il 623-bis, a tutela della riservatezza delle informazioni trasmesse a distanza in qualunque forma, quindi anche elettronica.

Art. 617-quater, '**Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche**': "Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione". La stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni (intercettate).
Art. 617-quinquies, '**Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche**': "Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni … è punito con la reclusione". Si è puniti solamente installando le apparecchiature, anche senza ascoltare comunicazioni.
Art. 617-sexies, '**Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche**': "Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione".
L'intercettazione è consentita solo in particolari eccezioni, come contrabbando di droga, esplosivi ecc…
Alcune fattispecie su cui è utile soffermarsi sono legate al grave e dilagante fenomeno della **pedopornografia**.

Art. 600-ter, "**Pornografia minorile**": "Chiunque, … con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico…, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto è punito con la reclusione e con la multa …", specificando ai commi successivi che "Chiunque … offre o cede ad altri, anche a titolo gratuito, il materiale pornografico … la pena è aumentata … ove il materiale sia di ingente quantità" e che "Chiunque assiste a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto".
Art. 600-quarter, "**Detenzione di materiale pornografico**": prevede la pena della reclusione e della multa per "Chiunque … consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto", prevedendo un aumento di pena laddove il materiale detenuto sia di ingente quantità.
Infine, un cenno ad un articolo per contrastare il revenge-porn:
Art. 612-ter, "**Diffusione illecita di immagini o video sessualmente espliciti**": "… 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 … e con la multa …".

Per aumentare le attività di contrasto al fenomeno dei crimini informatici, nel 2004, è stata istituita l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (**ENISA**), la cui attività di monitoraggio, di consulenza alle istituzioni e di contrasto al cybercrime se oggi risultasse indiscutibilmente utile, per il prossimo futuro andrebbe quantomeno potenziata.

Sezione 6

Dati personali

Ciascuna persona è padrona del suo essere e dei dati che la riguardano e l'ordinamento giuridico introduce una serie di strumenti idonei affinché ciascuno possa per controllarne l'integrità e contrastare eventuali abusi, per non trasferire ad altri le libertà che lo Stato riconosce. I dati che ci riguardano sono oggetto di trattamento in maniera distribuita da una moltitudine di sistemi di gestione, di analisi e di archiviazione (scuola, anagrafe ecc…). Difendere i dati che ci riguardano significa essere liberi di fare scelte, fuori dai condizionamenti esterni, ed essere liberi di esprimere la nostra persona, contro chi vorrebbe, e spesso ci riesce, l'omologazione, lo schiacciamento, il controllo.
Nella Convenzione internazionale a Roma nel 1950 è stato firmato
l'Art. 8: "Ogni persona ha diritto al rispetto della sua vita privata (anche virtuale) e familiare, del suo domicilio (anche informatico) e della sua corrispondenza (anche elettronica).".
A tutela dei diritti indicati nelle prescrizioni legislative appena riportate, di ordine generalissimo, ogni individuo ha il potere di ricorrere innanzi alla Corte europea dei diritti dell'uomo di Strasburgo in via sussidiaria, cioè dopo aver percorso le vie giurisdizionali del paese di origine. La prima legge italiana dedicata interamente alla protezione dei dati personali è la n. 675/1996, denominata "**Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali**". Ma con il decreto legislativo n. 196 del 30/06/2003, denominato "**Codice in materia di protezione dei dati personali**", l'Italia ha espresso il primo tentativo al mondo di composizione sistematica ed organica delle disposizioni relative alla tutela dei dati personali.
Il Regolamento dell'Unione europea n. 679/2016, denominato **General Data Protection Regulation (GDPR)** è stato approvato il 27 aprile 2016 dal Parlamento e dal Consiglio dell'Unione Europea. Si compone di 99 articoli e 173 'Considerando'. Il **Regolamento europeo** è una fonte normativa di portata generale, è valido e uguale per tutti gli Stati membri dell'Unione ed è obbligatorio in tutti i suoi elementi e direttamente applicabile. Le sue norme producono effetti vincolanti nei confronti di tutti coloro – autorità pubbliche e soggetti privati – che sono soggetti al rispetto del diritto dell'Unione europea. Il 25 maggio 2018, data in cui il GDPR è diventato pienamente operativo, il Gruppo Art. 29 (gruppo costituito da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati) è stato sostituito dal **Comitato europeo** per la protezione dei dati, quale organo avente il compito di garantire l'applicazione del Regolamento.

