CONCETTI GIURIDICI DI BASE

Cos'è il "diritto" e cos'è una "norma"

"*Ubi societas ibi ius*": ogni società, ogni comunità umana stabile non può "vivere" e funzionare senza un complesso di regole che disciplinino i rapporti tra gli individui, con apparati che si incarichino di farle osservare. Occorrono, quindi, regole di condotta che governino il comportamento che ogni membro del "gruppo" deve osservare per assicurare una ordinata e pacifica convivenza e facilitare la collaborazione tra i membri del gruppo.

Una delle funzioni del diritto è quella di risolvere i conflitti con l'applicazione di regole predeterminate, le quali stabiliscono quale fra gli interessi che dovessero eventualmente entrare in conflitto sia degno di protezione e debba prevalere e quali, invece, non siano degni di protezione (o non lo siano in relazione ad altre posizioni meritevoli di maggiore tutela) e debbano, pertanto, soccombere.

Il sistema delle regole mediante le quali è organizzata una determinata collettività e viene disciplinato e diretto lo svolgimento della vita sociale costituisce l'"ordinamento giuridico". Qualunque organizzazione sociale costituisce, dunque, un ordinamento giuridico, ossia un insieme di norme di condotta che regolano la vita dei membri di una comunità allo scopo di garantirne la pacifica convivenza e di regolare le azioni degli esseri umani che vi appartengono. In sintesi, dunque: il diritto è costituito dalle regole che disciplinano una determinata organizzazione e che, considerate nel loro insieme, formano un "ordinamento giuridico".

Il diritto non è monopolio di una sola organizzazione (nemmeno dello Stato), ma inerisce a qualsiasi organizzazione: comunità internazionale, confessioni religiose organizzate, imprese commerciali, associazioni sportive… tutte queste organizzazioni producono diritto, che a più livelli si intreccia con quello prodotto dalle altre organizzazioni. Ogni individuo è dunque assoggettato alle regole di uno o più ordinamenti ed esistono vari livelli di produzione di norme (pubblici, ma anche privati).

Oggetto di studio sarà, in particolare, il diritto che riceve attuazione nel territorio italiano, o comunque attraverso l'autorità dello Stato italiano o, in termini più tecnici, il diritto vigente in Italia (che include, per effetto dell'adesione dell'Italia all'Unione Europea, anche il diritto proveniente dall'Unione, nonché il diritto internazionale, formato, in estrema sintesi, dall'insieme delle convenzioni e dei trattati, multilaterali o bilaterali, di cui l'Italia è parte).

Le "regole" non provengono solo da soggetti "pubblici" (lo Stato, le autorità che trovano nello Stato la loro legittimazione, l'Unione Europea, ecc.), ma derivano anche da vincoli che i soggetti privati si "auto-impongono", nell'esercizio della loro autonomia (autonomia privata), regolando spontaneamente i propri rapporti mediante, ad esempio, la stipula di contratti, il compimento di atti unilaterali vincolanti, ecc.

"Come è fatta" una norma?

Una norma è un enunciato che si articola, in astratto, come segue:

- la formulazione di una **ipotesi di fatto** ("se succede X, allora Y"; "se si vuole porre in essere un'attività X, allora occorre fare Y", ecc.), che viene tecnicamente

definita "fattispecie" (che può essere anche complessa, ossia esigere che più fatti concorrano);

- l'**effetto giuridico** che è conseguenza del verificarsi, nei fatti, della suddetta specifica ipotesi, e che può consistere, ad esempio:
    - nell'acquisto di un diritto (ad esempio, se il soggetto X pone in essere un'attività Y, allora X ha diritto a ricevere l'incentivo Z);
    - nell'insorgere di un dovere o di una obbligazione (ad esempio, se il soggetto X si obbliga nei confronti di Y a porre in essere una determinata attività Z e X non adempie a questo obbligo, X è obbligato a risarcire il danno che ha causato a Y);
    - nell'applicazione di una pena o di una sanzione (ad esempio, se il soggetto X cagiona la morte di un essere umano Y, X è punito con la reclusione non inferiore a 21 anni).

Come nelle equazioni matematiche, dunque, anche nel diritto una variabile ne determina un'altra.

Come si evince dalla descrizione di cui sopra, le norme giuridiche sono:

- **generali**: non sono dettate per singoli individui, e quindi per applicarsi ad una sola persona o ad un gruppo di persone singolarmente e specificamente predeterminate (individuabili "con nome e cognome"), ma a tutti i consociati o a determinate classi/gruppi/categorie generiche (ad esempio, la categoria "studenti universitari", la categoria "produttori", la categoria "commercianti", ecc.);
- ed **astratte**: le norme non sono dettate per specifiche situazioni concrete, ma per fattispecie (ipotesi di fatto) astratte, ossia per situazioni descritte ipoteticamente e delle quali occorre, quando si applica la legge, verificare la sussistenza in concreto.

La norma ha quindi lo scopo di regolare una serie indeterminata di casi futuri ed eventuali e si presta ad applicarsi a chiunque si verrà a trovare nella situazione prevista dalla norma. Compito del giurista, dunque, è quello di applicare la norma, interpretarla e verificarne la applicabilità ad una determinata situazione di fatto, con ogni conseguenza.

Diritto pubblico vs. diritto privato:

Si è fatto cenno sopra alla cosiddetta "autonomia privata". Si tratta di un concetto fondamentale per il diritto ed è una locuzione con la quale ci si riferisce al potere dei privati di regolare liberamente i propri interessi e di decidere della propria sfera giuridica, nel rispetto dei limiti e degli obblighi stabiliti dall'ordinamento.

Il diritto viene tradizionalmente suddiviso in due macro-aree, ossia quella del diritto pubblico e quella del diritto privato:

- Diritto pubblico: disciplina l'organizzazione dello Stato e degli altri enti pubblici e regola come si esplicano i pubblici poteri (quali sono gli organi competenti ad esercitarli, come devono essere esercitati, ecc.). Regola, quindi, i rapporti dei quali è parte lo Stato o un altro ente pubblico.

Sotto-categorie del diritto pubblico sono, ad esempio, il diritto costituzionale, il diritto amministrativo, il diritto penale, il diritto tributario ed il diritto processuale.

- Diritto privato: disciplina le relazioni tra individui privati, per l'appunto, siano essi singoli o enti (società, associazioni, ecc.), che operano su un piano di "eguaglianza". È l'insieme delle regole affidate all'autonomia dei privati che regolano da soli i propri rapporti, ad esempio attraverso contratti (nei limiti previsti dal codice civile) o altri vincoli di natura, per l'appunto, civilistica (si pensi al matrimonio o alle unioni civili, che, tuttavia, pur essendo disciplinati in norme di natura privatistica, ed *in primis* nel codice civile, hanno un rilievo anche per lo Stato ed effetti di natura, dunque, pubblicistica)

  Ad esempio, si pensi al diritto dei contratti, al diritto delle società, alle norme sulla proprietà, così come a quelle in materia di diritto di famiglia, ecc.

Occorre comunque ricordare che quella tra diritto pubblico e diritto privato è una distinzione "tradizionale", soprattutto "didattica" ed orientativa, rielevante quale criterio di massima, nonostante la linea di demarcazione tra diritto pubblico e diritto privato sia quantomeno variabile e non tutto ciò che riguarda soggetti, attività e beni pubblici attenga al diritto pubblico. Anche dove ci si affida ai privati, lo Stato non è del tutto assente, ma si limita a definire il quadro entro il quale i rapporti privatistici si sviluppano, per assicurare che tra i soggetti privati esista una certa parità e che la loro attività non contrasti con l'interesse generale. Per contro, anche lo Stato e gli enti pubblici agiscono assai spesso secondo le norme di diritto privato: comprano o vendono beni, danno o prendono in locazione, partecipano a società per azioni o esercitano direttamente imprese come qualsiasi altro privato, ottemperando alle stesse norme che regolano i rapporti tra privati.

Le norme del codice civile che regolano gli istituti caratteristici del diritto privato (proprietà, contratto, responsabilità civile, impresa…) sono norme applicabili sia a soggetti privati, sia ai soggetti pubblici, salvo che non sia espressamente previsto che si applichino solo ai primi (come nel caso, ad esempio, degli istituti che regolano il diritto di famiglia).

Le fonti del diritto

Con la locuzione "fonti del diritto" ci si riferisce all'insieme degli atti e dei fatti (comportamenti materiali) che concorrono a produrre diritto, ossia ad introdurre nuove norme, a modificare quelle esistenti o a rinnovarle nel corso del tempo:

- atti: norme scritte emanate da organi o autorità titolari del potere di produrre norme (ad esempio, una legge del parlamento, un decreto di un sovrano assoluto, ecc.);
- fatti: usi e consuetudini che, in quanto affermatisi nel tempo e ripetutisi regolarmente, l'ordinamento riconosce come idonei a produrre diritto e vincolanti (si tratta di fonti che, nel nostro tempo, ricoprono una portata residuale). La consuetudine è un comportamento ripetuto nel tempo con la convinzione, da parte del corpo sociale, che ripetere quel comportamento sia giuridicamente dovuto.

Quelle di cui sopra sono le cosiddette "fonti di produzione", che si distinguono dalle cosiddette "fonti di cognizione", ossia i documenti e le pubblicazioni ufficiali dalle quali

si può prendere conoscenza del testo normativo (ad esempio, la Gazzetta Ufficiale della Repubblica Italiana o la Gazzetta Ufficiale dell'Unione Europea). Un'ulteriore distinzione è, poi, quella tra "fonti di produzione" e "fonti sulla produzione", ossia quelle norme che disciplinano da chi e come le norme vengono prodotte (ad esempio, la procedura con la quale il Parlamento approva le leggi).

Le fonti (di produzione) del diritto seguono una gerarchia, secondo uno schema che può essere descritto come una piramide, al cui vertice sono collocate le fonti di rango più elevato ed ai livelli inferiori quelle di minor rango. L'ordine gerarchico aiuta a risolvere eventuali conflitti fra norme (e fonti) che dovessero risultare in contrasto tra loro. La domanda è, dunque: quale tipo di norma prevale su quale, in caso di contrasto?

Le disposizioni preliminari al codice civile (cosiddette "Preleggi"), emanato nel 1942, individuano quattro tipologie di fonti: 1. la legge; 2. i regolamenti; 3. le norme corporative (che hanno perduto efficacia con la caduta del fascismo); 4. gli usi. All'elenco si sono aggiunte, nel dopoguerra, altre fonti (*in primis*, la Costituzione, entrata in vigore nel 1948, ma anche le norme derivanti dall'Unione Europea) e, dunque, la gerarchia delle fonti risulta oggi molto più articolata e complessa. Di seguito si esamineranno, in estrema sintesi, quali siano, per lo Stato italiano, le fondamentali fonti del diritto ed in quale ordine gerarchico esse si pongano.

Prima di procedere oltre nell'esame delle fonti del diritto, occorre premettere una sintetica digressione sulla tradizionale tripartizione dei poteri che caratterizza tutte le forme di stato democratiche. Il modello di tripartizione dei poteri consiste, in estrema sintesi, nella individuazione di tre funzioni pubbliche principali che sono tradizionalmente assegnate allo stato di diritto e che sono attribuite a distinti organi (o complessi di organi):

- il potere legislativo (il potere di "produrre leggi");
- il potere esecutivo (il potere di dare esecuzione alle leggi, attuandole e mettendo in pratiche politiche per perseguire gli obiettivi che lo stato si pone);
- il potere giudiziario (il potere di giudicare eventuali violazioni della legge e sanzionarle).

Nei modelli di stato democratici queste tre funzioni non vengono mai a sovrapporsi e non vengono mai attribuite allo stesso organo (o agli stessi organi), salvo specifiche eccezioni. Così, ad esempio, un organo che detenga il potere legislativo non può detenere anche quello esecutivo o quello giudiziario, e così via. Questo al fine di evitare eventuali distorsioni democratiche, abusi o fenomeni *lato sensu* corruttivi. Così, in Italia ma non solo:

- il potere legislativo è generalmente attribuito al Parlamento (che si compone, in Italia, di due camere, ossia la Camera dei Deputati ed il Senato);
- il potere esecutivo è attribuito al Governo (formato, in Italia, da diversi Ministeri ed a capo del quale è collocato il Presidente del Consiglio dei Ministri);
- il potere giudiziario è attribuito alla magistratura.

Il Presidente della Repubblica non è a capo di una specifica funzione, ma ha, in estrema semplificazione, il compito di coordinare gli organi deputati ad ognuna delle funzioni e di sorvegliare sul loro corretto funzionamento, nonché di essere garante del rispetto della Costituzione.

1. La **Costituzione**

Entrata in vigore nel 1948 (approvata da un'Assemblea Costituente eletta in seguito al referendum che, dopo la fine della seconda guerra mondiale, assegnò allo Stato la forma repubblicana in luogo di quella monarchica), è la norma fondamentale per il nostro Stato, l'atto supremo dell'ordinamento, di fronte al quale tutti gli altri atti fonte sono subordinati. Essa:

- è la fonte dalla quale traggono fondamento tutti i poteri costituiti (in primo luogo, quelli che sono deputati a creare le leggi) ed è, dunque, la fondamentale norma sulla produzione giuridica, regolando il processo di formazione delle leggi;
- può essere modificata soltanto mediante uno speciale procedimento di revisione costituzionale più complesso di quello previsto per le leggi ordinarie (cosiddetta "rigidità" della Costituzione), ed in ogni caso soltanto entro determinati limiti.

Esiste, infatti, un "nucleo rigido" di previsioni della Costituzione che non sono "negoziabili", né revisionabili, e che costituiscono principi fondamentali, tra cui il principio di eguaglianza, le norme sui fondamentali diritti e doveri dei cittadini (libertà di manifestazione del pensiero, inviolabilità della libertà personale del domicilio, libertà di circolazione, libertà di associazione, libertà di professione della fede religiosa, tutela della proprietà privata) e la forma repubblicana dello Stato italiano.

Al suddetto nucleo fondamentale di norme si aggiungono le altre norme della Costituzione, che disciplinano vari aspetti attinenti al funzionamento dello Stato, tra cui il processo di formazione delle leggi, la disciplina delle cariche istituzionali (ad esempio, il Presidente della Repubblica), il funzionamento degli organi (Parlamento, Corte Costituzionale, ecc.), il sistema elettorale, il sistema giudiziario, ecc.

La Costituzione italiana è definita come "rigida", in quanto una legge ordinaria dello Stato non può né modificare la Costituzione o altra legge di rango costituzionale, né contenere disposizioni in qualsiasi modo in contrasto con norme costituzionali.

Qualsiasi altra fonte del diritto che si ponga in contrasto con le norme della Costituzione è per ciò solo illegittima, ossia incostituzionale. Esiste un apposito organo, la Corte Costituzionale, cui è affidato il compito di stabilire se le disposizioni di una legge siano

in conflitto con norme costituzionali. Il singolo privato cittadino non può rivolgersi direttamente alla Corte Costituzionale per chiedere un controllo di legittimità costituzionale di una disposizione normativa, ma deve sollevare la questione nell'ambito di una specifica controversia dinanzi ad un giudice "ordinario" che, se ritiene la questione di costituzionalità meritevole di essere esaminata (ossia non manifestamente infondata), sospende il giudizio e devolve la questione (ossia "passa la parola") alla Corte Costituzionale. Se quest'ultima ritiene che una norma contrasti con quanto previsto dalla Costituzione, ne dichiara con sentenza la incostituzionalità, con l'effetto che la norma in questione cessa di avere efficacia dal giorno successivo alla pubblicazione della decisione.

2. Le fonti dell'**Unione Europea**

L'Italia aderisce dal 1957 all'Unione Europea (precedentemente, "Comunità Europea"), ed è anzi uno dei suoi paesi fondatori (insieme a Belgio, Germania, Francia, Lussemburgo e Paesi Bassi). Mediante tale adesione (effettuata mediante l'adesione a trattati internazionali), l'Italia, come tutti i paesi membri dell'UE, ha ceduto parte della propria sovranità (quantomeno con riguardo a talune materie) all'Unione ed ai suoi organi, i quali producono norme che si intrecciano con quelle nazionali e si inseriscono nel quadro delle fonti del diritto in funzione primaria, prevalendo sulle fonti interne di rango ordinario (leggi, atti aventi forza di legge, leggi regionali e regolamenti)[1].

All'UE gli Stati membri hanno attribuito una serie di competenze, delle quali:

- alcune esclusive, ossia afferenti ad ambiti nei quali soltanto l'Unione ha competenza a legiferare (dogane, politica monetaria, ecc.);
- ed altre concorrenti, ossia afferenti ad ambiti nei quali gli Stati membri possono legiferare soltanto laddove l'Unione non lo abbia già fatto, o comunque nel perimetro e secondo i principi tracciati dall'Unione (mercato interno, protezione dei consumatori, energia, ecc.).

Le principali fonti di matrice eurounitaria sono le seguenti:

- i regolamenti: sono atti di portata generale e direttamente efficaci ed obbligatori in tutti i loro elementi. In semplificazione estrema, si tratta di atti normativi applicabili dai giudici come se fossero leggi dello Stato Italiano, senza necessitare di essere recepiti dal legislatore italiano con un'apposita legge che ne "traduca" il contenuto in una fonte nazionale (ad esempio, il Regolamento sulla privacy noto come GDPR). In caso di contrasto tra un regolamento UE ed una legge nazionale, il giudice italiano deve disapplicare la norma interna e applicare con prevalenza la norma regolamentare;
- le direttive: sono atti normativi che necessitano di un recepimento da parte del legislatore nazionale per essere efficaci nell'ordinamento dei singoli Stati, e che devono dunque essere attuati mediante apposite leggi emanate dal Parlamento (ad esempio, la nostra normativa in materia di danno da prodotto difettoso, oggi contenuta nel Codice del Consumo, deriva da una direttiva comunitaria; lo stesso dicasi per molta della disciplina in materia di comunicazioni elettroniche, di sicurezza dei prodotti, di governo delle piattaforme, di tutela del consumatore e

[1] L'art. 117 della Costituzione afferma che "*La potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali*".

molte delle specifiche previsioni che costituiranno oggetto del corso). Si tratta di atti che hanno, dunque, come destinatario principale lo Stato membro, al quale è imposto l'obbligo di recepire le direttive adattando le proprie leggi a quanto previsto dalle direttive medesime entro il termine previsto da queste ultime.

I trattati UE hanno istituito la Corte di Giustizia dell'Unione Europea, competente per giudicare sull'interpretazione delle norme di diritto UE. Le sentenze della Corte di Giustizia sono vincolanti per i giudici nazionali.

3. Le **leggi** statali e regionali (le cosiddette "fonti primarie")

Le leggi statali ordinarie sono approvate con una procedura prevista dalla Costituzione, che prevede [i)] l'approvazione della legge da parte del Parlamento nelle sue due Camere (Camera dei Deputati e Senato), [ii)] la promulgazione della legge da parte del Presidente della Repubblica e [iii)] la pubblicazione della legge sulla Gazzetta Ufficiale.

Vi sono materie che non possono essere regolate se non mediante leggi (c.d. "riserva di legge"), e, dunque, non possono essere disciplinate da fonti normative di rango inferiore (ad esempio i regolamenti).

Alle leggi ordinarie sono equiparati i decreti legge ed i decreti legislativi, ossia provvedimenti che, quanto ad efficacia, hanno lo stesso valore di una legge ma che sono emanati non dal Parlamento, bensì dal Governo (sono i cosiddetti atti aventi forza di legge). Ciò può avvenire:

- o in virtù di una legge di delega del Parlamento, che incarica il Governo a legiferare su una determinata materia indicando i principi ed i criteri ai quali il Governo deve attenersi nel farlo;
- o in presenza di casi straordinari di necessità ed urgenza, ma in questo caso il Parlamento deve convertire in legge il decreto legge del Governo entro 60 giorni, altrimenti perde efficacia.

Vi sono, poi, materie sulle quali anche le singole Regioni hanno competenza a legiferare (con proprie leggi regionali), seppur nei limiti e secondo i criteri essenziali fissati a monte dalla legge statale. Si parla, in questi casi, di "competenza legislativa concorrente" (istruzione, tutela della salute, ecc.).

Speciale posizione tra le leggi ordinarie statali è ricoperta a quelle leggi definite "**codici**", ossia il codice civile (c.c.), il codice penale (c.p.), il codice di procedura civile (c.p.c.), il codice di procedura penale (c.p.p.) ed il codice della navigazione (cod. nav.). Si tratta di raccolte di norme, più o meno corpose, che disciplinano un intero settore del diritto in modo organico. Il codice civile, in particolare, è stato promulgato nel 1942.

4. I **regolamenti** (le cosiddette "fonti secondarie")

I regolamenti sono fonti subordinate alla legge che possono essere emanate dal Governo, dai ministeri e da altre autorità amministrative, anche non statali (ad esempio, l'Autorità Garante della Concorrenza e del Mercato, l'Autorità Garante per le Comunicazioni, l'Autorità di Regolazione per Energia Reti e Ambiente, ecc.), quando previsto dalla legge e nei limiti da quest'ultima fissati.

Si tratta generalmente di previsioni più specifiche e dettagliate delle leggi ordinarie e che sono volte a disciplinare singoli specifici aspetti (ad esempio, il funzionamento di un determinato ente, il regolamento sul funzionamento del Parlamento, ecc.).

5. Il **diritto internazionale**

Il diritto internazionale è il diritto della "comunità degli stati", ossia l'insieme delle regole con le quali gli stati sovrani regolano i rapporti tra loro, disciplinano la collaborazione reciproca su determinate materie ed assumono obblighi l'uno nei confronti dell'altro, con conseguenze anche sui rispettivi cittadini.

La fonte tipica del diritto internazionale è il trattato, che può essere sia bilaterale (tra due stati) che multilaterale (tra più stati)[2]. Il trattato deve poi essere "ratificato" dal legislatore nazionale e, dunque, recepito nel diritto del singolo stato. La ratifica è, dunque, l'atto giuridico mediante il quale un soggetto (lo stato) fa propri gli effetti di un accordo concluso con altri stati da un proprio rappresentante (spesso il Ministro degli Esteri).

Esistono vari trattati, ad esempio, in materia di tutela dei diritti umani, ma non soltanto: esistono convenzioni in materia di tutela dei brevetti (ad esempio, il Trattato di Cooperazione in materia di Brevetti del 1970, che ha istituito l'Organizzazione Mondiale per la Proprietà Intellettuale - OMPI, con sede a Ginevra, competente anche per il deposito unificato di domande di brevetto valide in uno o più dei 153 stati aderenti al trattato, come una sorta di *one-stop-shop*), così come di marchi e di contratto (ad esempio, la Convenzione di Vienna sulla vendita internazionale di merci).

