

Diritto dei Prodotti Digitali

Il **diritto dei prodotti digitali** riguarda tutte le norme che regolano la creazione, la distribuzione e l'uso di prodotti digitali, come software, app, e contenuti online. Ad esempio, quando si acquista un software, si sottoscrive una licenza d'uso, non si possiede il software stesso. Le leggi sul diritto d'autore proteggono chi crea il software, mentre le norme sulla privacy proteggono i dati degli utenti che utilizzano quel software.

Nome a Dominio (DNS - Domain Name System)

Un **nome a dominio** è l'indirizzo che identifica un sito web su Internet. Ad esempio, "google.com" è il nome a dominio di Google. Questo nome è parte del **Domain Name System (DNS)**, che traduce nomi di dominio come "google.com" in indirizzi IP numerici, rendendo possibile l'accesso ai siti web.

Nuovo scenario (dagli anni '60 a oggi)

Dagli anni '60, con la nascita di internet, è diventato necessario un sistema per identificare univocamente i computer collegati in rete. Oggi, ogni sito web ha un nome a dominio che lo rende unico e facile da ricordare. Ad esempio, il sito del governo italiano è identificato come "gov.it".

Indirizzo identificativo di un sito internet

Il nome a dominio è essenziale per l'identità di un sito web, come un marchio lo è per un'azienda. Ad esempio, "amazon.com" non è solo un indirizzo, ma anche un marchio potente che rappresenta un'azienda globale.

Funzione del DNS

Il DNS permette di usare nomi semplici al posto di complicati numeri IP. Ad esempio, anziché digitare "172.217.16.195", gli utenti possono semplicemente scrivere "google.com" per accedere al sito di Google.

Mancanza di definizione normativa

In Italia, non c'è ancora una definizione legale precisa per i nomi a dominio. Tuttavia, essi funzionano come un "indirizzo alfanumerico" che identifica un computer in rete. Ad esempio, se una persona cerca "universita.it", il DNS lo indirizzerà al sito corrispondente.

Composizione dei Nomi a Dominio

I nomi a dominio sono composti da più parti, ciascuna con una funzione specifica.

1. Primo livello (Top-Level Domain - TLD)

- Il **TLD** è la parte finale del nome a dominio, come ".com", ".it", o ".org". Ad esempio, ".it" in "unifi.it" indica che il sito appartiene a un dominio italiano.

2. Secondo livello (Second-Level Domain - SLD)

- Il **SLD** è la parte che precede il TLD ed è scelto dall'utente. Per esempio, in "facebook.com", "facebook" è il SLD, scelto dall'azienda Facebook.

La registrazione di un nome a dominio come "pizza.com" è unica, nessun altro può usarlo, e può essere soggetta a restrizioni se include nomi geografici o istituzionali riservati.

Disciplina e Regolamentazione

La registrazione e gestione dei nomi a dominio sono regolamentate da normative specifiche. Ad esempio, per registrare un dominio ".it", esistono regole che stabiliscono la lunghezza del nome e i caratteri utilizzabili. Solo i domini di secondo livello vengono registrati; eventuali sottodomini, come "shop.amazon.com", sono creati dall'amministratore del sito.

Un nome a dominio come "apple.com" è protetto allo stesso modo di un marchio, e le autorità, come l'ICANN, garantiscono che la registrazione e l'uso siano gestiti correttamente, rispettando la libertà di comunicazione e l'interoperabilità dei servizi internet.

Casi Omonimia

- es. Armani (giudizio negativo per il sig. L. Armani produttore di timbri –Italia) -non è stato applicato il first come first served è stata scelta la regolamentazione indicata dai codici di condotta
- A.R. Mani (giudizio positivo per il sig. A.R. Mani - USA) - è stato applicato il first come first served
- Gente.it ricorrente Rusconi editore –ricorso 2001 per la rivista Gente
- Caso Mediaset - Trib. Roma 12.06.2012

- Assegnazione - Register – Registrar
- Natura giuridica
- Bene (art. 810 c.c., 814 c.c.)
- ND aziendale (art. 2, co. 5 cpi -22 cpi)
- Tutela (art. 133 cpi)
- Diritto al nome
- Tutela (art. 7 c.c.)
- Tutela segni distintivi

Piattaforme Digitali

Le **piattaforme digitali** sono infrastrutture online che permettono l'interazione tra fornitori e consumatori. Ad esempio, Amazon è una piattaforma di incontro dove gli utenti possono acquistare beni e servizi. Invece, Facebook è una piattaforma per l'attenzione, dove gli utenti accedono gratuitamente ai contenuti, ma i loro dati vengono raccolti per scopi pubblicitari.

Scopo delle Piattaforme

Queste piattaforme mirano a orientare il comportamento degli utenti, raccogliendo dati e imponendo condizioni standard per l'uso dei servizi. Dato il loro impatto globale, come nel caso di Google, che opera in tutto il mondo, è necessaria una regolamentazione internazionale per garantire equità e tutela dei consumatori.