L'ambito di applicazione materiale e territoriale del GDPR

Il GDPR 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. Il GDPR 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:

1. l'offerta di beni o la prestazione di servizi ai suddetti Interessati nell'Unione
2. il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione

Il GDPR si rivolge a tutti coloro che trattano dati personali di residenti in Ue, indipendentemente da dove è ubicata la sede del trattamento.

Figure chiave del GDPR

I soggetti implicati nei processi di trattamento dei dati personali sono il **Garante**, il **Titolare** ed il **Responsabile del trattamento**, il **Responsabile per la protezione dei dati** e il **soggetto** Interessato. Il **Garante** per il trattamento dei dati è un'Autorità amministrativa indipendente; il Regolamento prevede la costituzione di un'Autorità di controllo in ciascuno Stato membro e fissa identici compiti e poteri per le Autorità in tutti i paesi dell'Ue. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione. Il Garante è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento. Tra i principali compiti assegnati al Garante si possono indicare i seguenti:

1. sorveglia e assicura l'applicazione del Regolamento;
2. promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento, con particolare attenzione ai minori;
3. fornisce consulenza al Parlamento nazionale, al Governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;
4. su richiesta, fornisce informazioni all'Interessato in merito all'esercizio dei propri diritti derivanti dal Regolamento e, se del caso, coopera a tal fine con le Autorità di controllo di altri Stati membri;
5. tratta i reclami proposti da un Interessato, o da un organismo, un'organizzazione o un'associazione e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini.

In estrema sintesi, si può dire che il Garante ha poteri di indagine, correttivi, autorizzativi, consultivi e di infliggere sanzioni amministrative pecuniarie.
Il **Titolare** è la persona fisica o la persona giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo, cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Il Titolare mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.
Il **Responsabile** del trattamento è la persona fisica o la persona giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo, designato dal Titolare del trattamento, che tratta dati personali per conto di quest'ultimo. È una figura facoltativa.
Tra le novità più rilevanti riportate nel GDPR vi è senz'altro il concetto di "**accountability**". Si tratta di una previsione, per così dire, strategica e consiste in una investitura del Titolare e del Responsabile di una particolare forma di responsabilità che li obbliga a dare conto del proprio operato. Questi, infatti, per garantire il corretto trattamento dei dati personali dovranno rendicontare il loro operato, dimostrando di aver adottato misure idonee per assicurare affidabilità e competenza nella gestione dei dati personali. Il principio di accountability è declinato in tre attività:

- la "**trasparenza**" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in quanto utenti del servizio;
- la "**responsività**" intesa come la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste in merito al trattamento effettuato
- la "**compliance**" intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione all'obiettivo stabilito nelle leggi che nel senso di osservare e far osservare le regole di comportamento a chiunque interviene nella filiera del trattamento. Il Titolare ed il Responsabile del trattamento devono essere in grado di dimostrare che hanno adottato un complesso di misure giuridiche, organizzative e tecniche per la protezione dei dati personali

L'accountability, così com'è intesa nel GDPR, determina una inversione dell'onere della prova in caso di danno di qualsiasi natura derivante dal trattamento dei dati relativi ad un soggetto: il Titolare e il Responsabile sono tenuti a dimostrare di aver utilizzato tutti gli accorgimenti necessari per scongiurare il verificarsi dell'evento dannoso (tecnicamente, **data breach**); il danneggiato dovrà soltanto dichiarare di aver subito un danno ed è in tal modo dispensato dal dimostrare, ad esempio, la falla del sistema informatico. Proseguendo nella disamina delle figure chiave enunciate nel GDPR, all'art. 37, è previsto il **Data Protection Officer** (**DPO**) o Responsabile della protezione dei dati (**RPD**). Si tratta di una persona fisica, il cui ruolo si colloca funzionalmente tra la vigilanza dei processi interni alla struttura e la consulenza; ha quindi una doppia veste e funge da '**ponte di contatto**' tra la realtà in cui opera e l'Autorità Garante nazionale. Il DPO deve essere nominato quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico. L'art. 39 prescrive che il DPO deve svolgere, in piena autonomia e indipendenza, i compiti qui di seguito sinteticamente riportati: informare e fornire consulenza al Titolare e al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR; sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati; cooperare con il Garante per la protezione dei dati personali.
L'Interessato o data subject, infine, è la persona fisica cui si riferiscono i dati personali. Il Regolamento non si applica nel trattamento di dati anonimi. Ai sensi dell'art. 4, par. 1, del GDPR, per **dato personale** si intende «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».