Efficacia della legge nel tempo e nello spazio

L'efficacia della norma consiste nella sua capacità di produrre effetti.

Una volta che la norma giuridica è stata emanata dagli organi competenti essa deve essere portata a conoscenza dei cittadini affinché possano osservarla. A tal fine la norma viene pubblicata sulla Gazzetta Ufficiale[3], e di regola entra in vigore dopo 15 giorni da tale pubblicazione, salvo che la legge stessa, come spesso avviene, non preveda un termine diverso.

L'efficacia della norma nel tempo va, dunque, dal momento della sua entrata in vigore fino a quello della perdita dell'efficacia, che può avvenire per effetto di abrogazione, sostituzione o modifica della stessa ad opera di altre norme (o anche, come si è detto, per effetto della dichiarazione di incostituzionalità della norma ad opera della Corte Costituzionale, o per annullamento da parte di un giudice - amministrativo - di regolamenti ritenuti illegittimi). Per "abrogazione" si intende la cessazione dell'efficacia di una norma per effetto di una fonte successiva di pari grado o di grado superiore[4].

---

[2] Altra fonte "tipica" del diritto internazionale è la consuetudine.

[3] Il riferimento è alla Gazzetta Ufficiale della Repubblica Italiana, ma esiste altresì una Gazzetta Ufficiale dell'Unione Europea, con le medesime funzioni.

[4] L'abrogazione può essere espressa o tacita. È espressa quando la legge successiva prevede specificamente che la sua entrata in vigore abroga, modifica o sostituisce le norme precedenti individuate dalla stessa (con previsioni quali "gli artt. X e Y della legge Z sono abrogati a partire dalla data di entrata in vigore della presente legge"). È tacita quando, pur non prevedendo espressamente l'abrogazione di alcuna norma, introduce contenuti che sono materialmente (e logicamente) incompatibili con quelli di norme precedenti.
L'abrogazione (espressa) può avvenire anche per effetto di un referendum abrogativo, strumento di democrazia diretta mediante al quale si richiede ai cittadini se vogliono o meno eliminare una determinata legge o parte di essa. Il referendum abrogativo non può concernere norme in materia di tributi, bilancio dello Stato, trattati internazionali, amnistia ed indulto. Il referendum abrogativo può essere richiesto da almeno 500.000 elettori o da cinque Consigli regionali e produce l'effetto di abrogare una norma ove ottenga un determinato quorum costitutivo (se partecipa alla votazione la maggioranza degli aventi diritto

Con la pubblicazione la legge si reputa conosciuta e diventa obbligatoria per tutti, ivi inclusi coloro che non ne abbiano mai avuto conoscenza. Vige, infatti, il principio per il quale *ignorantia legis non excusat*, in base al quale nessuno può invocare a propria giustificazione, per evitare una sanzione o comunque sottrarsi agli effetti della norma, di avere ignorato l'esistenza di una disposizione di legge.

In termini generali, la norma giuridica ha efficacia unicamente in relazione ai fatti che si verificano dopo la sua entrata in vigore (principio di irretroattività). Tale regola generale risponde ad una esigenza di certezza del diritto, ossia l'esigenza di mettere il cittadino nelle condizioni di sapere se un determinato comportamento è lecito o meno prima di porlo in essere, e di potere dunque prevedere le conseguenze giuridiche delle proprie azioni e decisioni. Principale eccezione a tale regola generale concerne la legge penale: la legge penale successiva, se più favorevole al reo, è retroattiva.

Quanto all'efficacia delle norme nello spazio (dove sono efficaci le norme di uno stato?), la problematica assume rilievo essenzialmente in scenari connotati da elementi di trans-nazionalità (ad esempio, una società estera, e dunque soggetta al diritto dello stato estero, che opera in Italia o viceversa) per comprendere quali norme si applicano in particolari circostanze.

Generalmente, le norme di uno stato sono efficaci solamente entro i confini dello stato stesso, ossia entro l'ambito territoriale nel quale lo stato esercita la propria sovranità (è il cosiddetto principio di territorialità), nel rispetto della sovranità degli altri stati (in termini generali, se le leggi emanate da uno stato avessero efficacia anche in un altro stato, ciò lederebbe la sovranità di quest'ultimo). Vi sono anche casi di applicazione extraterritoriale delle leggi statali (si pensi alle norme fiscali), ma occorre a tal fine che sussista un "collegamento" qualificato tra il soggetto estero ed il territorio italiano.

In termini estremamente generali, le leggi di uno stato si applicano anche agli stranieri che si trovano entro il territorio nazionale. Il principio si applica in primo luogo con riguardo alle leggi penali ed alle norme di polizia.

La tutela dei diritti ed il rispetto della legge: il potere giudiziario

Il rispetto delle leggi e la tutela dei diritti sono garantiti dal potere giudiziario, essenzialmente quindi dalla magistratura e dai tribunali. Quali magistrati e quali tribunali sono competenti dipende se si verta in ambito di diritto civile, di diritto penale o di diritto amministrativo:

- Diritto civile (o diritto privato): è il diritto dei rapporti tra soggetti privati, sia persone fisiche che persone giuridiche (obbligazioni, contratti, risarcimento del danno, testamenti, rapporti di famiglia, rapporti societari, ecc.);
- Diritto penale: è il diritto che riguarda i reati, ossia comportamenti che sono classificati come illeciti penalmente rilevanti, per i quali l'ordinamento prevede una pena (ergastolo, reclusione, arresto, ecc.);
- Diritto amministrativo: è il diritto che regola l'agire della pubblica amministrazione, quindi degli enti pubblici (Comuni, Regioni, lo Stato, l'Agenzia delle Entrate, i Ministeri, ecc.).

di voto) ed un determinato quorum deliberativo (se la maggioranza dei voti di coloro che hanno partecipato ha votato a favore dell'abrogazione).

Il diritto penale è amministrato dalla magistratura, che ha il compito di indagare sui reati e di perseguire i colpevoli, assicurando l'applicazione della pena prevista dalla legge. I privati che ritengono di avere subito un reato possono presentare denuncia o querela presso la forza pubblica, la quale poi indaga su quanto oggetto di denuncia o querela e, se ritiene sia stato commesso un reato, procede per ottenere l'applicazione della pena nei confronti del colpevole (la faccenda, dunque, viene gestita a livello di forza pubblica e, dopo la denuncia o querela, esce dalle mani del privato). Le questioni penali vengono, poi, portate davanti al tribunale penale, che decide l'applicazione della pena al colpevole.

Per le questioni di diritto amministrativo è competente una particolare tipologia di tribunali, che sono i Tribunali Amministrativi Regionali (T.A.R.), dinanzi ai quali i cittadini possono contestare ("impugnare", in termini tecnici) i provvedimenti adottati dalla Pubblica Amministrazione nei loro confronti.

Per quanto concerne, invece, i rapporti esclusivamente tra privati ogniqualvolta non venga in rilievo un reato - i rapporti, dunque, di natura civile - in termini estremamente semplici, colui che vuole tutelare un proprio diritto nei confronti di un altro soggetto deve "fargli causa", ossia citarlo in giudizio davanti al giudice (civile).

Per le cause in materia civile, sono previsti:

- il giudice di pace (che ha competenza limitata a cause di valore minore);
- il tribunale (giudice "di primo grado", competente per ogni questione che non sia di competenza del giudice di pace);
- la corte d'appello (giudice "di secondo grado", dinanzi al quale possono essere contestate - "impugnate", in termini tecnici - le sentenze del tribunale);
- la Corte di Cassazione (ultimo grado di giudizio, competente per eventuali contestazioni delle sentenze della corte d'appello ove errate in diritto).

La decisione assunta dal giudice in relazione ad un determinato caso è la sentenza, che stabilisce "chi ha ragione e chi ha torto" in una controversia tra chi ha fatto causa e chi è stato chiamato in giudizio, stabilendone anche le conseguenze (ad esempio, chi deve fare cosa, chi deve corrispondere un determinato importo a chi, chi deve risarcire il danno a chi, di chi è proprietà un determinato bene, ecc.).

Le sentenze, nel nostro ordinamento, non hanno valore vincolante generale, ma solo nei confronti delle parti del giudizio all'esito del quale sono state emesse: se X fa causa a Y davanti al tribunale Z ed il tribunale Z emette una sentenza nella causa, la sentenza ha effetto vincolante soltanto tra X ed Y (i quali sono tenuti a conformarsi a quella sentenza, e se non lo fanno commettono un reato). La sentenza può avere effetto di precedente, cioè può in qualche misura influenzare i giudici che successivamente dovessero trovarsi a giudicare una controversia analoga, ma questi resterebbero comunque liberi di decidere in altro modo (in questo senso, la sentenza non è vincolante per soggetti che non siano parte del giudizio nel quale è stata emessa).

Le sentenze della Corte di Cassazione hanno particolare valore e tendenzialmente tutti i giudici si conformano ad esse nella pratica, perché alla Corte di Cassazione è attribuito il compito di garantire la uniformità dell'applicazione della legge e della sua interpretazione.

I soggetti di diritto: persone fisiche e persone giuridiche

I "soggetti di diritto" sono coloro che possono essere titolari di situazioni giuridiche, ossia, in estrema semplificazione, di diritti, doveri ed obblighi (sono, in termini tecnici, titolari di "capacità giuridica").

I soggetti di diritto possono essere:

- **persone fisiche**, ossia, in termini semplici, gli esseri umani. Ogni essere umano è, per il diritto, una persona fisica.

  L'essere umano, per il solo fatto di essere nato, diviene automaticamente soggetto di diritto e, dunque, titolare di diritti e doveri (alcuni comuni a tutti, come ad esempio il diritto alla vita e quello alla libertà personale, altri specifici per alcune categorie di soggetti). La persona fisica sorge, dunque, al momento della nascita dell'essere umano;

- **persone giuridiche**, ossia gli enti, organismi unitari composti da un insieme di persone fisiche e da un complesso di beni (un patrimonio) organizzati per conseguire obiettivi determinati, ai quali l'ordinamento riconosce la capacità di essere soggetti di diritto, quindi di avere diritti, obblighi e doveri.

  Il più chiaro esempio di persona giuridica, di ente è la società di capitali (società per azioni o società a responsabilità limitata).

  Le persone giuridiche sono, dunque, entità che operano nel contesto sociale con una identità ed un ruolo distinti e diversi da quelli dei loro componenti. Ad esempio, i soci di una società per azioni sono giuridicamente distinti dalla società per azioni stessa e non coincidono con quest'ultima (in termini esemplificativi, la famiglia Agnelli/Elkann è diversa dalla FIAT).

  Un bene (ad esempio, un appartamento) può far capo direttamente all'ente in quanto tale (e non, dunque, ai singoli soggetti che lo compongono, che sono terzi rispetto all'ente). La responsabilità per un atto illecito (ad esempio, il ferimento di un passante, la violazione di una norma in materia di data protection, la violazione di un brevetto, ecc.) può far capo direttamente all'ente in quanto tale. Un contratto può intercorrere direttamente con l'ente in quanto tale (ad esempio, se X va in banca e parla con un funzionario della banca per ottenere un mutuo, il contratto di mutuo è stipulato tra X e la banca, e il funzionario resta estraneo ad esso, in quanto "organo" della banca).

  Così, se X vuole fare causa ad Amazon perché gli è stato consegnato un prodotto danneggiato, X fa causa ad Amazon in quanto ente, e non ai soci di Amazon, o al suo "proprietario", che restano estranei alla causa (perché il contratto di acquisto è stato stipulato tra X ed Amazon in quanto ente). Conseguentemente, se Amazon soccombe in giudizio (perde la causa) e viene condannata ad un risarcimento nei confronti di X, il risarcimento non è dovuto dai soci di Amazon personalmente (i quali non rispondono, dunque, con il proprio patrimonio personale), ma dalla sola Amazon, che risponde con il proprio patrimonio (soldi, beni immobili, ecc.).

Gli enti, ovviamente, non "esistono nel mondo materiale" e, dunque, non possono che agire che attraverso persone fisiche, che fanno parte della loro struttura organizzativa. Tali persone sono gli organi dell'ente, del quale fanno parte: ad esempio, per una società, i propri dipendenti ed i propri amministratori (amministratore unico o consiglio

di amministrazione, a sua volta composto da singole persone fisiche); ad esempio, per lo Stato, i suoi funzionari (dai Ministri fino all'impiegato pubblico).

L'ente risponde nei confronti dei terzi delle azioni dei propri dipendenti, dei propri organi o dei propri funzionari dei quali "si serve" per l'esecuzione delle proprie attività come se fossero proprie. Ad esempio, se un'auto dei carabinieri investe un pedone sulle strisce pedonali, dei relativi danni sarà chiamato a rispondere lo Stato; se un impiegato di una società non effettua le operazioni necessarie per proteggere i dati dei quali quella società si serve e ne deriva un danno per gli interessati, di tali danni risponde la società direttamente. Tanto, fermo restando che la società, pur rispondendo direttamente nei confronti dei terzi, potrà rivalersi sui propri organi per responsabilizzarli in relazione ai danni che questi ultimi hanno cagionato alla società stessa con la propria attività.

Taluni degli organi di un ente sono dotati di poteri di rappresentanza dell'ente nei confronti dei terzi, quindi di assumere impegni con terzi in nome e per conto dell'ente stesso, vincolando dunque (non se stessi, ma) l'ente al rispetto di quegli impegni. Ad esempio, contrarre un mutuo, acquistare un immobile, assumere un dipendente, ecc.: si tratta di contratti che materialmente vengono negoziati e firmati da un soggetto persona fisica (rappresentante dell'ente) ma che vengono stipulati dall'ente stesso, in capo al quale si producono gli effetti del contratto in questione.

Non tutti gli organi di un ente hanno la rappresentanza dell'ente stesso. Ad esempio, un operaio della FIAT non può, in generale, firmare un contratto con terzi che impegni la FIAT; l'Amministratore Delegato della FIAT, invece, può farlo.

Esistono:

- enti pubblici (Stato, Regioni, Comuni, Aziende Sanitarie Locali, INPS, INAIL, Garante per la Protezione dei Dati Personali, Autorità Garante per le Comunicazioni, Università Statali, Agenzia delle Entrate, ecc.);
- enti privati (società, associazioni riconosciute, ecc.).

Le obbligazioni e la responsabilità

Tra i soggetti di diritto esistono rapporti di varia natura, che il diritto tratta in modo diverso a seconda del loro contenuto e della loro origine. Uno di questi rapporti è l'obbligazione (o il rapporto obbligatorio) che vincola uno o più soggetti.

L'**obbligazione** è un rapporto giuridico in virtù del quale un soggetto è vincolato nei confronti di qualcun altro ad eseguire una determinata prestazione (cioè a tenere un determinato comportamento, a fare qualcosa, a dare qualcosa, o anche a non fare qualcosa). Perché si possa parlare di "obbligazione", la prestazione in questione deve essere patrimoniale, ossia suscettibile di valutazione economica.

Lo schema dell'obbligazione vede, dunque, il contrapporsi di due soggetti:

- il debitore, ossia colui che deve eseguire la prestazione;
- il creditore, ossia colui nei confronti del quale o nell'interesse del quale la prestazione deve essere eseguita.

Le due principali fonti delle obbligazioni (in estrema semplificazione ed ai nostri fini) sono il contratto ed il fatto illecito.

I. Il contratto e la responsabilità contrattuale

Sul concetto di contratto torneremo anche in seguito. Basti ora anticipare che il contratto è l'atto (spesso scritto ma a volte può essere anche non scritto) con il quale uno o più soggetti regolano i propri affari in relazione ad una specifica questione, obbligandosi reciprocamente a "fare qualcosa". Abbiamo già detto, infatti, che i soggetti privati possono decidere di vincolarsi reciprocamente al rispetto di "regole" che essi stabiliscono e che valgono, dunque, non per tutti, ma soltanto nei rapporti tra i privati medesimi (è il concetto di "autonomia privata"; v. sopra).

Le obbligazioni che derivano dal contratto possono essere di varia natura e dipendono dall'oggetto del contratto stesso: ad esempio, l'obbligazione di pagare un prezzo, l'obbligazione di fornire un determinato prodotto, l'obbligazione di consegnare un immobile, l'obbligazione di realizzare un certo prodotto o di erogare un certo servizio, ecc.

La corretta esecuzione di un contratto è il suo adempimento. Se una delle parti viola il contratto o non lo esegue o non lo esegue in modo esatto, si parla di inadempimento.

Il soggetto che non ha correttamente eseguito il contratto è inadempiente ed è responsabile nei confronti della propria controparte contrattuale (ossia dell'altra parte o delle altre parti del contratto) per tale inadempimento (responsabilità contrattuale). Il soggetto inadempiente, tra le altre cose, può essere anche tenuto a risarcire il danno che il proprio inadempimento ha causato all'altra parte.

II. Il fatto illecito e la responsabilità extracontrattuale

il **fatto illecito** è un comportamento contrario al diritto che viene posto in essere da un soggetto e che arreca danno ad un altro soggetto. Il fatto illecito è fonte dell'obbligo di risarcire il danno così causato (ad esempio, se X travolge in auto Y, il fatto illecito costituito dall'averlo travolto obbliga X a risarcire a Y il danno subito per effetto di tale evento).

Mentre dal contratto possono derivare obbligazioni di natura diversa a seconda dell'oggetto del contratto, l'obbligazione che deriva dal fatto illecito è di un solo tipo, ossia quella di risarcire il danno che il fatto illecito ha arrecato. Si tratta, dunque, di una specifica ipotesi di obbligazione (risarcitoria) che sorge tra privati per effetto di un semplice comportamento che uno di essi ha posto in essere, anche senza che tra di essi esista un contratto (responsabilità detta, per questo motivo, extracontrattuale).

La principale norma in materia di responsabilità extracontrattuale è quella (art. 2043 c.c.) secondo la quale "*qualunque fatto doloso o colposo che cagiona ad altri un danno ingiusto obbliga colui che ha commesso il fatto a risarcire il danno*".

Gli elementi necessari che devono sussistere perché vi sia questo tipo di responsabilità sono, dunque, i seguenti:

- fatto illecito, ossia un'azione "contraria al diritto" posta in essere da qualcuno;
- dolo o colpa di colui che pone in essere il fatto illecito, il quale, dunque, deve avere agito allo scopo specifico di cagionare il danno causato (dolo) oppure avere agito in modo negligente, trascurato e non accorto (colpa)[5];

[5] Per vero vi sono anche ipotesi in cui chi pone in essere un determinato comportamento che cagiona un danno ne risponde anche in assenza di sua colpa o di suo dolo.

- danno, ossia conseguenze negative che il fatto posto in essere da un determinato soggetto ha causato ad un altro soggetto;
- nesso di causalità tra fatto e danno, in base al quale il danno deve essere conseguenza del fatto posto in essere dal responsabile.

Esistono, poi, specifiche tipologie di responsabilità extracontrattuale (ad esempio, responsabilità per attività pericolosa, responsabilità da conduzione di veicoli, responsabilità per danni causati da cosa in custodia, responsabilità da animali in custodia, ecc.).

Il **risarcimento del danno** è finalizzato, in termini semplici, ad eliminare le conseguenze negative che un determinato fatto illecito ha causato. Spesso il risarcimento del danno è ottenuto mediante la corresponsione di una somma di denaro a titolo risarcitorio: il danno patito viene, così, stimato in termini monetari e colui che con il proprio comportamento lo ha causato è tenuto a versare la corrispondente somma a chi il danno ha subito[6].

Il risarcimento del danno non comprende solo la liquidazione delle perdite economiche (o economicamente rilevanti) subite per effetto della condotta del danneggiante, ma anche altre tipologie di pregiudizi patiti, afferenti a beni non economicamente rilevanti. Il risarcimento del danno comprende, dunque:

- il danno patrimoniale, ossia quello che si concretizza nella lesione di interessi economici del danneggiato, del patrimonio inteso in senso strettamente economico. Esempi di danno patrimoniale sono, fra gli altri, il valore di un bene che dovesse essere distrutto, il mancato guadagno derivante dalla mancata disponibilità di un bene, ecc.

  Ad esempio, se X ruba l'auto ad Y e nella fuga l'auto viene distrutta, X potrebbe dover risarcire a Y sia il valore dell'automobile, sia lo stipendio perso da Y che, a causa della mancata disponibilità della vettura, non ha potuto andare a lavoro per un numero n di giorni.
- il danno non patrimoniale, ossia quello che si concretizza nella lesione di interessi della persona non connotati da rilevanza economica. Esempi di danno non patrimoniale sono:
  - il danno biologico (ossia il danno alla salute, la lesione della integrità psico-fisica della persona, intesa in senso lato, anche agli aspetti "psicologici" della persona stessa);
  - il danno morale (ossia la sofferenza soggettiva che il fatto illecito ha causato al danneggiato);
  - il danno all'immagine (ossia alla reputazione personale e professionale di un determinato soggetto).
  - il danno esistenziale (ossia la compromissione delle varie attività nelle quali si esplica la vita umana; ad esempio, l'impossibilità di praticare sport,

[6] Si parla, in questo caso, di risarcimento "per equivalente". Un altro, più raro, tipo di risarcimento è quello "in forma specifica", mediante il quale colui che ha cagionato il danno è tenuto, ove materialmente possibile, a ripristinare la situazione esistente prima che si venisse a causare il danno (ad esempio, se X travolge con la propria auto la recinzione della casa di Y e la danneggia, X potrebbe essere condannato a ricostruire a proprie spese la recinzione).

l'impossibilità di avere una vita sessuale, l'impossibilità di avere una vita relazionale, ecc.).

Nel liquidare il danno non patrimoniale (ossia nel determinare l'importo del risarcimento che il danneggiante dovrà corrispondere al danneggiato) il giudice applica criteri equitativi, ossia criteri che gli consentono di tradurre in termini economici un danno "immateriale" quale quello non patrimoniale.

La responsabilità da prodotto

Una specifica tipologia di responsabilità extracontrattuale è la responsabilità da prodotto difettoso. Si tratta della responsabilità prevista dall'ordinamento (con norma di derivazione UE) in capo al produttore di un determinato bene di consumo che si riveli difettoso e che, a causa di tale difetto, causi un danno al consumatore che lo utilizza. Il produttore deve, pertanto, risarcire il danno che il suo prodotto difettoso ha causato.