Regolamentazione Europea delle Piattaforme Digitali

L'Unione Europea ha introdotto leggi per regolamentare le attività delle piattaforme digitali:

1. Direttiva 2018/1808/UE (Media Audiovisivi)

- Regola contenuti audiovisivi e piattaforme come YouTube, proteggendo i minori da contenuti inappropriati. Ad esempio, i video su YouTube devono rispettare certe linee guida per essere accessibili ai bambini.

2. Regolamento UE 2019/1150 (Platform to Business)

- Assicura trasparenza tra le piattaforme online e le aziende che le utilizzano. Ad esempio, impedisce ad Amazon di favorire i propri prodotti a scapito di quelli di terzi venditori sulla piattaforma.

3. Regolamento UE 2022/2065 (Digital Services Act - DSA)

- Stabilisce norme per la sicurezza online e la gestione dei contenuti illeciti. Ad esempio, Facebook deve rimuovere contenuti che promuovono il terrorismo o l'odio.

4. Regolamento UE 2022/1925 (Digital Markets Act - DMA)

- Prevede regole per evitare che grandi piattaforme, come Google, abusino del loro potere di mercato. Ad esempio, Google non può imporre l'uso del proprio motore di ricerca come predefinito sui dispositivi Android senza offrire alternative.

Soggetti Giuridici del Contratto Digitale

I **contratti digitali** coinvolgono principalmente il consumatore e il professionista. Ad esempio, quando si acquista un'app su Google Play, si accetta un contratto digitale con il fornitore dell'app. Questo contratto,

regolato dal Codice Civile Italiano, si conclude quando entrambe le parti accettano i termini proposti, come il prezzo e le condizioni d'uso.

Normativa

art. 13 d. lgs 9 aprile 2003 n. 70

Le norme sulla conclusione dei contratti si applicano anche nei casi in cui il destinatario di un bene o di un servizio della società dell'informazione inoltri il proprio ordine per via telematica.

Salvo differente accordo tra parti diverse dai consumatori, il prestatore deve, senza ingiustificato ritardo e per via telematica, accusare ricevuta dell'ordine del destinatario contenente un riepilogo delle condizioni generali e particolari applicabili al contratto, le informazioni relative alle caratteristiche essenziali del bene o del servizio e l'indicazione dettagliata del prezzo, dei mezzi di pagamento, del recesso, dei costi di consegna e dei tributi applicabili.

art. 13 d.lgs 9 aprile 2003 n. 70

L'ordine e la ricevuta si considerano pervenuti quando le parti alle quali sono indirizzati hanno la possibilità di accedervi.

Le disposizioni di cui ai commi 2 e 3 non si applicano ai contratti conclusi esclusivamente mediante scambio di messaggi di posta elettronica o comunicazioni individuali equivalenti.

Che incidenza hanno sulle norme del c.c. quelle peculiari contenute nell'art. 13, 70/2003

E cioè

1. Onere di accusare ricevuta dell'ordine
2. Ordine e ricevuta si considerano pervenuti se accessibili

Il contratto online

1. Non incide sulla formazione del contratto
2. Integra un'informazione negoziale

Diritti della Personalità in Rete

I **diritti della personalità** in ambito digitale proteggono aspetti come l'identità personale e la reputazione online. Ad esempio, se una foto di una persona viene alterata e pubblicata online in modo che distorca la sua identità, quella persona ha il diritto di chiedere la rimozione della foto e il risarcimento per i danni subiti.

Accordo Digitale e Contratto Telematico: Aspetti Normativi e Tutela dei Consumatori

Il panorama dei contratti digitali, compresi quelli telematici, rappresenta un campo di crescente rilevanza giuridica. Questi contratti, conclusi ed eseguiti attraverso la rete, pongono diverse sfide normative e interpretative, specialmente considerando la "metaterritorialità" di Internet e la necessità di una cyber law che coordini le norme dei diversi ordinamenti nazionali.

1. Accordo Digitale e Disciplina Applicabile

- La conclusione di un contratto digitale presenta incertezze legate alla modalità di perfezionamento tra parti assenti e in contesti transnazionali. Questo richiede l'integrazione di una disciplina generale con regole specifiche di settore, spesso definite dalla normativa europea e italiana.
- **Esempio:** Un'azienda italiana che vende software a clienti in vari paesi dell'UE deve rispettare non solo le normative nazionali, ma anche il **Digital Services Act (DSA)**, che impone trasparenza e tracciabilità nelle operazioni commerciali, specialmente per i fornitori di piattaforme online.

