Comparazione giuridica e nuove tecnologie

Corso di Laurea in Mediazione linguistica per l'impresa internazionale e i media digitali – Lezione 13

Jacopo Fortuna

Il diritto d'autore nell'era digitale

- Specialmente le normative relative alle opere dell'ingegno sono legate all'evoluzione tecnologica.

- Tre interessi dell'opera dell'ingegno: chi la crea, chi la fa circolare, chi la usa.

- Necessità di contemperare l'interesse pubblico ad accedere alle opere creative con la necessità di apprestare incentivi alla produzione delle stesse assicurando all'autore il monopolio sullo sfruttamento economico della propria opera.

- Il diritto d'autore oggi consente al creatore dell'opera di rivendicare la paternità della stessa, opponendosi anche alla sua mutilazione e/o deformazione (c.d. diritto morale d'autore), e di sfruttare economicamente l'opera attraverso:

- Diritto di pubblicazione
- Diritto di riproduzione
- Diritto di trascrizione
- Diritto di esecuzione
- Diritto di diffusione
- Diritto di distribuzione
- Diritto di traduzione ecc…

- **Questi sono i c.d. diritti patrimoniali d'autore.**

- In Italia il testo di riferimento per la protezione del diritto d'autore è la legge n. 633 del 22/04/1941, recante disposizioni sulla «Protezione del diritto d'autore e di altri diritti connessi al suo esercizio».

- Sfide dell'era digitale al diritto d'autore:

- Facilità di riproduzione delle copie dell'opera;
- Impossibilità di distinguere la copia dal master sul piano qualitativo;
- Dematerializzazione dell'opera;
- Facilità di distribuzione e comunicazione delle opere;
- Controllo della fruizione dell'opera.

L’evoluzione del concetto di opera e la nascita di nuove opere dell’ingegno

- Il codice civile e la legge sul diritto d’autore non definiscono l’opera dell’ingegno.
- Le norme di riferimento (art. 1, comma 1. legge n. 633 del 1941 sul diritto d’autore e l’art. 2575 cc.) si limitano a riconnettere le opere, qualunque ne sia il modo o la forma di espressione, a determinati campi di produzione dell’ingegno umano quali, ad esempio, la letteratura, la musica, le arti figurative, l’architettura, il teatro, il cinema etc…
- L’era digitale ha determinato un ampliamento delle tipologie di opere dell’ingegno protette (ad esempio, il software).
- L’opera può mutare o accrescersi, divenendo instabile (ipertesti e pagine web) – necessarie forme di tutela.

Il software

- Il software può essere considerato come uno dei nuovi beni creati dall'era digitale.

- Il codice è di regola scritto in codice sorgente con linguaggio di programmazione e poi viene tradotto in codice oggetto, comprensibile alla macchina.

- Attualmente la disciplina del software, a livello unionale, è contenuta principalmente nella direttiva 2009/24/CE del Parlamento europeo e del Consiglio relativa alla tutela giuridica dei programmi per elaboratore.

- I programmi per elaboratore sono tutelati sulla base del diritto d'autore come opere letterarie ai sensi della Convenzione di Berna sulla tutela delle opere letterarie e artistiche (Direttiva 2009/24/CE, art. 1, co. 1).

Per ciò che riguarda l'Italia, la disciplina sulla tutela del software è stata trasposta all'interno della legge n. 633 del 1941 sul diritto d'autore, al cui art. 1 è stato aggiunto il seguente comma: « Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie e artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399».

All'interno della legge sul diritto d'autore, ai programmi per elaboratore è specificamente dedicata la sezione VI, in particolare gli articoli 64-bis, 64-ter e 64-quater.

Il programma è tutelato solo se presenta caratteri di originalità, cioè se è il risultato di creazione intellettuale dell'autore (programmi nuovi o che forniscono un apporto innovativo al settore di riferimento).

Viene considerato autore di un programma per elaboratore la persona fisica che ha creato il programma o, qualora la legislazione degli Stati membri lo permetta, la persona giuridica designata come titolare del diritto. Se il programma è creato da un lavoratore dipendente nell'esecuzione delle sue mansioni o su istruzioni del datore di lavoro, quest'ultimo gode dell'esercizio esclusivo di tutti i diritti economici sul programma stesso, salvo diverse disposizioni contrattuali (Dir. 2009/24).