Perché vi sia responsabilità da prodotto, il danneggiato deve dimostrare:

- il difetto del prodotto;
- il danno subito;
- il nesso di causalità tra difetto e danno (quindi non tra il semplice utilizzo del prodotto ed il danno subito, ma tra il difetto del prodotto ed il danno).

Quindi perché vi sia questa ipotesi di responsabilità non occorre dimostrare il dolo o la colpa del produttore. Il mero fatto che un prodotto abbia un difetto espone il suo produttore all'obbligo risarcitorio anche in assenza di sua colpa.

Per "consumatore" si intende il soggetto che non utilizza il prodotto in una attività industriale, imprenditoriale o professionale, ma per uso "personale" in senso lato. Ad esempio, un soggetto che utilizzi un pc per uso personale (a casa propria, per svago o per semplici ricerche su internet o per giocare a videogames) è un consumatore e dunque ha diritto ad essere risarcito se difetti del pc causano un danno (ad esempio, il pc è difettoso e gli trasmette una scarica elettrica). Un soggetto che usi lo stesso pc nella propria attività d'impresa non può essere risarcito secondo la normativa in materia di responsabilità da prodotto, ma secondo le norme generali.

Se ad essere difettoso è un componente del prodotto e il danno deriva dal difetto di quello specifico componente, rispondono nei confronti del consumatore sia il produttore del prodotto finito, sia il produttore del componente difettoso.

Il software è un prodotto…? Il "prodotto", secondo la norma, è ogni bene mobile, anche se incorporato in un altro bene mobile o immobile. Il software può rientrare in questa definizione di "prodotto"?

DATI, PRIVACY E DATA PROTECTION

Diritto alla privacy e diritto alla protezione dei dati

"I dati ridefiniranno il nostro modo di produrre, consumare e vivere" (Commissione Europea, 2020). I dati rappresentano un asset essenziale e la loro circolazione è considerata come il motore della *data-driven innovation*, tanto da essere considerata dall'Unione una "libertà fondamentale tra i pilastri portanti del mercato unico europeo".

L'esigenza di regolare il diritto alla privacy e ad un corretto trattamento dei propri dati personali nasce con l'avvento e la diffusione delle tecnologie informatiche e telematiche e il loro impiego nel trattamento dei dati, posto che nel contesto digitalizzato il controllo sulla circolazione delle informazioni non poteva essere più svolto unicamente dall'interessato al quale i dati pertengono. La risposta del legislatore è stata quella di introdurre dei meccanismi che consentissero ai titolari dei dati di acconsentire o meno, a monte, all'immissione ed alla circolazione delle informazioni a loro riferite. Il consenso è, dunque, l'elemento fondamentale che governa il trattamento dei dati personali.

→ Nasce così il diritto alla protezione dei dati (**data protection**), in base al quale il titolare delle informazioni può limitare la circolazione dei propri dati, spostando la responsabilità sul soggetto al quale l'interessato ha ceduto l'informazione stessa, ossia il titolare del trattamento dei dati. Sulla base di tale diritto è stata, poi, sia a livello nazionale che a livello UE, coniata una articolata normativa che disciplina a quali condizioni, per quali finalità e secondo quali procedure i dati personali possono essere trattati.

Occorre, dunque, distinguere tra diritto alla privacy e diritto alla protezione dei dati, ossia due concetti che, nonostante vengano spesso sovrapposti, sono in realtà distinti:

- il diritto alla privacy è, in generale, il diritto alla riservatezza, ossia ad impedire interferenze nella propria vita privata, il diritto a mantenere la sfera della propria vita privata ed intima al riparo dagli altri (diritto ricavabile dalla interpretazione di articoli della Costituzione, quali quello alla inviolabilità della persona, e che deve essere controbilanciato rispetto ad altri interessi, quali l'interesse della società a conoscere determinate notizie o altre esigenze pubbliche);
- il diritto alla protezione dei dati è, invece, il diritto dell'interessato a controllare (ossia conoscere ed anche limitare) la circolazione di informazioni (dati) riguardanti la propria persona.

La normativa in materia di data protection disciplina, dunque, più specificamente, il rapporto tra due soggetti quanto al trattamento dei dati:

- l'**interessato** (il **data subject**), ossia la persona alla quale si riferiscono i dati;
- il **titolare del trattamento** (il **data controller**), ossia la persona (ivi incluse le autorità pubbliche) al quale l'interessato cede i dati e che stabilisce le finalità ed i mezzi del trattamento. È dunque colui che decide, in ultima istanza, come e perché trattare i dati dell'interessato.

Cos'è un "dato personale"? È qualsiasi elemento informativo (rappresentativo di una informazione) che sia in grado di essere riferita ad una determinata persona fisica e consenta, anche in combinazione ad altri elementi, di individuare il soggetto al quale tale informazione è riferibile. Non è, dunque, necessario che il dato sia affiancato dal

nome e cognome della persona al quale si riferisce, ma è sufficiente che l'interessato possa essere individuato all'interno di una categoria, anche da poche persone. Esempi di dati personali possono essere i seguenti:

- nome e cognome;
- dati relativi all'ubicazione;
- identificativo online;
- elementi relativi all'identità fisica;
- elementi relativi alla identità psichica, economica, culturale o sociale, ecc.

Spesso i termini "dato" ed "informazione" vengono usati come sinonimi, ma dal punto di vista informatico (ed anche giuridico) non è corretto. Infatti:

- un "dato" è una rappresentazione oggettiva, "grezza" e non interpretata della realtà, ossia ciò che è immediatamente percepito dall'esterno in relazione ad una persona senza alcuna particolare elaborazione;
- una "informazione" è una visione della realtà derivante dalla elaborazione e della interpretazione dei dati grezzi, ossia il significato che viene associato ai dati. L'informazione è, dunque, il risultato di una elaborazione di dati.

Il dato è, quindi, un elemento rappresentativo di una informazione. Potremmo, in termini molto semplici e riduttivi, dire che esiste un "primo livello", ossia il dato, ed un "secondo livello", un livello ulteriore che deriva dal dato, e che è, per l'appunto, l'informazione. Si parte da dati conosciuti per arrivare ad un risultato che precedentemente non era conosciuto (per "imparare qualcosa di qualcuno", potremmo dire), ossia l'informazione. Questo è fondamentale per comprendere i meccanismi di marketing (anche neuro-marketing) ed il funzionamento delle piattaforme, ad esempio (così come la normativa applicabile).

Le questioni di data protection si intrecciano, poi, con esigenze di sicurezza informatica dei dati (**data security**), da garantire attraverso lo sviluppo di sistemi gestionali il più sicuri possibile, specialmente con riferimento alla conservazione di dati nel cloud.

Dati personali vs. Big data. Il valore economico del dato come "oggetto di scambio"

La attuale normativa in materia di data protection (o comunque quella che sarà oggetto di studio) è relativa alla protezione dei soli dati personali.

Dati personali vs. Big data: i "big data" sono grandi volumi di dati, acquisiti principalmente in rete ed elaborati dall'Intelligenza Artificiale per trarne correlazioni e, dunque, nuove informazioni anche molto preziose. L'applicazione classica è quella della profilazione, che acquista dimensioni sempre più estese, tanto che si inizia a parlare addirittura di "privacy di gruppo" (group privacy).

Si tratta di dati di natura diversa, anche non necessariamente personali, anche in quanto potenzialmente anonimi. Ora, abbiamo detto che un dato per essere "dato personale" deve essere riconducibile, direttamente o indirettamente, ad una determinata persona, pertanto teoricamente un dato anonimo non è un dato personale, e dunque teoricamente la normativa in materia di data protection non potrebbe trovare applicazione. Ma, anche grazie all'analisi dei big data ed all'Intelligenza Artificiale,

potrebbe essere semplice "assegnare nome e cognome" ad un determinato dato inizialmente anonimo, e che dunque cesserebbe di essere tale. Cosa succede in tale caso quanto alla normativa applicabile?

Altra rilevante questione attiene al **valore economico del dato**.

È ormai principio assodato per il diritto quello secondo il quale i dati hanno un valore economicamente apprezzabile e, dunque, possono rilevare come "corrispettivo", come "prezzo" di un determinato servizio. Non è, dunque, corretto affermare, ad esempio, che i servizi di social network sono gratuiti, perché per il diritto "gratuito" è un prodotto o un servizio che viene fornito senza che chi lo fornisce riceva alcun tipo di corrispettivo (non necessariamente una somma di denaro, ma qualsiasi tipo di bene suscettibile di avere un valore economico, e dunque anche il dato)[1].

Il GDPR: elementi fondamentali della disciplina

Principale riferimento normativo in materia è oggi costituito dal Regolamento (UE) 2016/679 "*relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali, nonché alla libera circolazione di tali dati*", ossia il **Regolamento Generale sulla Protezione dei Dati (GDPR)**.

Alla luce del GDPR l'Italia ha poi modificato, nel 2018, il proprio precedente Codice della privacy (D.Lgs. n. 196/2003) per adeguarsi alle innovazioni portate dalla nuova norma, mediante il D.Lgs. n. 101/2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679). Il principale punto di riferimento resta, comunque, il GDPR, che è direttamente applicabile, mentre la normativa di fonte italiana assume rilievo di norme di contorno e completamento.

Gran parte delle norme previste dal GDPR si incentrano essenzialmente su un criterio di **gestione del rischio (risk management)**, che, come vedremo, impernia non soltanto la normativa in materia di data protection, ma anche gran parte delle vigenti e future regole in materia di "nuove tecnologie" (Intelligenza Artificiale, piattaforme, ecc.). Il principio consiste, in termini estremamente semplici, nell'obbligo di parametrare doveri e misure di sicurezza al rischio concreto connesso ad una determinata attività.

Qual è l'ambito applicativo del GDPR? In altri termini, a quali circostanze si applica il GDPR? In sintesi:

- il Regolamento tutela esclusivamente le persone fisiche, e non anche quelle giuridiche. Più in dettaglio, il GDPR:
    - tutela il diritto alla protezione del dato solo delle persone fisiche (in altri termini, l'interessato ai fini del GDPR può essere unicamente una persona fisica, e mai una persona giuridica); ma
    - impone obblighi e doveri (e sanzioni) sia alle persone fisiche che alle persone giuridiche, laddove esse trattino dati personali riferiti alle persone fisiche;

[1] Ad esempio, è stata accertato che il servizio di social network fornito da Facebook non può dirsi "gratuito" per il diritto, ed è stato dunque ordinato a Facebook di non utilizzare il claim che precedentemente poteva essere letto da tutti gli utenti nella pagina del sito utilizzata per il login, ossia "Iscriviti. È gratis e lo sarà sempre". Questo perché Facebook riceve dagli utenti un gran numero di dati che vengono utilizzati, ad esempio, a fini di marketing e profilazione, quindi Facebook riceve un corrispettivo. Il "prezzo" del servizio reso da Facebook sono i dati degli utenti.

- si applica a tutti i trattamenti elettronici, cartacei e manuali di dati personali;
- per "trattamento di dati personali" si intende qualunque operazione che abbia ad oggetto uno o più dati personali (raccolta, registrazione, organizzazione, conservazione, estrazione, consultazione, uso, comunicazione, diffusione, cancellazione, ecc.) Dunque, qualsiasi attività venga svolta con dati personali rientra nell'applicazione del GDPR.

  A tal fine non rileva che il dato sia raccolto o estratto da chi pone in essere l'attività. Anche la semplice conservazione di dati raccolti da altri, o la loro mera consultazione, o la comunicazione a soggetti terzi di dati raccolti da altri costituiscono "trattamento" ai fini dell'applicazione del GDPR. Lo stesso vale anche per la cancellazione o la distruzione di dati, anche laddove questi siano stati raccolti da soggetti diversi da chi poi li cancella o li distrugge;
- ha efficacia anche extraterritoriale, nel senso che si applica:
  - a tutti i trattamenti di dati effettuati da chiunque abbia sede nel territorio dell'Unione Europea, indipendentemente dal luogo in cui avviene il trattamento (indipendentemente, dunque, dal fatto che il trattamento sia materialmente effettuato o meno nell'Unione Europea, quindi anche al caso di imprese con sede nell'Unione Europea ma che svolgano attività unicamente in territori extra-UE);
  - a tutti i trattamenti svolti all'estero (fuori dall'UE) se e quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi a interessati che si trovano, anche "virtualmente", nell'Unione Europea (indipendentemente, quindi, dalla cittadinanza o dal titolo della permanenza degli interessati nell'Unione, che potrebbe essere anche solo temporanea);
- non si applica ai trattamenti posti in essere da persone fisiche per l'esercizio di attività a carattere esclusivamente personale o domestico (è la c.d. "*household exemption*").

I "protagonisti" del trattamento di dati personali

Quali sono gli "attori" del trattamento dei dati personali? In altri termini, quali sono i soggetti che il GDPR prende in considerazione per disciplinare come devono essere trattati i dati personali? Essi sono, in sintesi:

- l'interessato (il data subject), ossia la persona fisica alla quale si riferiscono i dati (la persona fisica, dunque, in relazione alla quale il dato veicola informazioni);
- il titolare del trattamento (il data controller), ossia la persona fisica o giuridica (ivi incluse le autorità pubbliche) che, singolarmente o insieme ad altri, determina le finalità, le modalità ed i mezzi del trattamento di dati personali dell'interessato e (spesso) pone in essere il trattamento.

  N.B.: nel caso di persona giuridica (società, ente, autorità pubblica, ecc.) il titolare è l'entità nel suo complesso e non le persone fisiche che "lavorano" per quell'entità (dipendente che materialmente compie attività sul dato, l'amministratore delegato, il dirigente responsabile, ecc.).

Per un determinato trattamento vi può essere anche più di un titolare. In questo caso si parla di "contitolari del trattamento", ossia due o più soggetti che stabiliscono insieme le finalità e le modalità del trattamento mediante un accordo interno tra loro. La presenza di più titolari del trattamento deve essere resa nota all'interessato. Ad esempio, si pensi al caso in cui un cliente affida un mandato difensivo a due avvocati invece che ad uno solo: in questo caso entrambi gli avvocati sono titolari, a pari titolo, del trattamento dei dati del cliente;

- il responsabile del trattamento (il data processor), ossia la persona fisica o giuridica (ivi incluse le autorità pubbliche) che tratta dati personali per conto del titolare del trattamento. È il soggetto (o i soggetti) che il titolare del trattamento eventualmente incarica di trattare i dati secondo le proprie istruzioni. Il titolare può anche direttamente trattare i dati, senza nominare alcun responsabile del trattamento, ma, se nomina un responsabile, il titolare ha poi il dovere di vigilare sull'osservanza delle proprie istruzioni da parte del responsabile.

  Ad esempio, si pensi ad una compagnia telefonica che incarichi una specifica agenzia di porre in essere attività di call center e marketing in una determinata zona e per un bacino di utenza individuato dalla compagnia telefonica stessa: in questo caso, la compagnia telefonica è il titolare del trattamento, mentre l'agenzia è il responsabile del trattamento;

- il soggetto autorizzato, ossia la persona fisica che il titolare o il responsabile del trattamento devono espressamente individuare all'interno della propria organizzazione e che materialmente compie le operazioni del trattamento (che può, naturalmente, essere solo una persona fisica). Si tratta di un soggetto che deve essere istruito e formato sulle modalità per lo svolgimento dell'attività;

- il Data Privacy Officer (DPO), ossia una persona fisica che deve essere designata dal titolare in caso vengano posti in essere trattamenti particolarmente "sensibili" o "complessi". In particolare, il DPO deve essere designato se:

  - il trattamento è effettuato da una pubblica amministrazione;
  - il trattamento richiede un monitoraggio regolare e sistematico degli interessati su larga scala;
  - il trattamento è effettuato su larga scala su dati sensibili (compresi i dati genetici e biometrici) e/o dati giudiziari.

  Il DPO deve avere una posizione di indipendenza rispetto al titolare. La sua funzione è quella di inserire nell'organizzazione del titolare un soggetto qualificato che gli fornisca consulenza in merito agli obblighi derivanti dalla normativa in materia di data protection, che vigili sull'osservanza di tale normativa, che ponga in essere attività di sensibilizzazione e formazione del personale e che eventualmente cooperi con il Garante per la Protezione dei Dati Personali.

  L'identità ed i contatti del DPO devono essere resi noti agli interessati.

In Italia esiste una autorità pubblica indipendente alla quale è attribuito il compito di sorvegliare sull'applicazione della normativa in materia di trattamento di dati personali al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche. Si tratta del **Garante per la protezione dei dati personali** (GPDP, comunemente noto come "Garante per la privacy", anche se tale nome non è rigorosamente corretto).

I principi fondamentali del trattamento dei dati personali

Il trattamento dei dati personali è consentito solo qualora sia necessario per adempiere alle finalità per le quali i dati sono stati raccolti, nei limiti dei dati necessari per gli scopi della raccolta e delle operazioni strettamente indispensabili per gli scopi stessi. I dati personali devono essere "*trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*" (art. 5 GDPR).

Il titolare del trattamento deve mettere in atto (ed essere in grado di dimostrare di avere messo in atto) misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente al GDPR.

Secondo il GDPR il trattamento di dati personali deve essere effettuato nel rispetto dei seguenti principi:

- **liceità**: occorre rispettare tutte le norme dell'ordinamento giuridico, non solo il GDPR e comunque quelle in materia di data protection;
- **trasparenza**: l'interessato deve sapere che i suoi dati sono oggetto di un trattamento, e quali dati lo sono;
- **limitazione delle finalità**: i dati oggetto di trattamento devono essere raccolti per finalità determinate ed esplicite (ossia comunicate chiaramente all'interessato) e successivamente trattati in conformità a tali finalità (ossia per gli scopi per i quali sono raccolti, e non per altri)[2];
- **esattezza dei dati**: i dati oggetto di trattamento devono essere esatti e, se necessario, aggiornati. Devono, dunque, essere adottate tutte le misure ragionevolmente esigibili per cancellare o rettificare tempestivamente dati che risultino inesatti rispetto alle finalità del trattamento;
- **minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto necessario per gli scopi del trattamento e non devono, dunque, eccedere rispetto alle finalità per cui sono raccolti o sono successivamente trattati;
- **limitazione della conservazione**: i dati devono essere conservati per un arco di tempo non superiore al conseguimento degli scopi per i quali sono trattati. Una volta raggiunto lo scopo del trattamento, i dati devono essere resi anonimi o cancellati.

Questi principi devono essere rispettati di default, sin dall'inizio della progettazione dell'attività in questione, prevedendo tutte le garanzie indispensabili al fine di tutelare i diritti degli interessati. Si parla, infatti, del principio della **privacy by default**, che prevede che le impostazioni di tutela della vita privata relative ai servizi e prodotti rispettino i principi generali della protezione dei dati, quali, per l'appunto, la minimizzazione dei dati e la limitazione delle finalità. Gli applicativi informatici devono, dunque, essere progettati a monte per rispettare tali principi, prima di procedere al trattamento dei dati vero e proprio.

Quanto al trasferimento dei dati all'estero (ossia, ai fini del GDPR, a soggetti situati al di fuori dell'Unione Europea), in termini generali il trasferimento è di base vietato qualora

[2] Unica eccezione considerata dal GDPR è quella dell'eventuale trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, che il GDPR considera comunque sempre compatibili con gli scopi originari del trattamento.

la legislazione del paese di destinazione non assicuri un livello di tutela adeguato (valutazione, questa, che spetta alla Commissione Europea). In caso contrario, il trasferimento verso paesi terzi può avvenire solo nel rispetto di alcune garanzie previste dal GDPR. Questo per evitare che venga aggirata la normativa di tutela prevista dal GDPR acquisendo dati in Europa e trattandoli, poi, all'estero, in paesi che non prevedano le garanzie contemplate dalla normativa UE.

Le basi giuridiche del trattamento

Il trattamento dei dati, secondo il GDPR, è lecito solo se viene svolto in presenza di una condizione che lo legittima, ossia di una base giuridica.

Le possibili basi giuridiche che legittimano il trattamento sono le seguenti:

a. il **consenso dell'interessato**, che deve essere prestato liberamente ed essere effettivo. In relazione a ciò:
    - occorre domandarsi quando possa essere definito "effettivo" e "libero" il consenso, anche in relazione alla comprensibilità delle informazioni che il titolare rende all'interessato per chiedergli il consenso (ossia l'informativa, v. sotto). Sicuramente non è libero, e dunque valido, il consenso ottenuto con violenza o minaccia o inducendo l'interessato in errore[3];
    - il consenso può essere prestato in qualunque forma, scritta od orale, fermo restando che il titolare del trattamento deve comunque essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento (il che può essere più complesso in presenza di un consenso non scritto);
b. il caso in cui il trattamento occorra per adempiere ad **obblighi legali**;
c. il caso in cui il trattamento sia **necessario per l'esecuzione di obblighi di un contratto del quale è parte l'interessato** (ossia nel caso in cui il soggetto X non possa eseguire un contratto che ha sottoscritto con Y se non trattando dei dati relativi ad Y);
d. il caso in cui il trattamento sia necessario per **perseguire un legittimo interesse del titolare del trattamento o di terzi**, ove si tratti di un interesse che, nel bilanciamento con quello alla protezione dei dati, prevalga su quest'ultimo;
e. il caso in cui il trattamento sia **necessario per l'interesse pubblico** (ad esempio, qualora il trattamento sia effettuato dalla Pubblica Amministrazione, ma solo nei limiti in cui il trattamento serva all'adempimento dei fini istituzionali dell'ente).

Nei casi di cui ai punti b., c. e d. di cui sopra, e solo in tali casi, il trattamento dei dati è legittimo anche senza il consenso dell'interessato, che costituisce, al di là di tali ipotesi, la regola generale in materia di data protection.

I dati "particolari"

Il GDPR disciplina in modo parzialmente differente, con ulteriori cautele, due categorie di dati ritenuti "particolari", ossia:

[3] L'età alla quale può essere validamente prestato il consenso è "abbassata" dall'UE a 16 anni (14 anni per l'Italia).

- **dati sensibili**: sono i dati suscettibili di rivelare l'origine etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale dell'interessato o comunque dati genetici, biometrici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona. Sono dati il cui trattamento può essere particolarmente lesivo dei diritti e delle libertà fondamentali dell'interessato, in quanto potenzialmente fonte di discriminazioni.