2. Contratto Digitale: Normativa di Riferimento

- La libera circolazione dei servizi dell'informazione e il commercio elettronico sono regolati dal D. Lgs. 70/2003, che recepisce la Direttiva 2000/31/CE sul commercio elettronico. Questo decreto disciplina, tra l'altro, l'inoltro dell'ordine e i requisiti formali dei contratti telematici.
- **Esempio:** Prima di concludere un contratto online, il professionista deve fornire al consumatore informazioni chiare e comprensibili sui principali termini del contratto, come previsto dall'art. 49 del Codice del Consumo. Se un sito di e-commerce omette di informare adeguatamente il consumatore sul diritto di recesso, potrebbe trovarsi in violazione di tale normativa.

3. Tutela del Cyber-Consumatore

- La protezione del consumatore digitale è centrale, con regolamenti come il **Regolamento 302/2018/UE** che vieta il geoblocking e altre discriminazioni basate sulla nazionalità. Inoltre, il pacchetto normativo ADR/ODR prevede piattaforme digitali per la risoluzione delle controversie derivanti da contratti online.
- **Esempio:** Se un consumatore tedesco acquista un bene su un sito italiano ma si vede bloccato l'accesso a certe offerte a causa della sua residenza, questo potrebbe costituire una violazione del divieto di geoblocking.

4. Informazione Precontrattuale e Requisiti Formali

- La normativa italiana prevede obblighi precontrattuali di informazione (art. 49 c. cons.) e requisiti formali specifici per i contratti telematici (art. 51 c. cons.). Questi includono, ad esempio, l'obbligo di fornire un riepilogo dettagliato delle condizioni contrattuali prima della conclusione del contratto.
- **Esempio:** Un e-commerce deve chiarire in modo evidente che l'ordine implica un obbligo di pagamento, pena la non vincolatività del contratto (art. 51, co. 2, c. cons.). Questo include anche la visibilità chiara delle informazioni sul prezzo totale, durata minima degli obblighi, diritto di recesso, ecc.

5. Conclusione del Contratto Digitale

- I contratti digitali possono essere conclusi secondo diversi schemi, come l'offerta al pubblico (art. 1336 c.c.) o il comportamento concludente (art. 1327 c.c.).
- **Esempio:** Nel caso di un contratto di e-commerce, il consumatore accetta l'offerta cliccando su un pulsante che conclude il contratto (schema "point and click"). Qui, il contratto è considerato concluso quando l'accettazione è conoscibile dal proponente, ad esempio tramite una notifica di conferma via email.

6. Tutela dei Consumatori Vulnerabili

- La normativa europea pone particolare attenzione alla protezione dei consumatori vulnerabili, come definiti dalla Direttiva 2005/29/CE. Questa protezione è necessaria per evitare lo sfruttamento attraverso pratiche commerciali sleali, come il design manipolativo delle interfacce digitali (es. "dark pattern").
- **Esempio:** Un consumatore anziano potrebbe essere particolarmente vulnerabile a pratiche commerciali scorrette come il design ingannevole di pulsanti per l'iscrizione a servizi, che rendono difficile la cancellazione.

7. Differenze tra Contratti Digitali e Telematici

- I contratti digitali includono una vasta gamma di accordi, dai contratti telematici, che possono riguardare beni fisici acquistati online ma consegnati offline, ai contratti per la fornitura di contenuti digitali, come file musicali o software scaricabili.
- **Esempio:** L'acquisto di un software tramite download è un tipico contratto di e-commerce diretto, mentre l'acquisto di un libro online, consegnato poi fisicamente, rappresenta un e-commerce indiretto.

Il caso Veronesi

- La Cassazione stabilisce che il diritto è stato violato e che “ciascun soggetto ha interesse, ritenuto generalmente meritevole di tutela giuridica virgola di essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale generale o particolare, è conosciuta o poteva essere conosciuta con l'applicazione dei criteri della normale diligenza e della buona fede soggettiva.
- Il medico ha interesse a non vedere all'esterno che venga alterata travisata offuscata contestata la propria identità e il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico professionale ecc e quindi ad essere considerato nel modo che più lo rappresentava nel proprio ambiente sociale”.
-
- il problema della tutela l'identità personale man mano diventa sempre più un problema ampio e di massa. Questo problema è diventato molto più ampio proprio con l'inizio dell'era digitale e con la quantità di informazione di dati che circolano nella rete punto
- Ecco perché l'identità personale deve sempre essere considerata soprattutto adesso che c'è la rete sia a livello identificativo sia a livello identitario.

Successione Digitale

1. Dati Digitali

I dati digitali, come foto, documenti e account online, possono avere una durata potenzialmente illimitata e spesso sopravvivono alla vita del loro creatore. Questo crea il problema della successione o trasferimento dei dati agli eredi dopo la morte del titolare. In alcuni casi, i «congiunti» possono richiedere il diritto di accesso a questi dati, soprattutto se ci sono ragioni familiari che lo giustificano.

Esempio: Immaginiamo un account di posta elettronica che contiene anni di corrispondenza personale e professionale. Alla morte del titolare, gli eredi potrebbero voler accedere a queste informazioni per gestire questioni in sospeso o per conservare ricordi preziosi.