Trattamento dei dati personali

Per trattamento dei dati personali si intende "**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, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".
Distinguiamo tre terminologie:

- Principio di **necessità**: il Titolare deve trattare **esclusivamente** i dati indispensabili per l'attività o il servizio che svolge per conto del soggetto Interessato.
- Privacy by **design**: il Regolamento intende richiamare l'attenzione dei Titolari sull'esigenza che la protezione dei dati personali venga garantita **fin dalla progettazione** dei sistemi o dei mezzi per il trattamento.
- Privacy by **default**: la protezione dei dati personali deve essere garantita per «impostazione predefinita», cioè i sistemi devono essere predisposti affinché la privacy sia garantita già dalla **prima applicazione**.

Liceità del trattamento

Il trattamento di dati personali di altre persone fisiche può essere effettuato solo se è fondato su una base giuridica certa. In altri termini, il trattamento è lecito soltanto se è fondato su uno dei seguenti punti:

1) l'Interessato ha espresso il proprio consenso per una o più specifiche finalità
2) è necessario per l'esecuzione di un contratto di cui l'Interessato è parte (busta paga ecc…)
3) è necessario per adempiere ad un obbligo legale al quale è soggetto il Titolare del trattamento (i dottori che devo spedire i dati dei pazienti o le università ecc…)
4) è necessario per salvaguardare degli interessi vitali dell'Interessato o di altre persone fisiche (ricovero di urgenza ecc…)
5) è necessario per l'esecuzione di un compito di pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento
6) è necessario per il perseguimento di un legittimo interesse del Titolare del trattamento (marketing), a condizione che non prevalgano i diritti e le libertà fondamentali dell'Interessato che richiedono una protezione maggiore dei dati personali (come i minori)

Ai sensi degli artt. 12-14, **l'informativa** è un documento che illustra le ragioni e le finalità della raccolta dei dati, la base giuridica del trattamento, i dati dei soggetti legittimati al trattamento, la natura obbligatoria o facoltativa del conferimento dei dati per ricevere un determinato servizio, il periodo di conservazione dei dati, i diritti degli Interessati, l'esistenza di un processo decisionale automatizzato (profilazione), l'eventuale trasferimento ad altri soggetti dei dati raccolti, l'eventuale trasferimento dei dati in paesi extra Ue, ecc. L'informativa deve essere, di norma, fornita direttamente agli Interessati al momento della raccolta dei dati (come la checkbox).

I soggetti cui si riferiscono i dati personali, nella loro qualità di Interessati, hanno il diritto in qualunque momento di chiedere al Titolare del trattamento informazioni in merito all'esercizio dei propri diritti. In particolare, hanno diritto di conoscere i contatti del Titolare, conoscere le finalità e le origini dei loro dati, chiedere la rettifica o cancellazione dei dati, revocare il consenso dei loro dati (in alcuni casi, non verranno più raccolti dati dal momento in cui viene revocato il consenso, ma rimangono quelli di prima). Tuttavia, è lecita l'ulteriore conservazione dei dati qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica e storica o finalità statistiche o per accertare, esercitare o difendere un diritto in sede giudiziaria. Qualora i dati personali siano trattati per **finalità di marketing** diretto, l'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità.