  Tali dati non possono essere oggetto di trattamento a meno che:

  - non vi sia il consenso esplicito dell'interessato per una o più finalità specifiche;
  - tali dati non siano stati resi manifestamente pubblici dall'interessato (il quale perde, dunque, in tal caso l'interesse al mantenimento del segreto);
  - il loro trattamento non serva per tutelare la salute di terzi;
  - il loro trattamento non serva per altre ipotesi (la gestione del rapporto di lavoro, finalità archivistiche, ecc.);
- **dati giudiziari**: sono i dati relativi alle condanne penali ed ai reati, per il cui trattamento valgono le basi giuridiche di cui sopra, ma subordinatamente al controllo dell'autorità pubblica e nei casi previsti dalla legge.

Gli adempimenti previsti in capo al titolare (o al responsabile)

I. Le misure di sicurezza

Il GDPR impone al titolare ed al responsabile di mettere in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio. Sono imposte, dunque, forme di tutela preventiva per evitare la lesione dei diritti tutelati dalla normativa.

Il principio-base è quello della gestione del rischio (risk management), in base al quale:

- occorre individuare quali sono i rischi specifici e concreti che una determinata attività o trattamento pone (ad esempio, perdita di dati, accesso ai dati da parte di soggetti non autorizzati, ecc.) e quali conseguenze possano derivarne per l'interessato (da modulare, naturalmente, in relazione alla tipologia di dati dei quali si tratta);
- individuare e porre in essere, sulla base della ricognizione di cui al precedente punto e tenendo conto dello stato dell'arte e dei costi di attuazione, le misure specificamente utili a scongiurare quegli specifici rischi, con un approccio, potremmo dire, tailormade rispetto al rischio.

Non può esistere, dunque, una "one-size-fits-all solution" e misure di sicurezza standard applicabili per tutti i casi, ma l'approccio che la normativa esige è di tipo concreto e specifico. Nella scelta delle misure tecniche ed organizzative occorre, poi, effettuare un bilanciamento tenendo conto anche della proporzionalità rispetto ai costi delle misure stesse (non è obbligatorio porre in essere soluzioni tecnologicamente avanzate ove le stesse risultino, in concreto, economicamente troppo onerose rispetto al business del titolare e, soprattutto, ai concreti rischi connessi alla sua attività).

A tal fine, è indispensabile che venga condotta una valutazione preventiva d'impatto sulla protezione dei dati, ossia il cosiddetto **Data Protection Impact Assessment**

(DPIA), volto a ponderare ex ante l'incidenza che una determinata soluzione tecnica potrà avere sulla tutela dei dati trattati, analizzando i vari possibili casi in ragione delle specificità correlate alle modalità di gestione delle informazioni. Il DPIA:

- si colloca, in primo luogo, in una fase preliminare dello sviluppo del prodotto o del servizio, ovvero quando il suo design non è delineato in maniera definitiva, bensì è ancora in uno stadio progettuale;
- deve essere ripetuto prima dell'attivazione del trattamento;
- deve essere effettuato anche successivamente con cadenza periodica.

Il DPIA può essere effettuato sempre, ma diventa obbligatorio se il rischio connesso al tema della protezione dei dati è elevato in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, specialmente in caso di utilizzo di nuove tecnologie (ad esempio, in caso di trattamento automatizzato; cfr. art. 22 GDPR), oppure quando si effettuano trattamenti di dati "particolari" (v. sopra), oppure quando il trattamento comporta la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Abbiamo già parlato sopra del principio della **privacy by default**, che deve guidare il titolare nell'approntare le misure di sicurezza idonee, che "di default" devono rispettare i principi che abbiamo già esaminato sopra.

Altro principio generale del GDPR, che si accompagna a quello di privacy by default, è quello detto della "**privacy by design**", da molti interpretato come il futuro della legislazione in materia di data protection (ma in realtà il principio del "by design" ispirerà probabilmente molta parte della legislazione delle nuove tecnologie ed in particolar modo dell'Intelligenza Artificiale, facendo della tecnologia il veicolo per garantire ex ante, a monte, il rispetto delle regole).

Si tratta di un principio secondo il quale la tutela dei dati personali deve essere incorporata a partire dalla progettazione di ogni processo aziendale (deve essere, in altri termini, uno dei presupposti sulla base dei quali si devono predisporre i processi aziendali, embedded ed incorporato "nel suo DNA", potremmo dire), anche e soprattutto nel ricorso alle relative applicazioni informatiche di supporto.

Si parla, ad esempio, della messa in atto, già nella progettazione dei sistemi informatici, di determinati meccanismi volti garantire che il sistema, a priori, non tratti dati personali per scopi diversi rispetto a quelli programmati, con apposite "barriere" e "blocchi". L'esigenza di protezione dei dati deve, dunque, essere considerata già nella fase di progettazione, e non solo a posteriori. In termini semplici: non posso progettare un determinato sistema e solo dopo chiedermi se quest'ultimo tuteli i dati personali degli interessati, ma devo pormi questa domanda prima, nel momento in cui inizio a progettare il sistema stesso.

Il principio della privacy by design richiede che la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali comporti l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione che dell'esecuzione del trattamento stesso, nell'intero ciclo di vita della tecnologia.

Ad esempio, a seconda dei casi le misure di sicurezza adeguate devono prevedere:

- la pseudonimizzazione e la cifratura dei dati personali;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- la capacità di assicurare la resilienza dei sistemi e dei servizi di trattamento (anche in termini di cybersecurity);
- una procedura di testing periodico per valutare regolarmente l'efficacia concreta delle misure adottate.

II. La predisposizione dell'informativa da fornire all'interessato

Prima della raccolta dei dati o al momento della raccolta il titolare deve fornire all'interessato la cosiddetta "informativa", finalizzata a consentirgli di esprimere un consenso al trattamento effettivamente informato.

L'informativa può essere fornita per iscritto, oralmente o con altri mezzi, ma occorre sempre tenere in considerazione, nella scelta della modalità con la quale rendere l'informativa, che il titolare potrebbe essere chiamato a dimostrare di avere reso l'informativa all'interessato (nel qual caso, un'informativa resa per iscritto agevolerebbe sicuramente l'adempimento a tale onere probatorio). Comunque l'informativa può essere resa oralmente solo se richiesto dall'interessato.

L'informativa deve:

- recare tutte le informazioni utili ad identificare il trattamento (modalità, finalità, durata e base giuridica del trattamento);
- essere concisa, trasparente e comprensibile, con un linguaggio semplice e chiaro;
- informare sulla natura del conferimento dei dati, ossia deve specificare se il conferimento dei dati da parte del titolare è facoltativo od obbligatorio in relazione a determinate finalità. Quindi occorre anche informare sulle eventuali conseguenze del rifiuto di conferire dati (ad esempio, l'impossibilità di eseguire un determinato servizio in assenza di conferimento di dati);
- indicare i dati, inclusi i contatti, del titolare e dell'eventuale responsabile;
- informare sui soggetti ai quali i dati potranno essere comunicati e sull'eventuale trasferimento all'estero (fuori dall'UE) degli stessi;
- informare sui diritti previsti dal GDPR per l'interessato (accesso, rettifica, cancellazione, portabilità, limitazione, opposizione; v. infra, pag. 13);
- informare sulla possibilità di revocare il consenso;
- informare sulla possibilità di proporre reclamo all'autorità di controllo (il Garante per la Protezione dei Dati Personali, il quale può adottare sanzioni nei confronti di chi viola la normativa in materia di data protection ed ingiungere di modificare il proprio comportamento).

Se i dati vengono acquisiti da soggetti diversi dall'interessato, non potendosi fornire l'informativa all'interessato stesso al momento dell'acquisizione, l'informativa deve essere fornita alla persona che fornisce i dati per poi comunicarla anche all'interessato entro un mese dall'ottenimento dei dati (cosiddetta informativa postuma).

III. La nomina del DPO (v. sopra)

IV. La tenuta del Registro delle attività di trattamento

Talune tipologie di titolari del trattamento devono tenere un **Registro delle attività di trattamento**, ossia un registro nel quale tenere traccia di tutti i trattamenti svolti presso il titolare. A tale obbligo sono tenuti:

- i titolari che abbiano oltre 250 dipendenti;
- i titolari che, pur avendo meno di 250 dipendenti, effettuano trattamenti:
    - che possano presentare rischi per i diritti e le libertà degli interessati; oppure
    - che non siano occasionali; oppure
    - che includano dati di natura particolare.

Il Registro può essere conservato anche solo in formato elettronico e deve contenere, tra l'altro, le seguenti indicazioni:

- finalità del trattamento;
- descrizione delle categorie di interessati e delle categorie di dati personali trattati;
- categorie di destinatari ai quali i dati saranno eventualmente comunicati;
- eventuali trasferimenti di dati verso paesi non UE;
- descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

V. La segnalazione all'autorità di controllo in caso di data breach

Il titolare è obbligato a notificare all'autorità di controllo e, nei casi più rilevanti, ai diretti interessati le violazioni dei dati personali dell'interessato dovute a violazioni dei propri sistemi informatici. La notifica deve essere effettuata senza ritardo e, comunque, entro 72 ore dal momento in cui il titolare è venuto a conoscenza del data breach.

La notifica non è obbligatoria sempre, ma la sua effettuazione è subordinata alla **valutazione del rischio per gli interessati**, che spetta al titolare, il quale la effettua sotto la propria responsabilità.

I trattamenti interamente automatizzati (e la profilazione)

Il GDPR prevede il diritto dell'interessato di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, laddove la decisione in questione produca effetti giuridici che lo riguardano o incida in modo significativo sulla sua persona (**art. 22 del GDPR**).

È un trattamento automatizzato di dati anche la cosiddetta **profilazione**. Per "profilazione" si intende l'insieme di attività di raccolta ed elaborazione automatizzata di dati inerenti alle persone fisiche che utilizzano un certo servizio al fine di suddividerli in gruppi a seconda del loro comportamento, con conseguente possibilità di adottare decisioni che li riguardano ed analizzare e prevedere le loro preferenze e i loro comportamenti futuri. In ambito commerciale, ad esempio, tale attività coincide con la definizione dei gusti e delle propensioni all'acquisto di un determinato consumatore mediante il monitoraggio delle attività che quest'ultimo compie sul web. Ciò al fine di consentire, ad esempio, offerte targettizzate o anche solo al fine di compiere indagini di

mercato o di ricerca e sviluppo, oppure di individuare su quali prodotti o settori è preferibile investire.

Sono automatizzati, fra gli altri, anche i trattamenti effettuati per l'analisi dei Big data, i quali sono analizzati ed elaborati grazie a sistemi di Intelligenza Artificiale.

L'assunzione di decisioni unicamente sulla base di un trattamento automatizzato, anche laddove comporti effetti significativi, è possibile solo in tre casi:

- se lo prevede la legge;
- se l'interessato ha dato il proprio espresso (effettivo e consapevole) consenso in tal senso (inteso come espresso, effettivo e consapevole consenso a sottoporsi al trattamento interamente automatizzato, non al trattamento in generale) → indispensabile se sono oggetto di trattamento automatizzato dati "particolari" (v. sopra);
- se è necessaria per l'esecuzione di un contratto sottoscritto dall'interessato.

In tali casi, deve comunque essere garantito il diritto dell'interessato:

- di **ottenere l'intervento umano** da parte del titolare;
- di **contestare la decisione** raggiunta mediante trattamento interamente automatizzato.

In ogni caso, l'interessato deve essere sempre informato non solo sull'esistenza del trattamento interamente automatizzato, ma anche sulle logiche e sui meccanismi mediante i quali il trattamento interamente automatizzato funziona (**diritto alla spiegazione**). L'informazione fornita deve essere **significativa** (quindi illustrativa delle caratteristiche del sistema e funzionale a garantirne la conoscibilità e la comprensibilità da parte dell'interessato)

Ma quale spiegazione è necessaria e sufficiente? In altri termini, sino a dove occorre spingersi nello spiegare all'interessato i meccanismi (talora anche molto complessi) sulla base dei quali il trattamento automatizzato è effettuato, le logiche seguite dall'algoritmo, ecc.? Quanto dettagliata deve essere l'informativa al riguardo?

Occorre anche considerare che l'informativa deve essere sempre **comprensibile** da chiunque, quindi anche da soggetti non esperti di tecnologie informatiche.

→ Esiste, dunque, l'esigenza di tenere in considerazione il **trade-off tra completezza dell'informazione resa e sua comprensibilità**.

→ La Corte di Cassazione ha recentemente (maggio 2021) affermato, con riguardo ad un caso concernente un sistema automatizzato utilizzato da una piattaforma per la definizione del rating reputazione[4], che:

- il consenso dell'interessato è fondamentale per la liceità del trattamento in questione;

[4] In particolare, il caso aveva ad oggetto un sistema informatico costituito da una piattaforma web (con annesso archivio informatico) il cui scopo era la elaborazione di profili reputazionali concernenti persone fisiche e giuridiche al fine di contrastare fenomeni basati sulla creazione di profili artefatti o "fasulli" e di calcolare, invece, in maniera imparziale il cd. "rating reputazionale" dei soggetti censiti, per modo da consentire a eventuali terzi una verifica di reale credibilità.

- il consenso dell'interessato deve essere effettivo e, a tal fine, deve essere consapevole e informato;
- di conseguenza, l'adesione ad una piattaforma da parte dell'interessato non comprendere di per sé anche l'accettazione di un sistema automatizzato che si avvale di un algoritmo per la valutazione di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati.

Il problema è, dunque, quello della **trasparenza vs. opacità dell'algoritmo** e dei processi decisionali "animati" dall'algoritmo. Il problema è particolarmente incidente per quei sistemi complessi per i quali lo stesso creatore o utilizzatore (dunque lo stesso titolare del trattamento) del sistema potrebbe avere problemi nella identificazione del processo decisionale e della motivazione sulla base della quale il sistema ha raggiunto una determinata conclusione.

Settori ed attività particolarmente interessati dalla problematica sono, ad esempio, i seguenti:

- attività di *credit scoring* (ai fini, ad esempio, del riconoscimento di un mutuo);
- attività della Pubblica Amministrazione che assuma decisioni sulla persona (provvedimenti) mediante trattamento automatizzato;
- attività giudiziaria ("sentenze robotiche");
- attività sanitarie (diagnostica).

I diritti dell'interessato

Il GDPR disciplina specifici diritti che possono essere esercitati dall'interessato in relazione al trattamento dei propri dati personali. In generale, questi diritti non sono "assoluti", ma devono essere sempre bilanciati con altri eventuali diritti del titolare del trattamento (ad esempio, l'esercizio del diritto di difesa in tribunale, oppure motivi di interesse pubblico rilevante, oppure per tutelare i diritti di un'altra persona fisica).

In particolare, tali diritti sono:

- diritto di **ottenere la conferma dell'esistenza di un trattamento di dati che lo riguardano**;
- diritto di **accedere ai dati** ed alle informazioni concernenti il trattamento (finalità, categorie di dati trattati, destinatari ai quali i dati saranno o sono stati comunicati, periodo di conservazione dei dati ed in generale le informazioni che devono essere oggetto dell'informativa);
- diritto di chiedere la **rettifica dei dati**, ossia il diritto di domandare la modifica dei dati trattati e la loro integrazione (aggiungendo dati a quelli già trattati dal titolare). Tale diritto può essere esercitato sempre in relazione alla finalità del trattamento (in altri termini, non posso ottenere la rettifica o l'integrazione dei dati se la modifica richiesta non ha nulla a che vedere con lo scopo del trattamento e non serva al miglior perseguimento di tale scopo);
- diritto di ottenere la **cancellazione dei dati**, qualora i dati non siano più necessari rispetto alla finalità del trattamento o in caso di trattamento illecito o qualora l'interessato abbia revocato il proprio consenso;

- diritto di chiedere la **limitazione del trattamento**, ossia il diritto di chiedere che i dati vengano soltanto conservati, con impossibilità di svolgere qualsiasi altra operazione mediante o in relazione ad essi;
- diritto di **opposizione**, ossia il diritto di chiedere che il trattamento venga cessato quando si tratta di trattamento svolto per finalità di marketing;
- diritto alla **portabilità dei dati**, a fronte del quale l'interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che lo riguardano ed ha diritto di trasmettere tali dati ad un altro soggetto che ne diventa il titolare del trattamento[5].

Le conseguenze di eventuali violazioni della normativa in materia di data protection

- responsabilità civile: obbligo in capo al titolare del trattamento (o al responsabile del trattamento, a seconda dei casi) di **risarcire all'interessato il danno** da quest'ultimo subito per effetto delle violazioni.

  Il risarcimento del danno viene determinato in base alle regole generali previste dal codice civile (sia danno patrimoniale che danno non patrimoniale; spesso si tratta di danno morale). L'obbligazione al risarcimento del danno sorge in qualunque caso in cui il danno subito dall'interessato sia in rapporto di causa-effetto con la violazione di una delle norme in materia di data protection.

  Per andare esente dall'obbligo di risarcimento, il titolare del trattamento deve dimostrare di avere adottato tutti gli accorgimenti previsti dalle norme in materia.

  Il trattamento di dati personali è "attività pericolosa"?

- responsabilità amministrativa: in caso di violazioni, il Garante per la protezione dei dati personali può imporre **sanzioni amministrative** in capo al titolare del trattamento.

  L'ammontare delle sanzioni, da 10 a 20 milioni di Euro, è proporzionato al fatturato mondiale annuo (2% o 4% del fatturato mondiale annuo, secondo il GDPR, a seconda della gravità della violazione e delle specifiche norme violate).

Profili di data protection online: i deepfake, le regole sui cookies, il trasferimento dei dati all'estero e il diritto alla deindicizzazione

1. Il fenomeno del deepfake

Il termine "*deepfake*", neologismo nato dalla combinazione di "*deep learning*" e "*fake*", si riferisce ad immagini, video o contenuti audio creati utilizzando tecniche di Intelligenza Artificiale (A.I.) - tra cui Generative Adversarial Networks (GANs) o Variational Auto-Encoders (VAEs) - volte a combinare, alterare, sovrapporre immagini o video originali ritraenti una persona con materiali ritraenti soggetti diversi, e dunque a simulare in modo estremamente realistico la voce, il volto, il corpo ed i movimenti di una persona. Vengono, così, generati audio, immagini o video **completamente falsi** che sono,

[5] Tale diritto può essere esercitato solo se il trattamento ha come base giuridica il consenso o l'esecuzione di un contratto e solo se i dati in questione sono oggetto di trattamento automatizzato (altrimenti l'onere imposto al titolare sarebbe eccessivo).

tuttavia, **difficilmente riconoscibili come tali**, anche ad occhio esperto (ed anche per gli stessi algoritmi impiegati per il deepfake detection).

Mediante tali sistemi, dunque, il volto di una persona può essere innestato sul corpo di un'altra, la voce di un soggetto può essere associata ad una persona diversa, i movimenti del corpo possono essere manipolati ed artefatti, le persone possono essere collocate in luoghi e contesti non reali, o comunque nei quali non si sono mai trovate, o possono sembrare pronunciare parole mai effettivamente pronunciate. I sistemi in questione possono, quindi, diventare lo strumento per la realizzazione di gravi forme di **furto d'identità** ai danni delle persone che compaiono in un prodotto deepfake, i quali subiscono una perdita di controllo non solo sulla (circolazione della) propria immagine, spesso carpita dai social network, ma anche delle proprie idee e dei propri pensieri, che possono essere oggetto di falsificazione e travisamento agli occhi di terzi; il tutto, sovente all'insaputa dell'interessato.

Accanto ad impieghi "virtuosi" delle tecnologie di deepfake (si pensi, ad esempio, in ambito sanitario, ai documentati impieghi di tali sistemi per "ridare la voce" a pazienti la cui capacità di parola era stata compromessa per effetto di malattie irrimediabilmente invalidanti; o, ancora, agli impieghi nel settore cinematografico o lato sensu artistico, oppure a fini satirici o parodistici), suscitano seria preoccupazione - anche in materia di data protection - i sempre crescenti fenomeni di applicazione di sistemi di deepfake con finalità decisamente meno edificanti ed addirittura lesive. Si pensi, ad esempio:

- al contributo che tali tecnologie forniscono ai dilaganti fenomeni di disinformazione ed alla creazione e diffusione di fake news, la cui circolazione, peraltro, è suscettibile di minare non soltanto la generale capacità del pubblico di distinguere il falso dal vero, ma anche di fidarsi di ciò che è effettivamente reale (è il fenomeno del c.d. liar's dividend);
- agli effetti che tali pratiche possono sortire in termini di distorsione dell'opinione pubblica, con immagini, audio o video deepfake suscettibili di essere mostrati od inviati agli elettori per dissuaderli dal votare un determinato candidato o per indurli a votarne uno diverso;
- all'impiego di tecnologie di deepfake per l'esecuzione di truffe mirate, ad esempio per raggirare la vittima e persuaderla a fornire dati personali o a compiere atti di disposizione patrimoniale (c.d. "spoofing"), o per aggirare sistemi di identificazione e riconoscimento facciale (il c.d. "morphing");
- all'utilizzo di tali sistemi per produrre pornografia, creando immagini e video falsi ma estremamente realistici di persone in atti sessuali, in situazioni compromettenti mai verificatesi, oppure ricostruendo in modo verosimile l'aspetto che avrebbe un determinato corpo umano sotto gli abiti, realizzando immagini di nudo adattate alla corporatura ed alle proporzioni del soggetto: è il c.d. "deepnude" (si stima che più del 95% delle applicazioni di tecnologie deepfake disponibili sul mercato sia attualmente impiegato per la produzione di varie forme di pornografia, realizzando prodotti che possono essere usati anche a finalità ricattatorie, o per screditare avversari politici). E si pensi, ancora, alle possibili ricadute su fenomeni quali il c.d. "revenge porn" o il cyberbullismo.

Non v'è dubbio che **i contenuti utilizzati per la creazione di deepfake (audio, immagini, video) possano costituire "dati personali" ai sensi del GDPR**, se ed in quanto idonei a consentire l'identificazione dei soggetti ai quali sono riferiti, e che la loro

manipolazione ad opera dei sistemi di A.I. usati per creare deepfake rappresenti un **"trattamento di dati"**[6].

Emergono due problemi principali al riguardo:

- Un primo tema concerne l'applicabilità delle regole, e delle tutele, previste dal GDPR a fattispecie quali quelle in esame, anche alla luce della c.d. "*household exemption*" prevista dal Regolamento, in virtù della quale, come si è visto, il GDPR non si applica ai trattamenti effettuati da una persona fisica "*per l'esercizio di attività a carattere esclusivamente personale o domestico*", in assenza, dunque, di "*una connessione con un'attività commerciale o professionale*".