2. Trasmissione Ereditaria dei Dati

Il concetto di «eredità digitale» si riferisce alla trasmissione dei dati digitali agli eredi. I «congiunti» possono avere un diritto personale (iure proprio) di accedere ai dati digitali del defunto, come le password di accesso agli account, che possono essere ottenute dai gestori delle piattaforme.

Esempio: Alla morte di una persona, i figli potrebbero richiedere l'accesso alle foto e ai documenti salvati nel cloud del defunto, utilizzando le password fornite dai gestori del servizio.

3. Identità Digitale

L'identità digitale rappresenta la presenza online di una persona, che può continuare ad esistere anche dopo la morte del titolare dei dati. Questo fenomeno porta alla creazione di «zombie digitali» o «cimiteri digitali», in cui profili social e altri account online continuano ad esistere senza che il proprietario sia più in vita.

Esempio: Un profilo Facebook potrebbe rimanere attivo per anni dopo la morte del titolare, diventando un luogo di commemorazione o rimanendo semplicemente inattivo, contribuendo così alla presenza di «zombie digitali».

4. Capacità Digitale

La capacità digitale di una persona, cioè la sua capacità di agire online, può essere distinta dalla capacità di agire nella vita reale. In molti paesi, l'età minima per accedere a determinati servizi online è diversa da quella richiesta per compiere atti legali nella vita reale.

Esempio: Negli Stati Uniti, un minore di 13 anni può creare un account su un social network, mentre in Italia l'età minima è 14 anni. Questo crea una discrepanza tra la «capacità digitale» e la capacità legale di agire nella vita reale.

5. Dati Post Mortem

Esiste una discussione sul diritto alla privacy dei dati personali dopo la morte. Con la morte del titolare, i dati generati digitalmente possono essere conservati su vari supporti, ma si pone la questione della loro durata, conservazione e del rischio di obsolescenza tecnologica.

Esempio: Documenti conservati in formato digitale potrebbero non essere più accessibili in futuro a causa dell'obsolescenza dei dispositivi o software necessari per leggerli, portando alla perdita di intere «generazioni» di dati.

6. Eredità Digitale Iure Successionis

L'ereditarietà digitale implica la conservazione e la trasmissione dei dati come parte del patrimonio del defunto. I dati personali possono essere considerati beni trasmissibili secondo le regole della successione ereditaria, e può essere predisposto un «testamento digitale» per specificare il destino di tali beni.

Esempio: Un individuo può designare una persona di fiducia a cui lasciare le password dei propri account, tramite un legato di password, garantendo la trasmissione dei dati agli eredi o per specifici scopi post mortem.

7. Altri Ordinamenti

Le leggi e le prassi sulla successione digitale variano notevolmente da paese a paese. Negli Stati Uniti, l'accesso agli account di un defunto è generalmente negato, a meno che non ci sia un consenso esplicito del titolare prima della morte o un ordine della corte. In Francia, invece, le clausole di intrasferibilità dei dati digitali sono inefficaci, e gli eredi hanno il diritto di accesso se il defunto non ha disposto diversamente.

Esempio: Nel caso di Marsha Mehran, una scrittrice deceduta, Google ha rifiutato l'accesso diretto all'account Google Drive richiesto dai genitori, ma ha consegnato una copia dei documenti su supporto digitale.

Francia

Nel 2016, la Francia ha introdotto una normativa specifica riguardante le successioni digitali, stabilendo importanti principi per la gestione dei dati digitali dopo la morte del titolare. Questa normativa ha reso inefficaci le clausole di intrasferibilità dei dati digitali, permettendo agli eredi di accedere ai dati del defunto, a meno che quest'ultimo non abbia disposto diversamente.

Principali Disposizioni:

- **Diritto di Disposizione Post Mortem:** Il titolare dei dati ha il diritto di decidere, tramite direttive generali o specifiche, come debbano essere trattati i suoi dati digitali dopo la sua morte. Questo può includere la possibilità di consentire l'accesso agli eredi o di designare un esecutore per gestire tali dati.
- **Non Trasmissibilità di Certi Contenuti:** Non tutti i contenuti digitali sono trasmissibili. Ad esempio, i diritti su servizi o contenuti digitali acquistati dal defunto, come collezioni di film o licenze software, non possono essere ereditati dagli eredi.
- **Testamento Digitale:** Il titolare può redigere una sorta di testamento digitale per definire le direttive sui dati personali, come la consegna a terzi o la designazione di un esecutore delle volontà digitali. Queste direttive sono modificabili e revocabili.
- **Accesso Limitato per i Familiari:** Se il defunto non ha lasciato specifiche disposizioni, i familiari hanno comunque un diritto limitato di accesso ai dati, funzionale soprattutto alla determinazione dell'asse ereditario e alla gestione di eventuali «ricordi di famiglia», come fotografie salvate in cloud.