Registri e Data Protection Impact Assessment (DPIA)

È previsto all'art. 30 che il Titolare e, ove previsto, il Responsabile del trattamento tengano i **registri delle attività** di trattamento svolte sotto la propria responsabilità. I registri del Titolare e del Responsabile hanno contenuti lievemente differenti e, per sommi capi, devono contenere: il nome e i dati di contatto del Titolare e del Responsabile e, ove presente, del Responsabile della protezione dei dati e le finalità del trattamento; la descrizione delle categorie di trattamenti e delle categorie degli Interessati; se vi è trasferimento dei dati verso paesi extra Ue; la descrizione delle misure di sicurezza, tecniche ed organizzative adottate. La valutazione d'impatto sulla protezione dei dati o **Data Protection Impact Assessment** (DPIA) è un'attività prescritta agli artt. 35-36. Allorquando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è previsto che il Titolare effettui, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Data Breach e violazioni

Il Regolamento prevede espressamente l'obbligo del Titolare di notifica e comunicazione tempestiva all'Autorità di controllo in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti Interessati. Nel caso in cui la violazione sia accertata e sia di grado elevato, la procedura prescrive, altresì, la comunicazione agli Interessati. Appurato il rischio conseguente dalla violazione, gli Art. 33 e 34 del GDPR indicano ai Titolari i termini, le modalità, i contenuti e le deroghe della notifica e della comunicazione di **data breach**. L'Art. 33 impone al Titolare di notificare la violazione all'Autorità di controllo entro 72 ore dal momento in cui ne viene a conoscenza. Il tempo di riferimento da cui iniziano a decorrere i termini della notifica viene individuato quindi nel momento in cui il Titolare acquisisce consapevolezza dell'avvenuta violazione.
L'art. 33 dispone l'obbligo in capo al Responsabile del trattamento di informare tempestivamente il Titolare dell'avvenuta violazione. In linea di principio, il Titolare deve considerarsi a conoscenza della violazione nel momento in cui il proprio Responsabile ne sia venuto a conoscenza.

Regime sanzionatorio

Per la violazione delle norme poste a tutela della protezione dei dati il GDPR prevede l'applicazione di **sanzioni amministrative** pecuniarie. L'Art. 82 del GDPR, prevede la possibilità per l'Interessato che subisca un danno materiale o immateriale di ottenere il risarcimento del danno dal Titolare o dal Responsabile. Si incorre nelle sanzioni nei casi qui di seguito esemplificati:

- violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- trattamento illecito di dati personali che non richiede l'identificazione dell'Interessato;
- mancata o errata notificazione e/o comunicazione di un data breach all'Autorità nazionale competente;
- violazione dell'obbligo di nomina del DPO;
- mancata applicazione di misure di sicurezza;
- inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;
- trasferimento illecito cross-border di dati personali ad un destinatario in un paese terzo

Codice etico, codice di comportamento e certificazione

Sono norme giuridiche di grado subordinato che si aggiungono alle norme primarie di settore. In particolare, il **codice etico** esprime i principi, i valori e gli ideali dell'ente/azienda/attività professionale in genere, giuda i processi decisionali e l'attività produttiva ed è rivolto all'esterno. Il **codice di comportamento**, che origina dal codice etico, ha rilevanza interna e guida l'agire dei singoli; è rivolto alle persone che lavorano presso un ente/azienda o che svolgono un'attività professionale o che con quella vengono in contatto nella qualità di utenti/clienti o prestano un servizio per conto della stessa.
All'art. 40 del GDPR si trova un riferimento specifico ai codici di condotta in materia di protezione dei dati personali. In particolare, è disposto che

1) Gli Stati membri, le Autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento
2) Le associazioni e gli altri organismi rappresentanti le categorie di Titolari del trattamento o Responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a:

    a. il trattamento corretto e trasparente dei dati;
    b. la raccolta dei dati personali;
    c. la pseudonimizzazione dei dati personali;
    d. l'informazione fornita al pubblico e agli Interessati;
    e. l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
    f. la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'Interessato;

Ai sensi dell'art. 42, gli Stati membri, le Autorità di controllo, il Comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai Titolari del trattamento e dai Responsabili del trattamento.
In conclusione, si può affermare che tra le misure volte a prevenire fenomeni di violazione della riservatezza rientrano anche i codici di condotta. La funzione di guida e di dissuasione dal commettere atti in violazione delle norme a protezione della riservatezza, soprattutto se contenute in codici di condotta certificati, aggiungono un importante tassello di compliance al GDPR che il Titolare può vantare.