→ Nell'interpretare l'estensione dell'ambito applicativo del GDPR, la Corte di Giustizia dell'Unione Europea tiene in considerazione, tra gli altri fattori, anche la fonte dalla quale i dati trattati vengono raccolti. Si è, ad esempio, affermato che la "*household exemption*" non può applicarsi laddove i dati personali in questione siano stati raccolti da una fonte di dominio pubblico, come i social media; e nemmeno se essi siano poi condivisi online, anche sui social media stessi. L'applicabilità dell'esenzione in parola deve, quindi, essere necessariamente valutata in considerazione delle specificità del caso concreto, ma non sembra possibile escludere a priori l'applicabilità del GDPR ai fenomeni in esame.

- Un secondo tema attiene alla individuazione di quale debba essere la sottostante base giuridica idonea a legittimare tali trattamenti di dati. Fermo restando che in ipotesi quali quelle di impiego di sistemi di deepfake per l'esecuzione di truffe o per la creazione e diffusione di deepnude nessuna base giuridica può legittimare siffatti trattamenti, nella maggior parte dei casi, l'unica base giuridica ammissibile non potrà che essere il consenso dell'interessato, mentre in altri casi ancora potrebbe valutarsi la possibilità di invocare la sussistenza di un interesse legittimo del titolare del trattamento all'utilizzo di tali dati (ad esempio, in caso di utilizzo per finalità satiriche o di critica politica); interesse, questo, in relazione al quale, tuttavia, deve sempre essere effettuata una operazione di bilanciamento con diritti ed interessi altrui, ed in particolare con i diritti dell'interessato.

Riconosciuta l'applicabilità delle norme di data protection ai casi in esame, l'interessato che veda la propria immagine e/o la propria voce utilizzata in prodotti deepfake in assenza del proprio consenso (o comunque in assenza di un legittimo interesse dell'utilizzatore ad effettuare tale trattamento) può ricorrere ai **rimedi** previsti dalla normativa, tra cui:

- il diritto ad ottenere la cancellazione dei propri dati;
- il diritto ad ottenere il risarcimento dei danni subiti.

L'esercizio di tali diritti può, tuttavia, rivelarsi, nella pratica, complesso, specialmente in considerazione delle difficoltà nel risalire al creatore dei deepfake e/o a colui che per la prima volta lo abbia messo in circolazione online. È probabile, dunque, che gli interessati rivolgano le proprie iniziative in via principale nei confronti delle piattaforme che dovessero ospitare tali contenuti, anche quali co-titolari del trattamento di dati in questione.

[6] Peraltro, è stato osservato come non soltanto i dati di input utilizzati per la creazione del deepfake possano costituire "dato personale" secondo la definizione del GDPR, ma come anche gli stessi prodotti deepfake possano diventare (veicolo di) dati personali relativi all'interessato che vi è ritratto.

Quanto ai fenomeni di **utilizzo di sistemi di deepfake a scopi di revenge porn**, ai sensi dell'**art. 612-ter del codice penale** ("*Diffusione illecita di immagini o video sessualmente espliciti*"), è punita la condotta di chi, "*dopo averli realizzati o sottratti*", "*invia, consegna, cede, pubblica o diffonde*" immagini o video a contenuto sessualmente esplicito destinati a rimanere private, senza il consenso della persona ritratta. Da più parti si dubita, tuttavia, della possibilità che la tutela offerta da tale norma possa estendersi anche alla diffusione di immagini o video non autentici, ma creati artificialmente (motivo per il quale è stata presentata una più specifica proposta di legge per punire l'impiego di sistemi quali quelli di deepfake per scopi di revenge porn; proposta che è, però, ancora all'esame del Parlamento).

Sul tema si sta muovendo anche il legislatore dell'Unione europea:

- la **proposta di Regolamento UE per un *Artificial Intelligence Act*** si limita a prevedere, allo stato, obblighi di trasparenza, e in particolare l'obbligo, in capo agli utenti di un sistema di A.I. "*che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ('deep fake')*", di rendere noto che il contenuto è stato generato o manipolato artificialmente → è un feature che deve essere aggiunto "by design" alle applicazioni di A.I. volte alla realizzazione di deepfake?;
- il ***Digital Services Act*** impone alle "*piattaforme online di dimensioni molto grandi*" che si avvedano della presenza di contenuti deepfake un obbligo di "etichettarli" come tali, "*in modo da informare in maniera chiaramente visibile per il destinatario dei servizi che si tratta di contenuti non autentici*".

2. La disciplina dei cookies

Esistono diverse tecniche utilizzate per raccogliere dati online e costituire, attraverso esse, un profilo dell'utente. Una di queste prevede l'utilizzo di **cookies**, ossia stringhe di testo che il browser colloca all'apertura di una pagina web sul terminale (computer) dell'utente e che salvano i dati dell'utente durante la visita di un sito web agevolandone l'utilizzo (ad esempio, memorizzando le preferenze linguistiche o i dati di login). I dati vengono memorizzati per essere poi ritrasmessi agli stessi siti alla visita successiva del medesimo utente.

Mediante i cookies è anche possibile monitorare la navigazione e raccogliere dati inerenti i gusti, le abitudini e le scelte personali degli utenti, consentendo così la ricostruzione di profili degli utenti medesimi anche molto dettagliati (ad esempio, permettendo la personalizzazione delle inserzioni pubblicitarie sul browser).

Anche queste modalità comportano un trattamento di dati. Ma si tratta di dati "personali"?

Generalmente un cookie contiene l'indicazione sulla sua "durata di vita" e un numero generato in modo casuale che consente il riconoscimento del computer dell'utente. Di regola, la memorizzazione dei dati dei cookies avviene in modo anonimo. Quindi potremmo non essere in presenza di "dati personali" nel senso che prevede il GDPR, che potrebbe quindi non applicarsi a queste tipologie di trattamento.

Esiste, tuttavia, una specifica normativa, di derivazione europea, che disciplina l'utilizzo dei cookies al fine di tutelare l'utente da forme di profilazione "occulta" e di consentirgli di controllare la circolazione dei dati inerenti alla propria navigazione online,

subordinando la memorizzazione di tali mediante cookies al consenso dell'utente (principio dell'opt-in).

Esistono due tipologie di cookies:

- **cookies tecnici**, ossia quelli che sono necessari per motivi, per l'appunto, tecnici e comportano una forma indispensabile (e spesso solo temporanea) di memorizzazione di dati. Essi consentono la normale navigazione di un sito o la implementazione di un servizio desiderato dall'utente, limitandosi a salvare le preferenze ed i criteri di navigazione di ogni utente. Ad esempio, si pensi ai cookies di sessione per la memorizzazione delle preferenze linguistiche, o quelli che salvano i dati di login e del "carrello" per siti di e-shopping, e che possono essere eliminati una volta semplicemente chiuso il browser;
- **cookies di profilazione**, ossia quelli che non sono tecnicamente necessari per il funzionamento del sito. Si pensi, ad esempio, ai cookies di tracciamento, oppure ai cookies che creano profili personalizzati relativi all'utente per finalità pubblicitarie e vengono utilizzati principalmente per finalità di marketing (cookies di profilazione).

  Talora i cookies di profilazione possono essere anche cookies di terze parti, ossia di soggetti diversi dal gestore del sito nel quale vengono utilizzati che abbiano fatto un accordo con il gestore del sito per potervi installare propri cookies.

→ Secondo la normativa, i cookies tecnici possono essere usati anche senza chiedere il consenso dell'utente. Per gli altri cookies, invece, è necessario:

- che all'utente venga fornita una informativa chiara e completa in merito all'utilizzo dei cookies;
- che l'utente esprima un valido consenso, prima del trattamento.

Tali obblighi incombono sul gestore del sito web che usa i cookies.

Sono previste modalità "semplificate" di trasmissione della informativa e di raccolta del consenso, che si articolano su due livelli di approfondimento successivi:

1. nel momento in cui l'utente accede ad un sito web deve essergli presentata una prima informativa "breve", contenuta in un banner a comparsa immediata e ben visibile sulla home page o su ogni altra pagina alla quale sia possibile accedere direttamente. La richiesta di consenso all'uso dei cookie deve essere inserita già nel banner contenente l'informativa breve;
2. il banner contenente l'informativa breve deve, poi, contenere il link ad una informativa "estesa", letta la quale gli utenti possono differenziare le proprie scelte in merito ai diversi tipi di cookies archiviati tramite il sito in questione.

L'informativa "breve" deve già contenere, oltre al link all'informativa "estesa", l'informazione che il sito utilizza cookies di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze dell'utente manifestate nel corso della navigazione, l'indicazione dell'eventuale utilizzo di cookies di terze parti e l'indicazione che la prosecuzione della navigazione comporta la prestazione del consenso all'utilizzo dei cookies.

Dell'avvenuta prestazione del consenso all'utilizzo di cookies di profilazione occorre tenere traccia (anche mediante appositi cookies tecnici), il che consente poi al gestore

del sito di non riproporre l'informativa "breve" ad ogni successiva visita dello stesso utente al sito.

Particolare attenzione va riservata ai **cookies analitici**, che consentono di monitorare l'uso del sito da parte degli utenti (ad esempio, quali pagine visitano e qual è il sito di provenienza) e consentono di migliorare il sito stesso. Talora anche i cookies analitici possono essere di terze parti, e non dunque del "titolare" del sito.

Ci si è interrogati molto sulla possibilità o meno di considerare i cookies analitici come cookies tecnici, oppure come cookies di profilazione o comunque non aventi finalità meramente tecnica (in fin dei conti, si diceva, il titolare del sito trae un'utilità apprezzabile anche economicamente dal loro utilizzo, posto che grazie ad essi può migliorare il proprio sito, il suo funzionamento, la sua attrattività, ecc.). In generale si distingue tra:

- cookie analitici "di prima parte", ossia facenti capo al titolare del sito → sono assimilabili a quelli tecnici, e dunque utilizzabili senza consenso dell'utente del sito (ma sempre con informativa);
- cookie analitici di terze parti, per i quali è possibile una equiparazione ai cookie tecnici solo laddove i dati siano anonimizzati; in caso contrario, occorrerà ottenere il consenso dell'utente del sito.

3. Il trasferimento dei dati all'estero

I trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (ossia Unione europea + Norvegia, Liechtenstein, Islanda) o verso un'organizzazione internazionale sono **consentiti** se ricorre una delle seguenti condizioni:

a. l'adeguatezza del Paese terzo o dell'organizzazione è riconosciuta tramite decisione della Commissione europea (che successivamente alla decisione monitora al fine di controllare che le condizioni che hanno giustificato tale decisione continuino a permanere);
b. in assenza di tale decisione, ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati.

4. Il trattamento dei dati da parte dei motori di ricerca: il diritto alla deindicizzazione

Il tema della deindicizzazione, che si inserisce nel più ampio tema della cancellazione dei dati presenti online, riguarda una serie di problematiche anche molto incidenti sui diritti individuali: dal diritto del pubblico a reperire informazioni a problemi di *data protection* e di diritto all'identità personale, sino ai limiti del diritto dell'interessato alla cancellazione dei propri dati.

In estrema sintesi, il diritto alla deindicizzazione è il diritto dell'individuo ad ottenere, se ne ricorrono i presupposti, che un motore di ricerca **rimuova taluni risultati** da quelli che il motore stesso mostra all'utente all'esito di ricerche compiute usando come chiave il proprio nome. È il diritto a ottenere la rimozione di alcuni URL dai risultati di ricerca forniti dal motore all'esito di una *query* formulata a partire dal nome dell'interessato. In altri termini, è il diritto a rimuovere un determinato dato dalla rete, o da un suo particolare segmento, sottraendolo alla disponibilità degli internauti o rendendone meno agevole la reperibilità online.

I presupposti di tale diritto sono:

- il decorso di un significativo lasso di tempo dall'evento al quale il contenuto si riferisce (l'evento non deve essere più "attuale");
- la carenza di un generale interesse del pubblico;
- la lesività del contenuto, ossia la sua idoneità a danneggiare il soggetto al quale si riferisce.

La deindicizzazione è una attuazione del diritto individuale a chiedere che determinati dati e notizie non restino perennemente suscettibili di nuova e ingiustificata divulgazione online, anche per non vedersi attribuita una "biografia telematica" diversa da quella reale e costituente oggetto di notizie ormai superate.

Il gestore del motore di ricerca ha assunto un ruolo sempre meno "passivo" nella erogazione del servizio. Tanto che - come ribadito dalla giurisprudenza - l'attività del motore di ricerca consistente nel trovare informazioni pubblicate online da terzi, indicizzarle, memorizzarle temporaneamente e metterle a disposizione degli utenti secondo un ordine di preferenza deve essere qualificata come "trattamento di dati personali" del quale il gestore del *search engine* è il titolare; trattamento, questo, diverso e distinto da quello posto in essere dal gestore del sito sorgente sul quale il dato è stato originariamente pubblicato.

L'attività dei motori di ricerca comprende anche la realizzazione di copie delle pagine web indicizzate, dette **copie *cache***, le quali vengono conservate per un limitato periodo di tempo presso i server del *provider*. Tale sistema ha lo scopo di migliorare l'efficienza del servizio, consentendo, ad esempio, di fornire i risultati di ricerca in tempi più rapidi, quantomeno per le *keyword* più frequenti. Grazie alla funzione "copia *cache*" i motori di ricerca svolgono, di fatto, una vera e propria attività di memorizzazione di gran parte dei contenuti della rete dagli stessi indicizzati. La cancellazione dalla memoria del *provider* della copia *cache* degli URL a determinate pagine web ha l'effetto di precludere la possibilità di rinvenire tali contenuti all'esito di una interrogazione del motore di ricerca effettuata con qualsivoglia parola chiave. Laddove, per contro, la mera deindicizzazione sortisce il più limitato effetto di escludere che un contenuto compaia tra i risultati di un motore di ricerca in esito a una interrogazione basata sul mero nome di una persona, eliminando, così, una particolare modalità di ricerca del dato, il quale resta comunque raggiungibile attraverso il *search engine* mediante ricerche più articolate e diverse rispetto alla mera *query* "nominale".

→ Come chiarito dalla Cassazione, non è automatico che alla deindicizzazione di un URL debba sempre corrispondere anche la cancellazione della relativa **copia *cache***, ma occorre valutare caso per caso le singole situazioni ed effettuare un bilanciamento degli interessi in gioco, ossia, da un lato, dell'interesse del pubblico a reperire una determinata informazione e, dall'altro, del diritto del soggetto interessato alla protezione della propria riservatezza ma, ancor più, la propria reputazione.

Sempre in materia di motori di ricerca, è altresì noto il caso del *tool* fornito da uno dei principali *search engine* che contempla l'automatico accostamento alle prime parole della *query* di altri termini ritenuti pertinenti sulla base delle più diffuse ricerche effettuate sul web anche da altri utenti. Al riguardo, è stato in più occasioni sollevato il tema della lesività di taluni degli accostamenti effettuati dal motore di ricerca, con riferimento in particolare all'affiancamento di taluni vocaboli più o meno "denigratori" a nomi di personaggi noti (ad esempio, a fronte dell'inserimento nella barra di ricerca del nome

“Mario Rossi”, il motore di ricerca suggerisce la ricerca “Mario Rossi truffatore”). In termini generali, la giurisprudenza ha qualificato tale funzionalità come ulteriore e accessoria rispetto al semplice servizio di *search engine*, ritenendo, quindi, che, limitatamente a tale funzione, il *provider* non operi come mero intermediario, bensì come produttore diretto dell’informazione, e dunque possa essere responsabile per danni creati da quell’informazione se lesiva dell’onore e della reputazione.

IL DIRITTO APPLICATO ALLA PRODUZIONE ED ALL'IMPIEGO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

N.B.: PER UNA PREPARAZIONE COMPLETA OCCORRE AFFIANCARE LE PRESENTI DISPENSE AL CONTENUTO DELLE SLIDE DISCUSSE NEL CORSO DELLE LEZIONI

I. Perché serve un "diritto per l'Intelligenza Artificiale"?

La rapida evoluzione nel settore dell'A.I. e del *machine learning*, il cui sviluppo ha conosciuto negli ultimi anni un'accelerazione senza precedenti, incidono su ogni aspetto della nostra vita (lavoro, impresa, salute, economia, giustizia, polizia, attività della pubblica amministrazione, settore bancario, socialità, mobilità, creatività, finanza, ecc.), ponendoci davanti a nuovi scenari e domande inedite, anche dal punto di vista del diritto.

Gli interrogativi più rilevanti, a livello giuridico, sorgono in relazione alla capacità della macchina "intelligente" di essere ***self-learning***, ossia di **evolvere e crescere con l'esperienza** e di **cambiare i propri meccanismi di funzionamento** (cosa, questa, ben diversa dal semplice aumento di capacità computazionale). La capacità di essere *self-learning* - che consente alla macchina di acquisire la **capacità di agire in autonomia** - pone importanti questioni con riferimento:

- sia al problema della ***explainability***, ossia la possibilità di spiegare il "perché" del comportamento dei sistemi di A.I. più avanzati;
- sia alla rilevanza della fase del ***training*** della macchina e della **qualità dei dati** alla stessa forniti.

L'ampia diffusione dell'utilizzo di forme di A.I. in diversi campi pone, altresì, interrogativi di non poco conto anche dal punto di vista etico: ci si chiede, in particolare, se si possa pretendere dalla macchina un comportamento etico e quali siano gli strumenti, anche sul piano regolatorio, per la creazione di un'**etica dell'A.I.**

Diversi sono gli interventi normativi volti a regolare il fenomeno "*Artificial Intelligence*". A livello europeo, tra i più recenti, si ricordano:

- le Linee Guida per una A.I. etica del 2019;
- la Proposta di Regolamento per un *Artificial Intelligence Act* dell'aprile 2021;
- la Proposta di Direttiva per una nuova responsabilità da prodotto del settembre 2022;
- la Proposta di Direttiva sulla responsabilità civile da A.I. del settembre 2022.

Analogamente, si registrano in Cina nuove linee guida etiche per l'A.I. e negli Stati Uniti: decine di proposte normative in materia di A.I., alcune già legge.

Anche alla luce di tali preliminari considerazioni, si delineano, dunque, i seguenti temi d'indagine:

- in che modo è consentito "produrre" un sistema di A.I.? E quali caratteristiche deve, o dovrà, avere perché sia lecito produrlo, commercializzarlo e usarlo?
- quali sono le responsabilità connesse alla produzione ed all'impiego di sistemi di A.I.? Come i soggetti coinvolti nella "filiera" della A.I. possono essere chiamati a

rispondere delle "azioni" di un sistema che non riescono a pienamente prevedere *ex ante* e comprendere *ex post*?

- quali cautele sono richieste per l'utilizzo di questi sistemi? Quale l'affidamento nelle decisioni automatizzate e quali i controlli richiesti da parte dello *human in command*?

II. La regolazione della "produzione" di Intelligenza Artificiale

II.A) Le decisioni automatizzate: trasparenza e rischi di discriminazione

I nuovi sistemi di A.I. operano sulla base di modelli non più fondati solo su un paradigma logico-deduttivo e deterministico (secondo il quale, dunque, fornendo ai "sistemi intelligenti" i medesimi *input*, ci si potrà attendere gli stessi *output*), bensì su modelli predittivi basati su correlazioni statistiche.

Le criticità - cui già si è fatto cenno - connesse a tale *modus operandi* riguardano:

- la **spiegabilità** e la **trasparenza dell'A.I.**: i sistemi operano sulla base di logiche diverse da quelle umane, con la conseguenza che i risultati ottenuti risulteranno difficilmente prevedibili *ex ante* e comprensibili *ex post*;
- il rischio di **risultati discriminatori** e ***bias* cognitivi**, sia a livello di modello di dati, sia a livello di modello di calcolo dell'A.I. (al riguardo si evidenzia la rilevanza della fase del *training* della macchina e della qualità del *data set* alla stessa fornito).

→ **Che cosa di intende per spiegabilità**? La spiegabilità è la proprietà di un sistema di poter dare una spiegazione ad un essere umano in modo soddisfacente e di poter, dunque, rispondere alla domanda "perché?".

→ **Che cosa di intende per interpretabilità**? Al fine di rispondere a questa domanda è opportuno introdurre una ulteriore fondamentale distinzione tra:

- **A.I. simbolica**, basata su regole logiche-deduttive e deterministiche (in tale categorizzazione rientrano, ad esempio, i sistemi esperti in ambito medico o giuridico);
- **AI sub-simbolica**, basata su teorie statistiche e probabilistiche (si pensi, ad esempio, i sistemi di *machine learning*, *deep neural network*, ecc.).

La prima è per definizione comprensibile e spiegabile "in modo nativo", ossia produce in modo autonomo elementi per capire il come ed il perché di un determinato *output* (si parla in questo senso di "**white box"**). La seconda, per la complessità dei parametri usati e per la natura non deterministica dei modelli adottati, non garantisce di fornire una comprensibilità diretta del meccanismo che ha prodotto un determinato esito (si parla in questo senso di "**black box"**).

→ **Come posso "aprire" il black box?**

Un primo tentativo volto a risolvere il problema della opacità dell'algoritmo e dei processi decisionali "animati" dall'algoritmo si rinviene nell'**art. 22 del GDPR** (vd. dispense su protezione dati personali), il quale disciplina le ipotesi di **trattamento dei dati interamente automatizzato**.

- Per rispondere alla domanda se le tutele ivi previste per l'interessato possano ritenersi sufficienti e quale sia il tipo di informazioni che devono essere fornite allo stesso, si rinvia, per completezza, a quanto più ampiamente esposto alle pagg.

11-13 delle dispense su "*Dati, privacy e data protection*".

- Per esempi concreti di casi in cui sono state affrontate le criticità connesse alla opacità dei sistemi di A.I., si rinvia a quanto illustrato sui "*Casi trasferimenti insegnanti*" del 2019 nelle *slide* "*La regolazione dell'Intelligenza Artificiale*".

II.B) Nuovi obblighi? Ed in capo a chi?

I soggetti coinvolti nella "filiera" in materia di A.I., sui quali possono e potrann gravare specifici obblighi ed ai quali possono essere attribuibili, a diverso titolo come si dirà *infra*, le responsabilità relative al comportamento della A.I., sono i seguenti:

- il creatore dell'algoritmo;
- il creatore/costitutore della banca dati o comunque del dataset fornito all'A.I.;
- il *trainer* dell'A.I.;
- il creatore del *software* che incorpora l'algoritmo;
- il produttore dell'*hardware* che incorpora il *software* che incorpora l'algoritmo;
- il distributore del sistema di A.I.;
- l'utilizzatore del sistema di A.I.