Esempio:

Se una persona deceduta aveva salvato molte foto di famiglia su un servizio di cloud, gli eredi, in assenza di altre disposizioni, possono accedervi per preservare questi ricordi, anche se non possono ereditare le licenze software acquistate.

Germania

In Germania, non esiste una normativa specifica che regoli la successione digitale. Tuttavia, la gestione del patrimonio digitale è disciplinata dalle leggi generali sull'eredità.

Caso Rilevante:

Un caso emblematico ha riguardato l'accesso dei genitori all'account Facebook della loro figlia deceduta. In questo caso, i genitori hanno chiesto di accedere all'account per comprendere i propositi della figlia prima della sua scomparsa.

- **Modalità Commemorativa:** Facebook aveva posizionato l'account della ragazza in modalità commemorativa, negando l'accesso ai genitori ai contenuti del profilo.
- **Decisione Giudiziaria:** La corte tedesca ha accolto la richiesta dei genitori, stabilendo che, alla morte del titolare di un account di social networking, il contratto si trasmette agli eredi, che quindi hanno diritto di accesso ai dati contenuti nell'account. Questo diritto di accesso è stato riconosciuto anche in considerazione della tutela post mortem della personalità e della protezione dei dati della ragazza.

Esempio:

In questo contesto, i genitori di una ragazza deceduta hanno potuto accedere al suo account Facebook per leggere i suoi messaggi privati e comprendere meglio i suoi ultimi pensieri, nonostante l'account fosse stato messo in modalità commemorativa.

Italia

In Italia, il diritto di accesso ai dati personali del defunto è regolato dall'art. 9, co. 3 del Codice della Privacy e dal GDPR. Questo diritto è riconosciuto ai congiunti che ne fanno richiesta per ragioni familiari meritevoli di protezione.

Principali Disposizioni:

- **Esercizio dei Diritti sui Dati del Deceduto:** I diritti sui dati personali del defunto possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, come un mandatario o un familiare con ragioni meritevoli di protezione.
- **Accesso ai Dati Personali:** I congiunti del defunto hanno il diritto di accedere ai dati personali e agli account di posta elettronica, social network e servizi di messaggistica del defunto, soprattutto se esiste il pericolo che tali dati vengano cancellati dopo la morte del titolare.
- **Modello di Accesso Italiano:** Il modello italiano tende a favorire il «diritto di accesso» dei congiunti ai dati personali del defunto, a meno che quest'ultimo non abbia disposto diversamente in modo valido.

Criticità:

- **Accesso Indiscriminato:** Esiste il rischio che i familiari possano accedere indiscriminatamente ai dati personali del defunto, senza un adeguato approfondimento sulle reali ragioni di tutela.
- **Privacy dei Terzi:** La privacy dei terzi coinvolti potrebbe essere compromessa, specialmente se le informazioni contenute nei dati personali del defunto riguardano anche altre persone.
- **Effetti Irreversibili:** La comunicazione delle password del defunto ai familiari può avere effetti irreversibili, e spesso queste decisioni vengono prese senza una valutazione approfondita del caso.

Esempio:

Dopo la morte di una persona, i familiari possono richiedere l'accesso al suo account di posta elettronica per recuperare informazioni importanti, ma questa operazione può mettere a rischio la privacy delle persone con cui il defunto aveva corrisposto.

Criticità Generali delle Piattaforme Online

Molte piattaforme online, come Facebook, Dropbox, Microsoft e altri, hanno adottato soluzioni diverse per la gestione degli account inattivi o appartenenti a persone decedute.

- **Facebook:** Consente agli eredi di nominare un gestore per l'account commemorativo o di far eliminare l'account in modo permanente. Se non viene fatta alcuna scelta, l'account viene posto in modalità commemorativa.
- **Dropbox e Altri Servizi:** In caso di inattività prolungata, gli account vengono cancellati o messi in uno stato di quiescenza. I dati possono essere recuperati solo se l'account viene riattivato entro un certo periodo.

Esempio:

Se un account Dropbox rimane inattivo per un lungo periodo, i dati potrebbero essere cancellati automaticamente. Tuttavia, se l'account viene riattivato entro un certo lasso di tempo, è possibile recuperare i file prima che vengano eliminati definitivamente.

Disciplina e Perfezionamento del Contratto Digitale: Aspetti Normativi e Criticità

Accordo Digitale: Disciplina e Incertezze

Il contratto digitale, o "accordo digitale", solleva numerose questioni giuridiche, specialmente riguardo alla disciplina applicabile e alle incertezze derivanti dalla sua natura transnazionale e dalla modalità di perfezionamento tra "absentes" (parti non presenti nello stesso luogo fisico). La "metaterritorialità" della rete Internet richiede l'adozione di una c.d. **cyber law**, ovvero un insieme di normative specifiche che possano coordinarsi efficacemente con le discipline dei singoli ordinamenti giuridici nazionali.

Il perfezionamento di un contratto digitale avviene seguendo le regole generali del diritto contrattuale, integrate da normative specifiche di settore e dalla normativa italo-europea, che offrono una protezione particolare al contraente debole, il cosiddetto "cyber-consumatore".

Contratto Digitale e Libera Circolazione dei Servizi

Il contratto digitale è regolato, tra gli altri, dal D.lgs 70/2003, che recepisce la Direttiva 2000/31/CE sul commercio elettronico. Tale normativa promuove la libera circolazione dei servizi della società dell'informazione, garantendo che il commercio elettronico possa svolgersi senza barriere tra gli Stati membri dell'Unione Europea.

Per gli aspetti non disciplinati dal Codice del Consumo, come ad esempio l'**inoltro dell'ordine**, si applicano le disposizioni del D.lgs 70/2003. Inoltre, gli obblighi di informazione precontrattuale, previsti dall'art. 49 del Codice del Consumo, e i requisiti formali dell'art. 51 del medesimo codice regolano la formazione del contratto telematico, garantendo trasparenza e comprensibilità per il consumatore.

Tutela del Cyber-Consumatore e Normative Specifiche

Il cyber-consumatore è particolarmente tutelato attraverso normative europee come il **Regolamento 2018/302/UE** sul geoblocking, che vieta blocchi geografici e discriminazioni basate sulla nazionalità, assicurando così un accesso equo ai servizi online. Inoltre, il sistema di rimedi previsto dal pacchetto normativo ADR/ODR facilita la risoluzione delle controversie tra consumatori e fornitori digitali attraverso piattaforme online dedicate.

Il **Digital Services Act (DSA)** introduce ulteriori obblighi per i fornitori di piattaforme online, specialmente per quanto riguarda la trasparenza e la tracciabilità delle operazioni commerciali, e impone specifici obblighi aggiuntivi a tali fornitori quando permettono ai consumatori di concludere contratti a distanza con operatori commerciali.

Contratti B2B e Autoregolamentazione

Nel contesto dei contratti digitali tra imprese (B2B) o tra professionisti, si osserva una tendenza verso l'autoregolamentazione, spesso mediante accordi quadro stabiliti dalle associazioni di categoria. Questi contratti si basano su principi di libertà contrattuale, con le parti che definiscono autonomamente i termini e le condizioni applicabili.

Informazione Precontrattuale e Requisiti Formali

Gli obblighi di informazione precontrattuale sono fondamentali nel contesto dei contratti digitali. Il D.lgs 70/2003 e il D.lgs 21/2014, che attua la Direttiva 2011/83/UE, stabiliscono che il cyber-fornitore deve fornire informazioni chiare e dettagliate al consumatore, comprese quelle relative alle funzionalità del contenuto digitale e alle misure di protezione tecnica applicabili.

In particolare, l'art. 51 del Codice del Consumo disciplina l'**inoltrò dell'ordine**, richiedendo che le informazioni siano fornite in modo comprensibile e adeguato per evitare le cosiddette **"internet cost traps"**, ovvero modalità ingannevoli di commercializzazione che possono confondere il consumatore riguardo ai costi reali del servizio o del prodotto.

Conclusione del Contratto Digitale: Modalità e Momento di Perfezionamento

Il perfezionamento del contratto digitale segue differenti schemi giuridici, a seconda delle modalità di interazione tra le parti:

1. **Schema Tradizionale (artt. 1326 e 1335 c.c.):** Questo schema si applica alle negoziazioni individualizzate, ad esempio via e-mail, dove proposta e accettazione avvengono tra soggetti determinati. Il contratto si perfeziona quando l'accettazione diventa conoscibile dal destinatario, ovvero quando arriva al suo domicilio informatico.
2. **Offerta al Pubblico (art. 1336 c.c.):** Questo schema è tipico del commercio elettronico, dove il consumatore aderisce a una proposta predefinita tramite un'azione specifica come il **point and click**. L'accettazione avviene mediante la compilazione di un modulo online predisposto dal professionista.
3. **Comportamento Concludente (art. 1327 c.c.):** Il contratto si considera concluso nel momento e nel luogo in cui l'esecuzione della prestazione ha inizio, senza una preventiva risposta, purché l'esecuzione sia conforme alla proposta e vi sia pronto avviso dell'avvenuta esecuzione.

In tutti questi schemi, la conclusione del contratto avviene quando l'accettazione perviene al domicilio informatico del destinatario, che è considerato raggiunto anche se il destinatario non ha ancora effettivamente preso conoscenza dell'accettazione stessa.

Aspetti Critici e Necessità di Ulteriori Regolamentazioni

Nonostante le normative esistenti, il panorama giuridico dei contratti digitali presenta ancora criticità, soprattutto in termini di protezione del consumatore e chiarezza normativa. La **necessità di una maggiore trasparenza** nelle transazioni digitali e la **protezione del cyber-consumatore** richiedono continui aggiornamenti legislativi e l'implementazione di normative più rigorose che possano prevenire abusi e garantire la sicurezza delle transazioni online.