II.C) La regolazione dell'A.I.: v. slides su Regolamento UE *Artificial Intelligence Act*

III. La responsabilità da produzione ed utilizzo dell'Intelligenza Artificiale: chi risponde dei danni causati dall'A.I.?

Come già rilevato, l'A.I. permette ai sistemi ed alle macchine autonomi ed "intelligenti" di sviluppare "*determinate caratteristiche autonome e cognitive*" e "*capacità di apprendere dall'esperienza e di prendere decisioni quasi indipendenti*" (Risoluzione Parlamento Europeo, febbraio 2017); ed, ancora, "*l'integrazione dell'IA nei prodotti può modificare il funzionamento di tali prodotti durante il loro ciclo di vita*", perché "*gli algoritmi possono continuare a imparare mentre vengono utilizzat*i" (Libro Bianco sull'A.I. UE, febbraio 2020).

Sotto il profilo giuridico della attribuzione delle responsabilità, tali caratteristiche pongono rilevanti quesiti; ed in particolare:

- se chi progetta, programma e "produce" il sistema può non essere sempre in grado di prevedere e prevenire le reazioni che il sistema sviluppa in relazione a quanto lo circonda, come può essere responsabile degli eventuali danni dallo stesso cagionati?
- in che modo tale soggetto può essere chiamato a rispondere di qualcosa che non è in grado di prevedere ed in relazione al quale (forse) non ha colpa? Esiste il rischio di un "vuoto di responsabilità"?
- è possibile affermare che più una macchina è autonoma, meno l'essere umano deve rispondere delle sue "azioni"?

→ Ma **a chi è possibile attribuire la responsabilità** per danni causati dal sistema "intelligente", tra i soggetti coinvolti nella "filiera" della A.I (creatore/produttore, creatore dell'algoritmo, addestratore, utilizzatore…)?

→ Ed ancora: è **sufficiente il rispetto dei requisiti tecnici di produzione dell'A.I**. che dovessero essere previsti dalla legge per andare esenti da responsabilità?

III.A) La responsabilità del produttore della A.I.: la responsabilità da prodotto difettoso

Con riferimento alle responsabilità attribuibili al produttore della A.I., viene in primo luogo in rilievo la normativa - concepita a livello unionale nella Direttiva 85/374/CEE e successivamente recepita a livello nazionale nel nostro Codice del consumo - in materia di **responsabilità da prodotto difettoso (*product liability*)**.

L'**onere probatorio** gravante sul danneggiato sulla base della normativa in esame prevede che lo stesso, al fine di ottenere il risarcimento del danno subito, possa limitarsi a dare prova dei seguenti elementi:

- della **difettosità del prodotto,** laddove il "difetto" consiste in un disallineamento del prodotto rispetto agli standard che la platea di utenti ha ragionevolmente diritto di attendersi;
- del **danno patito**;
- del **nesso di causalità** tra il suddetto difetto ed il danno.

N.B. **Non** sarà, invece, necessario per il danneggiato fornire la prova della **colpa** del produttore.

Evidente è, dunque, il favore accordato al consumatore dalla disciplina della *product liability* (si segnala, tuttavia, come in ipotesi di applicazione di tale disciplina ai sistemi autonomi, tale atteggiamento di favore nei confronti del consumatore potrebbe risultare frustrato dalla caratteristica della **opacità** - talvolta anche per il produttore - **del funzionamento del sistema "intelligente**": in altri termini, potrebbe risultare arduo fornire la prova sia del difetto che della correlazione causale tra difetto e danno).

La normativa in esame - applicabile anche al produttore di una componente del prodotto, il quale può rispondere direttamente nei confronti del consumatore - prevede, altresì, un'ipotesi di **esclusione della responsabilità** per danni causati da un difetto che non poteva essere previsto in base alle conoscenze scientifiche e tecniche disponibili al momento della messa a punto del prodotto (si parla, in questo senso, del cd. "**rischio da sviluppo**").

→ È **possibile applicare la disciplina della responsabilità da prodotto difettoso all'A.I**.?

Tale domanda assume particolare rilievo per il caso dell'**Internet of Things** (IoT), caratterizzato dalla connessione tra prodotti che interagiscono in *network*, coordinando le rispettive azioni per l'attuazione di obiettivi complessi. Tale caratteristica rende particolarmente arduo il riparto delle responsabilità per eventuali malfunzionamenti del sistema, specie quando a cagionare l'evento dannoso non sia un difetto del prodotto in sé considerato, ma un difetto dell'interazione dei *device.*

→ Ma, prima ancora, l'**A.I.** può definirsi "**prodotto**" ("*standalone*")? O è una **componente** di un prodotto ("*embedded*")?

Secondo la disciplina della responsabilità da prodotto, può definirsi tale "*ogni bene mobile, anche se incorporato in altro bene mobile o immobile*" (ivi inclusa l'elettricità) e la Proposta di UE di Regolamento definisce espressamente l'A.I. come "prodotto".

→ Quando l'**A.I.** può definirsi **difettosa**? Cosa è "difetto" quando parliamo di A.I.?

Al pari di quanto previsto per gli altri beni al consumo, il difetto del prodotto *A.I.-powered* consiste nel disallineamento dello stesso rispetto agli standard ragionevolmente attesi dall'utente.

Due le categorie di difetti che possono caratterizzare un la categoria di prodotti in esame:

- difetti genetici (si pensi, ad esempio, all'inserimento nel sistema A.I. di una linea di codice errata, ad una eccessiva permeabilità dell'A.I. alle aggressioni di *hacker*);
- difetti non genetici, ossia generati nel corso del processo di apprendimento ed evoluzione.

III.B) La Proposta di Direttiva per una nuova responsabilità da prodotto (settembre 2022)

Le considerazioni sinora svolte sono state in parte recepite e taluni degli interrogativi posti hanno trovato risposta nella recente **Proposta di Direttiva sulla responsabilità da prodotto difettoso**, con la quale la Commissione europea mira a sostituire le norme attualmente vigenti - alle quali si è sinora fatto cenno - per adattarle ai nuovi prodotti a elevato contenuto tecnologico, non solo all'A.I. (provvedimento "gemello" a quello in esame è la Proposta di Direttiva sulla responsabilità civile da A.I., presentata anch'essa nel settembre 2022 e volta ad adeguare le norme esistenti in materia di responsabilità civile all'A.I.).

Tale documento - che, **allo stato**, rimane ancora una **proposta** - propone, infatti, una "*revisione alla luce degli sviluppi connessi alle nuove tecnologie, ivi inclusa l'A.I., ai nuovi modelli di business dell'economia circolare […], nonché alla luce delle criticità emerse in relazione al riparto degli oneri probatori tra consumatore e impresa, specialmente in considerazione dell'incremento della complessità scientifica*".

- ❖ Per le "nuove" definizioni di "prodotto", di "componente", di "difetto" e di "rischio da sviluppo", si rinvia alle *slide* "*Responsabilità da Intelligenza Artificiale*".

III.C) La responsabilità da attività pericolosa

Accanto alla normativa della *product liability*, in relazione ai nuovi sistemi intelligenti, viene, altresì, in rilievo quella relativa all'esercizio di attività pericolosa, disciplinata dall'art. 2050 del codice civile, il quale prevede che "*chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno*".

→ L'**A.I. è "pericolosa"** per natura? Il ricorso alla A.I. si rivela, per sua natura, suscettibile di rendere pericolose attività che altrimenti non sarebbero tali?

In questo senso parrebbe deporre anche la Proposta di Regolamento sull'A.I. che - come già accennato - espressamente individua, a monte, delle specifiche forme di A.I. che definisce **"ad alto rischio"** (tra le quali inserisce, peraltro, il settore dei trasporti, con i veicoli a guida autonoma).

Sulla base della disciplina in esame, la responsabilità dell'esercente attività pericolosa può essere esclusa solo ove lo stesso dimostri di avere adottano preventivamente **tutte** le **misure (preventive) idonee** ad evitare il danno.

→ **Quali sono le "misure idonee**"?

La valutazione dell'idoneità di tali misure dovrà esser effettuata con un **giudizio *ex ante*** in relazione all'esigenza di evitare la generale situazione di pericolosità (e non lo specifico evento lesivo) e dovrà necessariamente essere condotta alla luce delle **conoscenze e delle tecnologie esistenti al momento della produzione**.

→ **Cosa è da considerarsi "pericoloso"**? Solo la produzione, o anche la vendita, l'utilizzo…dell'A.I.?

LA PROTEZIONE DEI "BENI INFORMATICI" (SOFTWARE, BANCHE DATI, SITI WEB): DIRITTO D'AUTORE E BREVETTI

Diritto d'autore e brevetti: elementi essenziali

La legge riconosce la necessità di tutelare l'atto creativo e/o inventivo, di garantire, dunque, determinati diritti e protezioni a chi è il creatore di una opera che, per sue caratteristiche, sia meritevole di essere tutelata, anche incentivando il suo autore, o l'inventore di un ritrovato tecnico. Nasce per questo motivo la **disciplina in materia di proprietà intellettuale (diritto d'autore) ed industriale (brevetti[1])**.

Si tratta di una disciplina che ha lo scopo di favorire, dunque, la creazione e lo sviluppo tecnologico ed incentiva l'essere umano a creare/inventare, garantendogli una retribuzione e diritti connessi alla creazione/invenzione. È questa l'esigenza principale sottostante alla normativa in materia di proprietà intellettuale ed industriale, della quale nelle seguenti pagine si tracceranno gli elementi essenziali prima di procedere all'esame delle sue applicazioni con riferimento al mondo dell'informatica.

I. Il diritto d'autore

La disciplina in materia di diritto d'autore - composta di fonti di diversa provenienza, nazionale, internazionale ed europea (diverse direttive, tra le quali la più recente è la Direttiva 2019/790, emanata proprio per adattare la disciplina del diritto d'autore alle opere dell'ingegno informatiche ed alle tecnologie emergenti) - è nata principalmente per tutelare le opere dell'ingegno "tradizionali" (opere letterarie, musicali, artistiche, cinematografiche, ecc.), ma è stata poi adattata ed integrata per applicarsi anche alla protezione di opere dell'ingegno quali software, banche dati, ecc.

La normativa in materia di diritto d'autore tutela le **creazioni intellettuali definite come "opere dell'ingegno"**, ossia una particolare espressione del lavoro intellettuale.

Opera dell'ingegno è, in termini generali, ogni risultato creativo raggiunto mediante il prevalente impiego delle facoltà della mente umana. Opere dell'ingegno sono, ad esempio, le opere letterarie, scientifiche, musicali, teatrali, della scultura, della pittura, del disegno e delle arti figurative, così come i disegni e le opere dell'architettura, le opere di *design* industriale, le opere cinematografiche e fotografiche, ma anche i "programmi per elaboratore" (i software) e le banche dati. Il che significa che il software può essere protetto mediante diritto d'autore, quindi che il creatore del software può essere titolare di diritto d'autore sul software stesso, e che colui che crea una banca dati può, a certe condizioni che vedremo, essere titolare del diritto d'autore sulla banca dati.

Perché un'opera possa essere tutelata da diritto d'autore essa deve essere realizzata, ossia deve estrinsecarsi nel mondo materiale, qualunque ne sia il modo o la forma di espressione (anche senza fissazione su un supporto materiale): le semplici idee astratte non rilevano come opera dell'ingegno e non sono protette dal diritto d'autore fino a quando non si concretizzano, non trovano realizzazione.

Non ogni espressione dell'intelletto, poi, merita tutela, ma solo quelle:

[1] Ai nostri fini si dedicherà specifica attenzione alla tematica dei brevetti. Occorre, però, evidenziare che la normativa in materia di proprietà industriale tutela anche altri beni, come i marchi, la ditta, i disegni industriali, ecc.

- **dotate di carattere creativo e, dunque, originali**, ossia quelle che costituiscono una individuale e personale espressione dell'idea da parte dell'autore dell'opera;
- **nuove**, ossia sufficientemente diverse da opere precedenti.

Oltre alle opere "create dal nulla", la normativa protegge anche le opere derivate, ossia quelle il cui contenuto è, in parte, non originale. Perché un'opera derivata possa essere protetta da diritto d'autore, al contenuto preesistente (quello non originale) deve essere affiancata una porzione originale oppure il contenuto preesistente deve essere, nel suo complesso, strutturato in modo originale (si pensi, ad esempio, alla versione remixata di una canzone, o alla traduzione in un'altra lingua di un'opera letteraria).

Il creatore di un'opera dell'ingegno dotata di carattere creativo, originale e nuova è, dunque, titolare del diritto d'autore su quell'opera e, per diventare tale, non è necessaria una particolare procedura di "registrazione" dell'opera o di "deposito" o di presentazione di apposita "domanda" presso pubblici uffici (come invece succede, ad esempio, per i brevetti), ma è sufficiente creare l'opera. Il semplice atto creativo di un'opera dell'ingegno originale e nuova fa nascere il diritto d'autore in capo al creatore, che diventa dunque titolare dei diritti connessi a quell'opera (sia morali che patrimoniali, come diremo).

In termini generali, qualsiasi utilizzo dell'opera protetta da diritto d'autore è soggetta al previo necessario consenso dell'autore. Il titolare del diritto d'autore vanta due tipologie di diritti sull'opera dell'ingegno:

- diritto morale sull'opera: è il diritto ad essere riconosciuto come autore dell'opera, il diritto dell'autore di vedersi riconosciuta la paternità dell'opera e di rivendicarla (ad esempio, il diritto di uno scrittore ad essere riconosciuto come autore di un determinato romanzo, o il diritto di un compositore di essere riconosciuto come autore di una determinata sinfonia).

  È un diritto irrinunciabile, che dura per tutta la vita dell'autore e che non può essere ceduto (inalienabile): ciò significa che l'autore non può cedere ad altri il diritto ad essere riconosciuto come autore di una determinata opera;
- diritti patrimoniali sull'opera: sono i diritti di utilizzo e sfruttamento economico dell'opera (venderla, farne copie, darla in licenza, ecc.), traendone il corrispettivo beneficio. Comprendono, ad esempio:
  - il diritto di pubblicazione;
  - il diritto di riproduzione, ossia di fare copie dell'opera e di distribuirle, anche a pagamento (una modalità di distribuzione di un'opera è, ad esempio, consentirne il download da un sito web);
  - il diritto di comunicazione al pubblico o di mettere l'opera a disposizione del pubblico in modo che ciascuno possa avervi accesso (si pensi, ad esempio, all'upload di un'opera su internet);
  - il diritto di elaborazione dell'opera, ossia di "trasformarla" o di apportarvi modifiche.

  I diritti in questione riguardano sia l'opera nel suo complesso, sia singole parti dell'opera (l'autore può decidere di "dividere" la sua opera e di "venderne" singole parti separatamente).

I diritti patrimoniali durano per tutta la vita dell'autore e per 70 anni dopo la sua morte (perché, come diremo, per il diritto italiano "autore" di un'opera può essere solo una persona fisica, soggetta, quindi, a morire).

Sono diritti che, di regola, appartengono all'autore dell'opera, che però li può cedere a soggetti terzi. Non sempre, quindi, l'autore è titolare sia del diritto morale sull'opera che dei diritti patrimoniali sulla stessa (se i diritti patrimoniali su una certa opera appartengono ad un soggetto diverso dall'autore, è questo soggetto che deve dare il proprio consenso ad ogni utilizzo dell'opera).

I singoli diritti patrimoniali sono fra loro indipendenti ed autonomi e come tali possono essere trattati e ceduti. Ad esempio, l'autore di un libro può cedere ad un soggetto terzo il diritto di trasformarlo in una pièce teatrale e metterlo in scena, oppure in un film, mantenendo in capo a sé tutti gli altri diritti patrimoniali o cedendone altri a soggetti ancora diversi. La qual cosa può rendere anche molto complessa la gestione dei diritti connessi ad un'opera dell'ingegno, necessitando l'adozione di dettagliate disposizioni contrattuali.

Come già anticipato, in via generale, per il diritto italiano, **"autore" di un'opera può essere solo una persona fisica**, eccezion fatta per alcuni (limitati) casi specificamente previsti dalla legge. È possibile, però, "scorporare" diritti morali e diritti patrimoniali. Mentre "autore" resta sempre una persona fisica, che mantiene i diritti morali sull'opera, una persona giuridica può essere titolare dei diritti patrimoniali sull'opera in alcune ipotesi nelle quali la legge vuole proteggere l'investimento economico di alcuni soggetti. Per comprendere meglio il concetto, si pensi:

- ai diritti di utilizzazione economica sui software, sulle banche dati e sulle opere di *design* industriale creati dal lavoratore dipendente in esecuzione delle sue mansioni o su istruzioni del datore di lavoro, che appartengono al datore di lavoro stesso, anche se persona giuridica;
- ai diritti di utilizzazione economica sulle riviste o sui giornali, che appartengono all'editore, il quale può essere anche una persona giuridica;
- ai diritti di utilizzazione economica di un'opera cinematografica, i quali appartengono al produttore, che può essere anche una persona giuridica.

La titolarità dei diritti sull'opera può appartenere a **uno o più soggetti**, a seconda delle dinamiche che hanno condotto alla realizzazione dell'opera. Un'opera dell'ingegno può essere anche il frutto dell'apporto intellettivo originale di più soggetti. In questo caso si parla:

- di opera in comunione se i singoli apporti e contributi dei diversi autori "si fondono" in un'opera complessivamente organica, diventando inscindibili ed indistinguibili nell'opera finale e non potendo essere "usati" separatamente (ad esempio, un film con due registi, oppure un romanzo con due autori). In questo caso il diritto d'autore appartiene a tutti i coautori in parti uguali (a meno che non esista un accordo scritto tra i coautori in altro senso);
- di opera collettiva se i vari contributi che compongono l'opera restano creazioni autonome anche nell'opera finale, la quale è il frutto dell'attività di un soggetto che ne ha curato la scelta, l'"assemblaggio" ed il coordinamento (si pensi, ad esempio, ad un quotidiano, che è composto da singoli articoli di diversi giornalisti-autori che restano potenzialmente isolabili). In questo caso il singolo contributo resta di titolarità del suo autore, mentre autore dell'opera collettiva è il soggetto

che organizza e dirige la sua creazione (nell'esempio del quotidiano, il suo direttore, persona fisica che è titolare del diritto morale d'autore sul quotidiano nel suo complesso, mentre i diritti di sfruttamento economico del quotidiano, tra cui il diritto di incassare i proventi della sua vendita, spettano al suo editore, che può essere anche persona giuridica).

II. Invenzioni e brevetti

Il diritto d'autore protegge, abbiamo detto, le opere dell'ingegno a carattere creativo. Diversa è, invece, la normativa in materia di brevetti, che tutela le **invenzioni a carattere tecnico** (in qualsiasi settore della tecnica), quelle che siano idonee ad avere una applicazione industriale. L'invenzione è, dunque, la soluzione ad un problema tecnico suscettibile di applicazione industriale, sia essa, ad esempio, un prodotto nuovo ed innovativo, un macchinario applicato nell'industria, un procedimento particolare scoperto per la realizzazione di un determinato prodotto, ecc.).

Per essere tutelata l'invenzione deve essere **brevettata**: non è, dunque, sufficiente il semplice atto inventivo, come invece avviene per le opere tutelate da diritto d'autore, ma occorre esperire una apposita procedura per vedersi riconoscere il diritto di brevetto su una determinata invenzione. Il brevetto è quindi lo strumento, l'atto che consente a chi ha realizzato una invenzione di poterla produrre e commercializzare in esclusiva sul territorio dello stato dove il brevetto è stato registrato.

Perché un'invenzione possa essere brevettata essa deve essere:

- nuova: non deve essere mai stata prodotta o brevettata in alcuna parte del mondo. Il requisito della novità si valuta sulla base dello stato della tecnica al momento del deposito della domanda di brevetto. Se un certo ritrovato è già stato realizzato o brevettato in Cina (con un brevetto che ha efficacia solo in Cina), chiunque in Italia potrà produrlo e venderlo, ma non potrà brevettarlo;
- inventiva: non deve essere soltanto nuova, ma non deve essere "banale" rispetto allo stato della tecnica. Deve rappresentare un progresso, un passo in avanti nello sviluppo della tecnica di settore;
- industriale: deve poter essere riprodotta a livello industriale.

L'invenzione deve essere anche attuata: come per il diritto d'autore, le semplici idee o le teorie, per quanto innovative, non possono essere brevettate se non trovano una loro estrinsecazione "nel mondo reale".

Sono brevettabili anche i **procedimenti**, con il c.d. brevetto di procedimento. Si parla di brevetto di procedimento quando l'invenzione consiste in un'idea non materiale, quale ad esempio una nuova procedura industriale o un metodo di lavorazione per la realizzazione di prodotti. Il brevetto per un'invenzione di procedimento può essere depositato indipendentemente dal fatto che tramite il procedimento brevettato si ottenga un prodotto in sé già noto: sono, infatti, considerate invenzioni di procedimento anche le invenzioni di un procedimento per ottenere prodotti già noti, così come anche le invenzioni per nuovi usi di prodotti in sé noti.

Per ottenere il brevetto occorre seguire una determinata procedura:

1. deposito della apposita domanda di brevetto presso l'ufficio competente per il rilascio di brevetti (per l'Italia è l'UIBM – Ufficio Italiano Brevetti e Marchi), descrivendo l'invenzione che si chiede di brevettare con un grado di dettaglio

abbastanza elevato ma non eccessivo, in modo da rendere la tutela non eccessivamente rigida.

Occorre indicare, tra le altre cose: 1) le caratteristiche dell'invenzione che si intendono tutelare, che sono chiamate "rivendicazioni"; 2) il nome dell'inventore, che deve essere sempre una persona fisica.

È la fase più importante, perché un errore in questa fase può pregiudicare l'intero iter brevettuale e la successiva tutela. Occorre depositare anche documentazione tecnica a sostegno della domanda e pagare le relative tasse di deposito;

2. prima fase di "segretezza", che generalmente dura 18 mesi dal deposito della domanda ed alla quale segue la pubblicazione della domanda e della relativa documentazione (ma l'inventore può anche domandare che la domanda e la documentazione vengano pubblicate immediatamente al deposito);
3. esame preliminare, ricerca di anteriorità e opinione scritta dell'Ufficio Europeo dei Brevetti, che valuta la novità, l'inventività e l'applicazione industriale dell'invenzione;
4. esame di merito e conclusione, con la concessione del brevetto o il rifiuto della domanda.

Il provvedimento finale, con la eventuale concessione del brevetto, solitamente si ha entro 24-30 mesi dal deposito della domanda. Gli effetti del brevetto, però, decorrono dalla data in cui la domanda con la descrizione dell'invenzione è resa accessibile al pubblico.