I Soggetti Giuridici del Contratto Digitale

Nel contesto del contratto digitale, i principali soggetti giuridici sono il **consumatore** e il **professionista**. La qualificazione di questi soggetti è fondamentale per la corretta applicazione delle norme di tutela e per la determinazione degli obblighi e dei diritti che sorgono dall'accordo contrattuale.

Il Consumatore

Il **consumatore** è definito come la persona fisica che agisce per scopi estranei alla propria attività imprenditoriale o professionale. Il Codice del Consumo, nel delineare i diritti e le protezioni accordate al consumatore, riconosce la sua posizione di debolezza contrattuale rispetto al professionista. La tutela del consumatore si estende non solo al momento della conclusione del contratto, ma anche alle fasi precontrattuali e post-contrattuali, assicurando che egli sia adeguatamente informato e protetto contro pratiche sleali o ingannevoli.

Il Professionista

Il **professionista**, d'altra parte, è la persona fisica o giuridica che agisce nell'ambito della propria attività commerciale, industriale, artigianale o professionale. Nel contesto del contratto digitale, il professionista è tenuto a rispettare una serie di obblighi informativi e formali, volti a garantire che il consumatore sia pienamente consapevole delle condizioni contrattuali e dei propri diritti.

Qualificazione e Protezione

La **qualificazione** dei soggetti come consumatori o professionisti ha un impatto significativo sulla normativa applicabile. Il Codice del Consumo distingue tra il **consumatore medio**, definito dalla Direttiva 2005/29/CE come un soggetto "normalmente informato, ragionevolmente attento e avveduto", e il **consumatore vulnerabile**, che, a causa di specifiche caratteristiche personali (come l'età, la salute mentale o fisica), può essere più suscettibile a pratiche commerciali sleali. In quest'ultimo caso, la normativa europea e italiana prevede forme di tutela rafforzata per prevenire lo sfruttamento di tali vulnerabilità.

Conclusione del Contratto Digitale

La **conclusione del contratto digitale** avviene attraverso tecniche di comunicazione a distanza, spesso senza la presenza fisica dei contraenti (c.d. **contratto inter absentes**). I contratti digitali possono essere di vario tipo, includendo accordi B2C (Business to Consumer), B2B (Business to Business), e P2P (Peer to Peer). La protezione del consumatore, soprattutto in ambito B2C, è garantita da una serie di norme che disciplinano le modalità di conclusione del contratto, i requisiti informativi precontrattuali, e il diritto di recesso.

Contrattazioni Elettroniche e Tutela dei Soggetti nel Mercato Digitale

Le **contrattazioni elettroniche** rappresentano una categoria di accordi caratterizzati dall'uso di strumenti tecnologici per la loro conclusione ed esecuzione. Questi contratti, regolati dal D. lgs. 70/2003 (che recepisce la Direttiva 2000/31/CE sul commercio elettronico), includono diverse tipologie di transazioni, dalle vendite di beni fisici a quelle di contenuti digitali.

Protezione del Consumatore e del Contraente Debole

La **protezione del consumatore** nelle contrattazioni elettroniche si concentra su diversi aspetti, tra cui l'obbligo del professionista di fornire informazioni chiare e complete prima della conclusione del contratto, e l'adozione di misure contro le pratiche commerciali sleali. Un esempio emblematico è il divieto di **geoblocking**, regolato dal Regolamento (UE) 2018/302, che mira a prevenire discriminazioni basate sulla nazionalità o sulla residenza del consumatore.

Il **Digital Service Act (DSA)** introduce ulteriori obblighi per i fornitori di piattaforme online, con l'obiettivo di garantire la trasparenza e la tracciabilità delle operazioni commerciali, e di proteggere i consumatori nelle transazioni a distanza.

Informazione Precontrattuale e Requisiti Formali

Gli **obblighi informativi precontrattuali** sono essenziali per assicurare che il consumatore possa prendere decisioni consapevoli. Il Codice del Consumo e il D. lgs. 70/2003 delineano le informazioni che il professionista deve fornire, incluse le caratteristiche essenziali del bene o servizio, il prezzo totale, e le condizioni di recesso. In particolare, l'articolo 51 del Codice del Consumo richiede che l'ordine del consumatore sia chiaro e comprensibile, prevenendo così pratiche ingannevoli come le **internet cost traps**.

Conclusione del Contratto e Obblighi delle Parti

La **conclusione del contratto digitale** avviene secondo diverse modalità, come il **point and click**, dove il consumatore accetta i termini del contratto attraverso un'azione specifica (es. cliccare su un pulsante). In altri casi, il contratto può essere concluso attraverso comportamenti concludenti, dove l'accettazione è implicita nell'azione del consumatore.

Il contratto digitale genera **effetti obbligatori** e, in alcuni casi, reali, imponendo alle parti il rispetto delle obbligazioni assunte. In conformità con l'articolo 1372 c.c., il contratto ha forza di legge tra le parti, e il mancato rispetto delle obbligazioni può comportare conseguenze legali.

Specificità del Contratto Digitale

Il **contratto digitale** rappresenta una categoria eterogenea che include tutti gli accordi conclusi o eseguiti attraverso il web o altre tecnologie digitali. Questi contratti possono essere suddivisi in:

- **Contratti telematici:** riguardano beni materiali o digitali venduti online, ma con esecuzione offline.
- **Contratti di fornitura di contenuto digitale:** interamente eseguiti online, come il download di file o servizi digitali.
- **Cyber contratti e contratti automatici:** conclusi attraverso apparecchi automatici o sistemi digitali.

Questi contratti sollevano questioni di **metaterritorialità**, richiedendo un coordinamento tra le normative nazionali e la creazione di un quadro giuridico sovranazionale, spesso definito come **cyber law**. La tutela del **cyber-contraente debole** rimane una priorità, con regole specifiche che si applicano sia al perfezionamento del contratto che alla sua esecuzione.

Responsabilità nei Sistemi di Intelligenza Artificiale

1. Sviluppo dell'Informatica e Autonomia delle Macchine

- **Evoluzione delle Attività Informatizzate:** La crescente autonomia delle attività gestite da macchine intelligenti, che richiedono meno intervento umano, solleva interrogativi sulla responsabilità.
- **Uso delle "Macchine" Intelligenti:** Si evidenzia l'importanza di identificare chiaramente i soggetti responsabili in caso di eventi dannosi, soprattutto in relazione ai sistemi di intelligenza artificiale (AI).

2. Funzionalità e Vantaggi dell'AI

- **Ricorso ai Sistemi di AI:** L'impiego dell'AI è funzionale per migliorare l'efficienza, ridurre il rischio di danni derivanti da errori umani e aumentare la sicurezza generale nelle attività automatizzate.

3. Accertamento della Responsabilità

- **Eventi Lesivi e Nuove Fattispecie di Danno:** L'AI introduce nuove tipologie di danno, rendendo necessaria una protezione specifica per chi subisce danni da sistemi AI.
- **Nesso di Causalità:** Diventa cruciale stabilire un nesso di causalità tra il danno e la condotta del soggetto ritenuto responsabile, considerando anche le peculiarità dei sistemi AI.

4. Disciplina Europea e Armonizzazione

- **Normative Europee:** L'Unione Europea mira a armonizzare la disciplina relativa all'uso delle nuove tecnologie, con particolare attenzione all'AI.
- **Definizione di Sistemi AI:** L'AI è descritta come software capace di generare output (come previsioni o decisioni) che influenzano l'ambiente circostante, basandosi su obiettivi definiti dall'uomo.

5. Pregiudizi e Responsabilità

- **Causalità Presunta e Condotta Colposa:** Se un danno è causato da un malfunzionamento di un sistema AI, la responsabilità potrebbe ricadere sul convenuto se viene dimostrata una violazione dell'obbligo di diligenza.
- **AI ad Alto Rischio:** In caso di danno prodotto da un sistema AI classificato come "ad alto rischio", il fornitore e l'utente hanno l'obbligo di fornire tutte le prove pertinenti, bilanciando la tutela del danneggiato con la riservatezza delle informazioni.

6. Obblighi di Diligenza e Esenzione di Responsabilità

- **Digital Service Act:** Introduce obblighi di diligenza per le piattaforme online in relazione ai processi decisionali algoritmici, con possibilità di esenzione dalla responsabilità per i fornitori di servizi intermediari.

7. Equiparazione del Produttore di Beni Materiali e Software

- **AI come Servizio:** L'AI è considerata come un insieme di beni materiali e non, interconnessi. In caso di malfunzionamento, l'utilizzatore può essere esonerato da responsabilità se il danno è incontrollabile.
- **Responsabilità del Produttore:** Il produttore è responsabile per non conformità agli standard tecnici previsti, con il difetto accertato in relazione alle circostanze in cui il danno si è verificato.

8. Autonomia della Macchina e Danno da "Cose Intelligenti"

- **Normativa Applicabile:** L'art. 2051 c.c. prevede la responsabilità per i danni causati dalle cose custodite, inclusi i sistemi AI, salvo prova di caso fortuito.
- **Sistemi AI e Robot:** La legge può includere i sistemi AI o robot tra le "cose" responsabili, estendendo le norme che regolano il danno causato da animali dotati di intelligenza diversa da quella umana.

9. Ruolo del Custode del Sistema AI

- **Responsabilità del Custode:** Il proprietario o i soggetti preposti all'operatività del sistema AI sono responsabili per l'influenza esercitata sul sistema e devono dimostrare eventuali casi fortuiti che interrompono il nesso causale.