È anche possibile depositare una domanda di brevetto europeo, che consente di avvalersi di un'unica procedura per l'ottenimento di un brevetto che conferisce al suo titolare gli stessi diritti che deriverebbero da un brevetto nazionale anche in ciascuno degli stati che aderiscono alla Convenzione sul brevetto europeo. In termini semplici, invece di dovere depositare una domanda di brevetto in ognuno di questi stati, è sufficiente depositare una sola domanda di brevetto europeo che, se accolta, acquisisce validità anche negli altri stati.

Esiste anche la possibilità di ottenere un "brevetto internazionale", sulla base di un trattato internazionale al quale aderiscono allo stato 153 paesi e che è gestito dal WIPO (World Intellectual Property Organization). Il trattato ha lo scopo di facilitare la richiesta di protezione per una invenzione simultaneamente in più paesi, depositando un'unica domanda internazionale di brevetto presso l'ufficio competente di uno degli Stati membri, anziché diverse domande nazionali o "regionali" presso gli uffici competenti di ciascuno di essi. È poi l'ufficio competente di ogni stato a rilasciare il brevetto.

Il brevetto su una invenzione ha una durata di 20 anni dalla data del deposito della domanda di brevetto (e ogni anno occorre versare una sorta di "tassa di mantenimento" del brevetto). Dopo 20 anni, il brevetto non può essere rinnovato e scade, e dunque l'invenzione diventa liberamente riproducibile da chiunque.

Il brevetto decade (quindi perde d'efficacia anche prima dello scadere dei 20 anni):

- se il titolare non paga le "tasse di mantenimento" del brevetto;
- per non uso prolungato del brevetto: l'invenzione deve essere attuata entro 3 anni dalla concessione del brevetto o 4 anni dal deposito della domanda.

Il titolare del brevetto ha il diritto di produzione esclusiva dell'invenzione, quindi il diritto di vietare a terzi di produrre, usare, mettere in commercio, vendere, applicare l'invenzione, se non con il consenso del titolare del brevetto, e dunque di trarre profitto dall'invenzione. Ogni utilizzo non autorizzato dell'invenzione oggetto di brevetto è una contraffazione dell'invenzione.

Anche per le invenzioni e i brevetti, come per il diritto d'autore, si distingue tra diritti morali e diritti patrimoniali:

- i diritti patrimoniali sono i diritti del titolare del brevetto di trarre guadagno dall'utilizzo del brevetto (suo impiego, sua concessione ad altri, ecc.).

  Sono diritti che possono essere ceduti anche a terzi, come per il diritto d'autore;

- il diritto morale è il diritto dell'inventore di essere riconosciuto come inventore dell'invenzione.

  È un diritto che non può essere ceduto a terzi, ma l'inventore può essere diverso dal titolare del brevetto: ad esempio, l'invenzione è creata da un dipendente di una società nell'esercizio delle sue mansioni ed il brevetto viene depositato dalla società. In questo caso il dipendente è l'inventore, mentre il titolare del brevetto (e dunque il soggetto che ha i diritti patrimoniali connessi a quel brevetto) è la società datrice di lavoro.

  Come già anticipato, l'inventore deve essere sempre una **persona fisica**.

Diverso dall'invenzione è il **modello di utilità**, ossia una forma nuova di un prodotto che dà al prodotto stesso una particolare efficacia o facilità o comodità di applicazione o di impiego (ad esempio, un coltello per mancini, una particolare forma di pallone da calcio che lo renda più aerodinamico, ecc.). I modelli di utilità non sono, dunque, una nuova soluzione ad un problema tecnico, ma una sorta di miglioramento della soluzione tecnica già precedentemente nota (in questo senso non costituiscono un nuovo avanzamento della tecnica di settore). Per semplificare all'estremo, possiamo dire che il modello di utilità è una soluzione migliorativa di oggetti già esistenti, mentre l'invenzione è la creazione di qualcosa che prima non esisteva. Anche i modelli di utilità in Italia possono essere brevettati, ma il brevetto dura 10 anni dal deposito della sua domanda (e non 20 come il brevetto).

La protezione del software mediante diritto d'autore

Originariamente sugli strumenti di tutela del software era sorto un dibattito tra chi sosteneva che il software avesse una natura tecnica e che potesse, quindi, essere protetto come un'invenzione e chi, invece, lo considerava come una particolare forma di scrittura, e dunque come un'opera dell'ingegno a carattere creativo.

È prevalsa, in sostanza, la seconda impostazione: i software (i "programmi per elaboratore", come li chiama la legge sul diritto d'autore) sono, dunque, in generale proteggibili mediante diritto d'autore (ad eccezione, come vedremo, di specifiche ipotesi nelle quali il software può essere oggetto di brevetto), come le opere letterarie. In altri termini, il creatore di un software è titolare del diritto d'autore (dunque dei diritti morali e dei diritti patrimoniali d'autore, v. sopra) sul software creato.

La protezione del software riguarda qualunque tipo di software (sistemi operativi, programmi applicativi, ecc.) e concerne:

- sia il codice sorgente (cioè l'insieme delle istruzioni scritte dal programmatore in un determinato linguaggio di programmazione, in qualsiasi linguaggio il codice sorgente sia scritto);
- sia il codice oggetto (cioè l'insieme delle istruzioni del programma tradotte in linguaggio macchina, ossia in codice binario);
- sia i relativi materiali preparatori (i diagrammi di flusso, le specifiche funzionali, le descrizioni di sequenza, ecc.).

Non sono tutelati, invece, le idee ed i principi alla base del codice sorgente od oggetto di un programma.

Perché un software possa essere proteggibile mediante diritto d'autore, deve essere **originale**, dunque non frutto di una mera azione di copiatura. In un mercato "affollato" come quello del software, è relativamente facile che un software possa essere oggetto di diritto d'autore: la soglia della creatività necessaria a tal fine è relativamente bassa ed è generalmente sufficiente che il software non sia frutto di mero plagio e che non sia del tutto banale, che vi sia, dunque, uno sforzo creativo che si estrinsechi nella scelta delle diverse opzioni informatiche e nella loro diversa rappresentazione, richiedendosi un sufficiente grado di valore aggiunto rispetto alla situazione anteriore.

Il diritto d'autore sul software "nasce" semplicemente con la sua creazione, senza necessità di "registrazioni" o di presentare domanda presso alcun pubblico ufficio, diversamente da quanto avviene per il brevetto. Tuttavia, per dare un livello minimo di "oggettività" alla tutela, potrebbe essere consigliabile depositare il software presso il Pubblico Registro per il Software, tenuto dalla SIAE, al fine di ottenere una prova "documentata" dell'esistenza del software e dell'identità di chi lo ha creato (paternità). Occorre a tal fine presentare una domanda alla SIAE con:

- indicazione dell'autore o degli autori del software;
- data di pubblicazione del software;
- in allegato un esemplare del programma su supporto digitale contenente il codice sorgente o il codice oggetto o entrambi.

All'autore del software è riconosciuto il diritto esclusivo di effettuare o autorizzare:

- la riproduzione, permanente o temporanea, totale o parziale, del software con qualsiasi mezzo e con qualsiasi forma (anche il caricamento, la visualizzazione, l'esecuzione, la trasmissione o la memorizzazione del software richiedono l'autorizzazione del titolare del diritto d'autore se comportano la riproduzione);
- l'adattamento ed ogni modifica del software;
- qualsiasi forma di distribuzione al pubblico (vendita, licenza, ecc.).

Spesso alla creazione del software collaborano più soggetti, quindi il software potrebbe essere:

- o un'opera collettiva, nel qual caso la titolarità spetta a chi ha coordinato la realizzazione del software;
- o un'opera in comunione, nel qual caso la titolarità del diritto d'autore sul software spetta a tutti i co-creatori (i quali potranno disciplinare tale diritto mediante un accordo tra di essi).

I diritti di utilizzazione economica sui software creati dal lavoratore dipendente in esecuzione delle sue mansioni o su istruzioni impartite dal datore di lavoro spettano al datore di lavoro (sia persona fisica che persona giuridica), mentre il diritto morale d'autore spetterà sempre alla persona fisica che ha nei fatti creato il software (il dipendente).

Software open source e diritto d'autore: un software open source è reso tale per mezzo di una licenza mediante la quale i titolari dei diritti d'autore su un determinato software ne "aprono" il codice sorgente alla modifica, studio, distribuzione e riutilizzo da parte di soggetti terzi. Si tratta, dunque, di una metodologia di sviluppo di software basata su specifiche licenze (licenze open source), le quali si distinguono dalle licenze relative a software proprietari per la pubblicazione del codice sorgente (che non sempre, però, avviene gratuitamente).

Nel caso di software open source, quindi:

- i diritti esclusivi individuati dalla legge rimangono in capo al titolare, il quale, però, può decidere liberamente di astenersi dal far valere in tutto o in parte questi diritti e nel contempo può concedere a terzi determinate facoltà d'uso del software attraverso uno strumento che è il contratto di licenza d'uso (vd. pagine successive);
- l'utilizzo e la modifica del codice preesistente può implicare la creazione di un'**opera derivata**, se sufficientemente creativa e originale, senza per ciò limitare in alcun modo i diritti dell'autore del software;
- se non sussistono i requisiti perché si parli di un'opera derivata (quindi se il risultato non è sufficientemente creativo e originale), si potrà applicare la disciplina delle **opere collettive**, in forza della quale ogni contributo aggiuntivo potrà avere autonoma protezione se distinguibile e scindibile dall'opera originaria, mentre autore dell'opera risultante dall'unione dei vari contributi sarà chi ha organizzato e diretto la creazione dell'opera (spesso questo aspetto è disciplinato nelle licenze);
- se i contributi aggiuntivi non sono né originali né scindibili tra loro, possono essere assoggettati alle norme sulle **opere in comunione**, in base alle quali il diritto d'autore appartiene in comune a tutti i coautori.

La questione può essere anche estremamente complessa e non verrà qui trattata nella sua completezza, ma ci si limiterà a brevi cenni. L'open source software è, del resto, un bene in costante evoluzione, che si forma per accrescimento, grazie ai contributi (leciti perché autorizzati) di elaborazione, correzione, variazione e sviluppo apportati da più soggetti. Il problema della plurisoggettività è, dunque, da considerarsi intrinsecamente connesso alle normali dinamiche creative ed attributive del software a codice aperto. Molto dipende, comunque, da quanto previsto dalle licenze che disciplinano l'open source, che dovranno quindi essere scritte con estrema attenzione.

La protezione brevettuale del software (v. anche specifica dispensa sul tema)

Come si è detto, in termini generali, il software in quanto tale non può essere brevettato, ma gode unicamente della tutela offerta dal diritto d'autore (più debole rispetto a quella offerta dal brevetto). Esistono, però, **condizioni alle quali un software può anche essere brevettato** (o può essere sia oggetto di diritto d'autore che oggetto di brevetto). Ciò può avvenire:

- se il software, come succede per tutte le altre invenzioni, risolve con una soluzione innovativa e non ovvia (per una persona competente in materia) un problema tecnico (se ha, quindi, una sua applicazione "industriale"), offrendo quindi un contributo allo stato dell'arte della tecnica di settore;
- comunque, solo se il suo effetto tecnico va oltre la normale interazione tra programma e computer, tra software e dispositivo hardware. È quindi fondamentale, affinché un software possa essere brevettato, che vi sia un effetto tecnico derivante dall'esecuzione del software stesso, che può essere riscontrato sia all'esterno del PC (ad esempio, in sistemi di controllo di processi o apparecchiature), sia all'interno del PC stesso (ad esempio, nella gestione dei dati nella memoria del computer oppure nella gestione delle risorse hardware).

Ogni programma per elaboratore produce un effetto tecnico tangibile, ovvero gli impulsi elettrici azionati dall'hardware. Perché il software sia brevettabile, questo non è sufficiente, ma il software deve produrre un effetto tecnico ulteriore. Ad esempio:

- è brevettabile un software che implementa il funzionamento dei freni di un'autovettura; il software che consente il funzionamento di un frigorifero, di un forno, di un robot aspirapolvere… Può essere brevettato anche il software che permette ad un computer di accendersi e di espletare le sue funzioni prettamente fisiche;
- non sono brevettabili invece un software gestionale, un software per la gestione della contabilità, un motore di ricerca…

Il brevetto offre al software una tutela "più forte", e comunque diversa, rispetto a quella offerta dal diritto d'autore:

- il diritto d'autore protegge il software "per come è scritto", e tutela quindi la forma del codice. Quindi ogni volta che viene scritto un programma che esegue la stessa funzione di un software già esistente, ma utilizzando una scrittura differente, non si ha violazione dei diritti d'autore del creatore del software pre-esistente;
- il brevetto, invece, protegge la funzionalità del software, ossia il modo in cui funziona ed il risultato al quale porta, a prescindere dalla forma del codice. Il che significa che è impedita, per esempio, la progettazione da parte di terzi di un codice differente che dia lo stesso risultato.

La tutela brevettuale è, dunque, più completa e più forte, ma è anche più complessa (e più costosa) da ottenere. Occorre, poi, ricordare che la tutela brevettuale dura 20 anni dal deposito della domanda.

La protezione del software nei contratti di sviluppo software e nella licenza

I diritti su un software realizzato in base ad un **contratto di sviluppo software** (ossia un contratto mediante il quale una parte incarica un singolo professionista o una software house di sviluppare un software nel proprio interesse, al fine di raggiungere un determinato obiettivo) generalmente appartengono al soggetto che ha commissionato il software: questo con riguardo, naturalmente, ai soli diritti patrimoniali d'autore, mentre il diritto morale d'autore spetterà sempre a chi ha creato il software. Qualora il creatore del software intenda mantenere per sé taluni diritti relativi all'utilizzo del software, dovrà disciplinare tale aspetto nel contratto.

Il più comune metodo di distribuzione al pubblico di un software in modo tale da proteggere, al tempo stesso, il diritto d'autore del suo creatore/titolare è la **licenza**. Con la licenza, il titolare del software ne concede l'utilizzo, per un determinato periodo, ad un soggetto terzo, che paga un corrispettivo per questo utilizzo.

Con la licenza d'uso l'utilizzatore non acquista la proprietà del software, ma solo il diritto di usarlo in modo limitato, in base alle condizioni d'uso previste nella stessa licenza. La licenza, quindi, non trasferisce la proprietà dei diritti connessi al software ad un soggetto diverso: il software ed i relativi diritti d'autore restano sempre di titolarità di chi l'ha creato (o, per quanto concerne i diritti patrimoniali d'autore, degli eventuali diversi soggetti che tali diritti hanno acquistato), ma con la licenza si concede la possibilità di usare il software anche a soggetti terzi, nei limiti previsti dalla licenza stessa, che è essenzialmente un contratto che disciplina le modalità attraverso le quali il soggetto terzo (licenziatario) può usare il software (farne copie, anche di riserva, modificarlo, ecc.). Di particolare importanza è, nello specifico, chiarire nel contratto di licenza che il diritto di utilizzo è limitato ad un determinato periodo, al fine di evitare l'esaurimento del diritto d'autore

La licenza generalmente concede ampi diritti al licenziatario (diritto ad ottenere gli eventuali aggiornamenti del software, diritto di farne copie ove necessarie per l'uso per il quale la licenza è stata concessa, ecc.). Talora il licenziatario ha anche il diritto di effettuare il reverse engineering (o decompilazione) di un software, ossia di effettuare quelle operazioni necessarie a ricostruire il codice sorgente partendo dal codice oggetto, apprendendo la struttura e le caratteristiche del software: in termini generali, il licenziatario può effettuare tale operazione soltanto quando indispensabile per conseguire la interoperabilità (ossia la compatibilità) con un proprio programma creato autonomamente e comunque le informazioni apprese mediante il reverse engineering non dovranno essere divulgate a terzi e dovranno essere utilizzate solo per scopi "personali" del licenziatario, che non potrà applicarle industrialmente.

Per quanto concerne il software si distinguono tre tipologie di licenze:

- licenze di tipo **proprietario**, ossia quelle delle quali abbiamo parlato sinora, le quali concedono agli utenti soltanto alcune facoltà di utilizzo del software, mantenendo in capo al titolare i diritti esclusivi di utilizzazione economica del software stesso;
- licenze di software libero con permesso d'autore (**copyleft**), che utilizzano il diritto d'autore per garantire a chiunque la possibilità di copiare, modificare e migliorare il software e di ridistribuirlo al fine di permettere a tutta la comunità di godere dei risultati raggiunti, evitando al tempo stesso, però, che terzi possano utilizzare il codice sorgente per realizzare software proprietario. L'utilizzo di questa tipologia di licenze non significa necessariamente che l'accesso al software venga concesso gratuitamente;
- licenze **permissive**, ossia quelle che, oltre a concedere all'utente il diritto di utilizzare liberamente, copiare e modificare il software, consentono anche la possibilità di distribuirlo con una licenza differente da quella originaria, anche di tipo proprietario, seppur rispettando alcune condizioni indicate nella licenza stessa.

Altra possibilità, sempre più utilizzata dai produttori di software, è il ricorso al **cloud-computing**, che consente alle software house di "distribuire" i propri software senza bisogno di cederne "materialmente" delle copie (sia che sia su supporto fisico o

mediante download). I contratti di licenza diventano così degli abbonamenti, che permettono agli utenti di accedere ad un servizio online per un periodo limitato di tempo (software-as-a-service). In questo modo le software house possono mantenere un controllo molto più incisivo sui propri software, evitando la cessione sia del codice sorgente che del codice oggetto.

La tutela delle banche dati

Le banche dati non sono brevettabili, perché sono il risultato di una attività puramente intellettuale che esula dal campo della tecnologia. Le banche dati possono godere, a seconda delle loro caratteristiche, di due tipologie di protezione, che sono alternative:

- diritto d'autore, oppure
- diritto sui generis.

Premettiamo che, secondo la legge, una "banca dati" è tale solo se si tratta di una raccolta di dati:

- sistematicamente e metodicamente disposti ed ordinati.

  Quindi raccolte non ordinate o puramente casuali di dati non potranno essere considerate "banche dati";

- individualmente accessibili grazie a mezzi elettronici o in altro modo.

  Quindi i dati devono essere disposti in modo da consentire all'utilizzatore di accedere ai singoli dati ed al loro insieme. In altri termini, gli elementi che compongono la banca dati (i singoli dati) devono essere indipendenti tra loro e suscettibili di avere valore ed utilità ove singolarmente considerati. Ad esempio, il requisito dell'indipendenza degli elementi di una banca dati non sussisterà laddove tra loro vi sia una correlazione stretta simile a quella esistente tra gli elementi inseriti in opere audiovisive, letterarie o musicali (laddove è la correlazione tra gli elementi che fa acquisire valore ai singoli elementi, che altrimenti sarebbero privi di valore).

  Deve, inoltre, esservi la possibilità di accedere alla singola informazione in modo diretto (mediante ricerche, indici, catalogazioni, ecc.).

Una banca dati può essere riprodotta su supporto cartaceo o su supporto elettronico o nella memoria di un elaboratore.

Una volta chiarito cosa si intenda per "banca dati" ai fini del diritto, occorre specificare che le banche dati sono riconosciute dalla legge come opera dell'intelletto meritevole della tutela prestata dal **diritto d'autore** quando la raccolta dei dati risulta dotata di originalità e creatività nella **selezione** e **disposizione** dei dati stessi.

La protezione che il diritto d'autore offre alle banche dati, infatti, riguarda la **struttura** delle banche dati e non il loro contenuto (non, quindi, i dati che sono ricompresi nel database): in altri termini, ad essere creativo ed originale deve essere la modalità di selezione, raccolta, conservazione ed organizzazione dei dati, non i dati stessi. Per stabilire se una banca dati costituisce o meno una creazione intellettuale meritevole di tutela mediante diritto d'autore occorre guardare alla originalità della scelta o della disposizione del materiale contenuto nella banca dati, e non alla qualità o al valore estetico della banca dati.

L'originalità della banca dati può risultare, dunque:

- dalla scelta dei materiali (dati) inseriti, se paragonati ad eventuali precedenti raccolte dello stesso tipo;
- dalla originale disposizione del materiale, se sistematica o metodica (se non fosse sistematica o metodica, non potremmo parlare di "banca dati", come abbiamo detto). Ad esempio, assumono importanza i collegamenti fra i dati, il loro ordine sequenziale, il loro coordinamento.

Il creatore della banca dati (il suo autore) è titolare dei diritti esclusivi di utilizzazione economica sulla banca dati stessa, tra cui:

- la riproduzione, permanente o temporanea, totale o parziale, con qualsiasi mezzo ed in ogni forma;
- la traduzione, l'adattamento, diverse disposizioni e ogni modifica;
- ogni forma di distribuzione al pubblico[2].

Spesso le banche dati sono opere "plurisoggettive", alla cui creazione collaborano normalmente più soggetti. Quindi i diritti d'autore potranno appartenere a colui che ha coordinato la realizzazione della banca dati, se opera collettiva, oppure a tutti i coautori, se opera in comunione. Potrebbe anche trattarsi di una opera derivata, frutto dell'elaborazione di banche dati preesistenti.

In termini generali, sono rare le banche dati che sono dotate della originalità e creatività sufficienti per potere essere protette mediante diritto d'autore. Il diritto (Direttiva UE 96/9/CE) ha allora creato un'altra forma di protezione per banche dati "non creative", che trova spesso applicazione alle banche dati, ossia quella del diritto sui generis del costitutore della banca dati.

Le raccolte di dati che non soddisfano i requisiti di proteggibilità necessari per il diritto d'autore (originalità e creatività nella selezione e disposizione dei dati) possono, dunque, essere protette mediante **diritto sui generis**. Si tratta di un diritto che protegge il risultato finale di un'attività che non dia vita ad un'opera dell'ingegno (che sarebbe invece protetta da diritto d'autore), ma ad un bene comunque meritevole di tutela per gli investimenti finanziari, di tempo e di lavoro che sono serviti per realizzare la banca dati. Il diritto sui generis, quindi, serve per remunerare ("ricompensare", potremmo dire) gli investimenti effettuati da chi ha realizzato la banca dati.

Il diritto sui generis non è applicabile a qualsiasi banca dati, ma è concesso solo per le banche dati che non avrebbero potuto essere ottenute, verificate o presentate senza considerevoli risorse umane, tecniche e finanziarie (tempo, lavoro, energia e denaro). Non esiste un criterio assoluto per comprendere quando l'investimento è "rilevante" e dunque la banca dati può essere tutelata mediante diritto sui generis, ma la valutazione deve essere calibrata in rapporto al settore di appartenenza, al livello degli investimenti normalmente effettuati da altri soggetti appartenenti al medesimo settore o dal medesimo soggetto per operazioni analoghe.

Il titolare del diritto sui generis è il costitutore della banca dati (in questo caso non si può parlare di "autore della banca dati"). Il costitutore della banca dati è una persona (fisica

[2] Non sono soggette ad autorizzazioni le attività di accesso o consultazione della banca dati quando abbiano esclusivamente finalità didattiche o di ricerca scientifica non svolta nell'esercizio di una impresa. Questo vale solo per l'accesso e la consultazione, non anche per le eventuali riproduzioni permanenti dell'intera o di parte della banca dati su altro supporto, per le quali occorre comunque la autorizzazione del titolare, anche se per finalità didattiche o di ricerca scientifica.

o giuridica, ma spesso giuridica) che sostiene i rilevanti investimenti (di tempo, di denaro e di lavoro) per la creazione della banca dati.

Il costitutore ha il diritto di vietare le operazioni di estrazione della totalità o di una parte sostanziale dei dati contenuti nella propria banca dati. Ha anche il diritto di vietare il reimpiego della totalità o di una parte sostanziale di tali dati, ossia ogni forma di messa a disposizione degli stessi mediante distribuzione di copie, noleggio, trasmissione, con ogni mezzo ed in ogni forma.

Il diritto sui generis del costitutore dura 15 anni, che si contano dal 1° gennaio dell'anno successivo alla data di completamento della costituzione della banca dati. Se vengono apportate al contenuto della banca dati modifiche o integrazioni sostanziali comportanti nuovi investimenti rilevanti il termine di 15 anni si può rinnovare per altri 15 anni.

Attenzione: esiste una fondamentale differenza tra la protezione della banca dati mediante diritto d'autore e mediante diritto sui generis:

- il diritto d'autore protegge **la banca dati nel suo insieme**, quale particolare "forma espressiva", ossia il modo in cui il materiale informativo è selezionato e disposto, non i dati che in essa sono contenuti;
- il diritto sui generis protegge il contenuto informativo, o meglio l'insieme dei dati contenuti nella banca dati, nella misura in cui la ricerca, la verifica e la presentazione dei dati stessi abbia richiesto un investimento rilevante.

In entrambi i casi non è, comunque, il singolo dato ad essere protetto, ma l'insieme ordinato dei dati. Quindi ogni altro soggetto può costituire una banca dati equivalente accedendo autonomamente a gli stessi dati mediante altre fonti.

La tutela delle opere multimediali: focus sulla protezione dei siti web e delle opere dell'ingegno pubblicate online

L'opera dell'ingegno multimediale è quell'opera complessa nella quale coesistono e si combinano opere di generi diversi (immagini, testi, parole, suoni) e che è fruita mediante media diversi. La coesistenza dei diversi media è resa possibile dalla traduzione delle diverse opere in un formato omogeneo, ossia quello digitale, amministrato da un software "di gestione", che ne consente anche la fruibilità da parte dell'utente. Altro elemento che contraddistingue l'opera multimediale è, infatti, la sua interattività, per la quale chi la "consulta" può muoversi all'interno dell'opera secondo associazioni predeterminate dal suo creatore o anche eventualmente introdotte dall'utente stesso (dipende da che tipo di fruibilità l'opera offre).

La legge sul diritto d'autore menziona soltanto le opere multimediali ma non esistono norme specifiche su tali opere, diverse da quelle che regolano le altre opere dell'ingegno. L'opera multimediale, in quanto prodotto "di combinazione", è quindi generalmente considerata come "opera collettiva", quindi autore dell'opera multimediale sarà colui che è il suo "assemblatore", cioè che ha reso possibile la coesistenza delle diverse parti, mentre gli autori delle singole parti continueranno ad essere considerati tali per ciascuna delle parti che compone l'opera.

Una particolare tipologia di opera multimediale è, ad esempio, il **videogioco**, che spesso costituisce un'opera collettiva, come risultato dei contributi di diversi autori che mantengono il loro diritto d'autore sulla specifica parte da loro creata (ad esempio, singoli personaggi, singoli scenari, singole ambientazioni, singole storylines, ecc.),

mentre il titolare del diritto d'autore sull'intero videogioco sul suo complesso è il soggetto che ha coordinato tutti i vari "pezzi" che lo costituiscono.

Un'altra tipologia di opera multimediale è il **sito web**, il quale è costituito da grafica, immagini, testi e suoni combinati tra di loro in modo da risultare interattivi. Il sito web è ricompreso tra le "opere dell'ingegno di carattere creativo" meritevoli di tutela mediante diritto d'autore, ammesso che abbia un grado di creatività tale da meritare tutela per le scelte estetiche e tecniche che lo contraddistinguono.

Per vedere riconosciuti e tutelati i diritti connessi al sito web, il creatore non deve presentare alcun tipo di richiesta o domanda perché tali diritti vengono acquisiti automaticamente con la creazione del sito: è sufficiente, quindi, creare un sito, un testo o una grafica frutto del proprio ingegno per diventare automaticamente l'autore ai fini giuridici ed acquisire il diritto a che nessuno possa diffondere, copiare o utilizzare quanto creato senza l'esplicito consenso dell'autore.

Il sito web è generalmente assimilato ad un'opera collettiva[3]. Pertanto:

- il programma che genera o fa funzionare il sito web è autonomamente tutelabile per chi lo ha creato;
- i diritti d'autore sulle singole parti che possono essere pubblicate su un sito web restano singolarmente di titolarità del loro autore (ad esempio, un testo letterario o un video o una canzone pubblicati su un sito web);
- la grafica del sito, il suo layout, se originale, è meritevole di tutela come qualsiasi altra immagine artistica, a prescindere dai contenuti del sito stesso[4].

  Quindi, anche se i singoli contenuti del sito web sono di per sé banali (e dunque non proteggibili mediante diritto d'autore), se l'autore del sito web li ha disposti in modo creativo ed originale il sito web può essere riconosciuto come meritevole di tutela mediante diritto d'autore.

Da un punto di vista tecnico, il **nome a dominio di un sito web** è una sequenza alfanumerica associata all'indirizzo IP che in rete identifica il computer o il server sul quale è ospitato il sito internet. Poiché è più semplice ricordare un nome rispetto ad una sequenza numerica, è stato creato il sistema DNS - Domain Name System, che ha la funzione di associare ad ogni indirizzo IP una sequenza alfanumerica, ossia il nome a dominio (è, semplificando, il nome che compare dopo www. negli indirizzi web). In termini ancor più semplici, il nome a dominio corrisponde all'"indirizzo virtuale" di una pagina web.

Per ottenere la registrazione di un nome a dominio occorre presentare apposita domanda ad una delle varie Registration Authorities, nazionali o internazionali, che operano sulla base del principio "first come, first served": il nome a dominio, infatti, previo pagamento dei diritti di registrazione, viene assegnato automaticamente al soggetto che per primo ne faccia richiesta senza alcun tipo di verifica preliminare da parte dell'autorità circa la legittimità o meno della domanda di registrazione.

Il codice della proprietà industriale italiano riconosce il nome a dominio come un segno distintivo dell'impresa, come il marchio, riconoscendo la funzione distintiva del nome a

[3] Per molto tempo si è discusso sulla possibilità di qualificare il sito web come opera collettiva, mentre alcuni autori lo assimilavano ad una banca dati. Il dibattito è, ad oggi, ancora aperto, anche se sembra preferibile optare per la tesi che assimila i siti web alle opere collettive.

[4] Naturalmente, se si utilizzano come base strutture predisposte da soggetti terzi che le concedono in licenza (ad esempio, si pensi a Wordpress), risulta carente il requisito della originalità.

dominio e la conseguente meritevolezza di tutela. Pertanto, il nome a dominio può essere legittimamente registrato solo nella misura in cui non violi il diritto sui segni distintivi spettanti ad altri soggetti (per comprendere, io non potrei registrare come mio nome a dominio la parola “Barilla”, anche se per assurdo un tale nome a dominio non fosse già registrato). In particolare, la registrazione di un nome a dominio costituisce violazione della privativa se riproduce un marchio precedentemente registrato oppure identifica un sito commerciale relativo a prodotti o servizi identici o affini, creando confusione tra gli utenti.

Se il sito web può essere di per sé oggetto di diritto d’autore e meritare protezione, il creatore di un sito può liberamente inserire nel proprio sito **link** che rinviano a contenuti di altri siti web o tale condotta costituisce violazione del diritto d’autore sul sito web al quale i link rinviano? In altri termini, l’inserimento di un link di un sito di un soggetto terzo in un proprio sito web può costituire forma di utilizzo non autorizzato dei contenuti del soggetto terzo (eventualmente tutelati mediante diritto d’autore, se opere dell’ingegno)?

Sul tema si è aperto un ampio dibattito a più livelli, sia internazionale che europeo. Secondo alcuni, i titolari di siti web, per la natura della rete, nel momento in cui rendono disponibili sul loro sito determinati contenuti ed aprono al libero accesso del pubblico le proprie pagine web, concederebbero una “implicit license to link”, ossia in modo implicito autorizzerebbero qualunque altro operatore a creare connessioni con tali materiali (salve diversa indicazione espressa in merito).

Taluni commentatori trattano anche diversamente alcune tipologie di linking:

- il surface linking, ossia l’inserimento di un link che conduca alla homepage di un altro sito web; pratica che viene ritenuta lecita;
- il deep linking, ossia l’inserimento di un link che, evitando le pagine di presentazione ed introduzione di un sito altrui, consentono di visualizzarne direttamente un determinato contenuto specifico. Alcuni manifestano perplessità sulla liceità di tale pratica, perché consentirebbe di “violare” l’ordine e la struttura di un sito pianificata da chi quel sito ha creato, alterandone anche il numero di visualizzazioni ed ingenerando anche confusione sulla paternità dei contenuti dei vari siti. Occorre comunque un’analisi caso per caso, per assicurarsi che l’inserimento di link di siti altrui in un sito web non danneggi il titolare del sito al quale si inserisce il link;
- il framing, ossia una particolare forma di deep linking con la quale viene richiamato e presentato il contenuto di un altro sito, creando una cornice grafica (frame) all’interno della quale viene poi visualizzato il contenuto presente in un altro sito. Il risultato può essere quello di ingenerare nel navigatore l’impressione che tali contenuti siano del sito che li richiama.

Su tali questioni si è pronunciata la Corte di Giustizia dell’Unione Europea (nel 2014), che ha chiarito che è lecito il rinvio mediante link a contenuti non protetti di un altro sito web. La realizzazione di un link ad un’opera protetta da diritto d’autore ma che sia liberamente accessibile in internet non costituisce, in generale, violazione del diritto d’autore del titolare dell’opera. A conclusioni diverse si dovrebbe giungere nell’ipotesi in cui un collegamento cliccabile consentisse di eludere misure restrittive adottate dal sito in cui l’opera protetta si trova per limitare l’accesso del pubblico ai soli abbonati. Rileva anche l’eventuale scopo di lucro del linking.

La tutela delle opere e delle invenzioni generate dall'A.I.: v. slide discusse a lezione e sentenza n. 1107/2023 della Corte di Cassazione

TUTELA DEL SOFTWARE: TRA DIRITTO D'AUTORE E BREVETTO

Quando un software può essere tutelato esclusivamente dal diritto d'autore e quando può essere coperto anche da brevetto

I) La tutela del software offerta dal diritto d'autore

La disciplina in materia di diritto d'autore è nata per tutelare le opere dell'ingegno c.d. "tradizionali" (letterarie e artistiche), ma è stata nel corso del tempo adattata ed integrata affinché potesse essere applicata anche alla protezione di opere dell'ingegno informatiche ed alle tecnologie emergenti, quali software, banche dati, ecc.

Nel nostro ordinamento, dunque, i programmi per elaboratore sono tutelati dalla legge sul diritto d'autore al pari delle opere letterarie, **"*in qualsiasi forma espressi, purché originali quale risultato della creazione intellettuale dell'autore*".**

A lungo tempo è prevalsa l'impostazione secondo la quale la tutela offerta al software - come particolare "forma di scrittura" e opera dell'ingegno a carattere creativo - dal diritto d'autore fosse l'unica possibile. Tale impostazione, come si dirà nel prosieguo, è stata, tuttavia, mitigata a partire da alcune pronunce dell'Ufficio Brevetti Europeo (EPO), il quale ha esteso a talune tipologie di software anche la tutela industriale.

Affinché un software possa essere tutelato da diritto d'autore, lo stesso deve presentare - al pari di qualsiasi altra opera dell'ingegno - i seguenti caratteri:

- quello della **novità**: il software deve essere sufficientemente diverso dai software precedenti;
- quello della **originalità** e della **creatività**: il software deve essere dotato di carattere creativo ed essere, dunque, originale, ossia deve costituire una individuale e personale espressione dell'idea dell'autore e non essere frutto di una mera copiatura.

L'interpretazione fornita dai giudici in relazione ai requisiti della originalità e della creatività del software è molto ampia ed in quanto tale idonea a fornire adeguata tutela ad una platea piuttosto vasta di programmi per elaboratore tra quelli che affollano il mercato. È stato, infatti, sancito che:

> «*La creatività e l'originalità sussistono anche qualora l'opera sia composta da idee e nozioni semplici, comprese nel patrimonio intellettuale di persone aventi esperienza nella materia propria dell'opera stessa,* ***purché formulate e organizzate in modo personale, e autonomo rispetto alle precedenti***» (Corte di Cassazione, 2007).

Ai fini di ricevere tutela mediante il diritto d'autore, un software deve, dunque, oltre che presentarsi come nuovo, essere, altresì, frutto di uno sforzo creativo minimo ed essere dotato di un sufficiente grado di valore aggiunto rispetto ai software precedenti.

II) La tutela brevettuale del software

Come già anticipato, i programmi per elaboratore sono qualificati dal legislatore italiano come opere creative dell'intelletto umano, e, dunque, soggette alla disciplina del diritto d'autore. Esistono, tuttavia, condizioni alle quali un software può essere anche brevettato.

I requisiti necessari per la tutela brevettuale di un software sono i medesimi richiesti per tutte le altre invenzioni, ed in particolare:

- quello della **novità**: il programma per elaboratore non deve essere mai stato prodotto o già brevettato in alcuna parte del mondo. L'accertamento di tale

requisito è svolto sulla base dello stato della tecnica al momento del deposito della domanda di brevetto;

- quello della **industrialità**: il software deve poter trovare applicazione a livello industriale;
- quello del carattere **inventivo**: il software deve non solo deve essere nuovo, ma anche risultare non banale, e, dunque, rappresentare un progresso, un passo in avanti nello sviluppo della tecnica di settore.

Ma non solo. Non è, infatti, sufficiente che il software risolva, con una soluzione innovativa e non ovvia un problema tecnico, offrendo, quindi, un contributo allo stato dell'arte della tecnica di settore. Per poter ricevere tutela brevettuale, il software deve, infatti, produrre anche un **effetto tecnico**.

Che cosa si intende per effetto tecnico?

La già richiamata impostazione secondo la quale il software può ricevere tutela esclusivamente dalla disciplina sul diritto d'autore si fonda sulla considerazione che lo stesso sia generalmente privo di funzione tecnica.

Si sono, tuttavia, registrati in ambito europeo taluni tentativi volti ad adeguare la disciplina brevettuale all'ambito del software. In particolare, lo sforzo della Commissione europea è stato diretto a risolvere i dubbi interpretativi sorti sul punto tentando di fornire definizioni univoche di "*invenzione attuata per mezzo di elaboratori elettronici*" e di "*contributo tecnico*". La proposta avanzata dalla Commissione non ha, tuttavia, superato il vaglio del Parlamento europeo.

In assenza di una espressa previsione normativa, l'estensione della tutela brevettuale al software è stata, pertanto, possibile grazie agli sforzi interpretativi messi in atto dall'Ufficio Brevetti Europeo. Pur ribadendo che software "*in quanto tale*" non può ricevere tutela industriale, lo European Patent Office ha sancito che "*un programma che presenta **effetti tecnici ulteriori o che vadano al di là della normale interazione software-hardware** non deve essere escluso dalla brevettabilità*" (Decisione EPO T1173/97).

Ogni programma per elaboratore produce un effetto tecnico tangibile, ovvero gli impulsi elettrici azionati dall'hardware, ma, ai fini della sua brevettabilità questo non è sufficiente. È, infatti, riconosciuta la brevettabilità di quelle invenzioni attuate per mezzo di elaboratori elettronici che risolvono un problema tecnico o che forniscono un contributo allo stato dell'arte in un settore tecnico**,** giudicato non ovvio da una persona competente nella materia.

L'effetto tecnico ulteriore prodotto dal programma per elaboratore può essere riscontrato:

- sia all'**interno** dell'elaboratore stesso: si tratta delle invenzioni afferenti all'architettura del programma, alle metodologie di programmazione, alla sistemistica (sistemi operativi, gestione di database, interfacce utenti) ai programmi applicativi, ecc.
- sia all'**esterno** dell'hardware mediante il quale vengono gestiti procedimenti che producono effetti tangibili non banali: si tratta dei sistemi di elaborazione e di conversione di segnali (da elettrici in elettronici, da analogici in digitali), ecc.

Alla luce di quanto detto, sono, dunque, brevettabili - perché aventi "effetto tecnico" e laddove soddisfino gli altri requisiti di novità, industrialità e carattere inventivo - ad esempio:

- i software che ottimizzano la memoria interna del computer;
- quelli che consentono una gestione oculata della carica del cellullare;

- quelli che consentono di controllare un processo industriale o il funzionamento di apparecchiature domestiche (domotica);
- quelli che fanno funzionare il navigatore GPS o gestiscono i consumi energetici di un'auto ed il sistema ABS;
- i software che consentono la compressione audio mp3 per la diffusione della musica in streaming, o quelli che permettono di ridurre la distorsione o il rumore di fondo di una registrazione audio o video;
- quelli che stanno alla base dei sistemi di crittografia delle smart card a doppia chiave, ecc.

Non sono, invece, brevettabili - in quanto privi di effetto tecnico - i software che afferiscono a metodi per lo svolgimento di attività intellettuali come, ad esempio:

- quelli che eseguono calcoli matematici;
- quelli che gestiscono la contabilità o i prodotti presenti in un magazzino;
- quelli che consentono di registrare i pazienti in un ospedale e gestire le relative cartelle cliniche;
- quelli che assistono l'utente nell'organizzazione delle attività della giornata;
- quelli che permettono di compilare la lista della spesa e gestire la dieta;
- quelli mediante i quali viene riassunto o tradotto un documento, ecc.

Anche le **app** sono brevettabili se aventi "effetto tecnico ulteriore". Sono, dunque, brevettabili le app che permettono una migliore performance del dispositivo ("effetto interno") e quelle che consentono di interagire con il mondo esterno in maniera non banale ("effetto esterno"). È l'esempio delle app mediante le quali è possibile controllare dal dispositivo l'allarme della propria abitazione, il sistema di video sorveglianza, di riscaldamento o l'impianto audio.

III) Tutela del software a doppio binario

Quanto detto in relazione alle diverse caratteristiche ed ai differenti requisiti richiesti rispettivamente per la tutela del software mediante copyright e mediante brevetto, non deve tuttavia indurre a ritenere che l'operatività di una tutela escluda l'altra. Vige, infatti, in relazione al software, un doppio binario di tutela: d'autore per la sua estensione statica di codice e brevettuale per il suo contenuto innovativo.

Come già visto, la Legge sul diritto d'autore tutela il software nella sua **forma espressiva**, "per come è scritto". Da ciò consegue che non si registra alcuna violazione del diritto d'autore nell'ipotesi in cui venga realizzato un programma che esegue la stessa funzione e risponde alla medesima esigenza, ma utilizzando un diverso codice. Dunque, se un'azienda concorrente progetta un software che realizza lo stesso risultato mediante un diverso codice sorgente, tale azienda non viola il diritto d'autore di quella che per prima aveva progettato quel software.

Il diritto d'autore fornisce, pertanto, una buona tutela, ma piuttosto limitata e non sempre soddisfacente, soprattutto in considerazione di quelli che sono gli investimenti che stanno alla base della progettazione e della realizzazione di un software, nonché i risvolti economici della sua commercializzazione.

Il brevetto, invece, tutela tutte le funzioni del software, cioè sia **come funziona**, sia **il suo risultato**. La tutela brevettuale è, dunque, più ampia, e, generalmente, preferibile, rispetto

a quella fornita dal diritto d'autore, proprio perché "protegge" il software indipendentemente dal codice in cui lo stesso è stato scritto.

Si è detto, tuttavia, che non sempre è possibile ottenere questa più ampia tutela fornita dal brevetto: se, infatti, il software è originale - oltre che creativo e nuovo - ma non ha "effetto tecnico" o non risolve un problema tecnico, questo potrà essere tutelato esclusivamente dal diritto d'autore.

Esclusa tale ipotesi, come anticipato, la tutela del diritto d'autore e quella brevettuale possono anche **coesistere**, in quanto forme di tutela rivolte a proteggere caratteristiche e funzionalità diverse di uno stesso programma. In relazione ad un medesimo software si potrà, infatti, sia depositare apposita domanda di brevetto presso l'Ufficio Italiano Brevetti e Marchi (cui seguiranno, prima che sia eventualmente concesso il brevetto, le fasi della segretezza, dell'esame preliminare, della ricerca dell'anteriorità e dell'esame di merito), sia - ma non necessariamente - depositare il software presso la SIAE (in particolare presso il Pubblico Registro per il Software, tenuto dalla SIAE), al fine di ottenere quantomeno una prova "documentata" dell'esistenza del software e dell'identità di chi lo ha creato.

****

Acquisiti gli strumenti basilari, sufficienti a dare quantomeno risposta alla generale domanda "quando un software può essere tutelato esclusivamente dal diritto d'autore e quando può essere coperto anche da brevetto", occorre, tuttavia, considerare come l'enorme varietà di software che si affacciano quotidianamente sul mercato possa rendere l'indagine infinitamente più complessa di quella che può essere facilmente svolta in relazione agli esempi forniti in questa sede. La tecnicità del requisito dell'"effetto - appunto - tecnico ulteriore" richiesto per la brevettabilità di un software impone, infatti, il coinvolgimento - oltre che di un legale - anche di un esperto del settore in grado di accertare se il software in relazione al quale si intende depositare la domanda di brevetto sia effettivamente idoneo a risolvere un problema tecnico o a fornire un contributo allo stato dell'arte o meno.