Principio dell'esaurimento: la prima vendita della copia di un programma nell'UE da parte del titolare del diritto o con il suo consenso esaurisce il diritto di distribuzione della copia all'interno dell'UE, ad eccezione del diritto di controllare l'ulteriore locazione del programma o di una sua copia (direttiva 2009/24/CE, art. 4, co. 2).

- L’**utilizzazione** del software di regola avviene grazie a una licenza di tipo proprietario, il c.d. End User License Agreement (EULA).

- Principale strumento di distribuzione di massa del software proprietario: in tal caso la distribuzione non avviene attraverso la vendita ma attraverso una mera licenza d’uso.

- Anche le banche dati rientrano nella disciplina del diritto d’autore.

- Evoluzione del concetto di autore e del rapporto tra autore e fruitore (ad esempio ipertesto).

- Modelli di common-based peer production (ad esempio Wikipedia).

Ruolo degli intermediari e misure di protezione

- Le opere dell'ingegno di regola circolano a mezzo degli intermediari (ad es. editore).

- La digitalizzazione delle opere sembra ridefinire il ruolo degli intermediari:

- Internet rafforza la fruizione planetaria delle opere dell'ingegno (file sharing).
- Sparizione della correlazione tra opera e supporto che la contiene.
- Affermazione di nuovi intermediari di opere digitali (es. Spotify e Netflix).

- I titolari dei diritti d’autore e di diritti connessi hanno il diritto di apporre sulle opere misure tecnologiche di protezione efficaci.

- Le blockchain possono essere applicate come misure tecnologiche di protezione.

- La tecnologia può essere usata per tutelare gli autori, poiché la clausola di un rapporto contrattuale può essere tradotta in linguaggio informatico ai fini dell’enforcement del rapporto (ad es. limite di volte alla fruizione di un film).

Direttiva (UE) 2019/790 (e D.lgs. attuativo n. 177/2021)

- La direttiva stabilisce norme volte ad armonizzare ulteriormente il diritto dell'Unione applicabile al diritto d'autore e ai diritti connessi nell'ambito del mercato interno, tenendo conto in particolare degli utilizzi digitali e transfrontalieri dei contenuti protetti.

- La direttiva contiene misure per l'adeguamento delle eccezioni e delle limitazioni all'ambiente digitale e al contesto transfrontaliero oltre che misure volte a migliorare le procedure di concessione delle licenze e a garantire un più ampio accesso ai contenuti.

Altre misure adottate dalla direttiva

1) Protezione delle pubblicazioni di carattere giornalistico in caso di utilizzo online.

- Utilizzo da parte di grandi piattaforme degli articoli di giornale, ad esempio per realizzare delle rassegne stampa automatizzate;

- Obbligo per i prestatori di servizi della società dell'informazione di versare una remunerazione.

2) Utilizzo di contenuti protetti da parte di prestatori di servizi di condivisione di contenuti online.

- Accesso al pubblico a opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti.
- Necessaria autorizzazione dai titolari dei diritti, ad esempio mediante la conclusione di un accordo di licenza, al fine di comunicare al pubblico o rendere disponibile al pubblico opere o altri materiali.
- Fenomeno delle opere protette caricate dagli utenti sulle piattaforme (ad esempio, YouTube).

3) Equa remunerazione di autori e artisti (interpreti o esecutori) nei contratti di sfruttamento.

Legge n. 93 del 14 luglio 2023

- Legge sulla prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante reti di comunicazione elettronica.
- Rafforzamento della tutela del diritto d'autore online, anche attraverso il riconoscimento di nuovi poteri all'Autorità per le garanzie nelle comunicazioni:

- Provvedimenti urgenti e cautelari dell'Autorità per le garanzie nelle comunicazioni per la disabilitazione dell'accesso a contenuti diffusi abusivamente.
- Misure per il contenimento della pirateria cinematografica, audiovisiva o editoriale.
- Campagne di comunicazione e sensibilizzazione.
- Sanzioni amministrative.

Per concludere sul diritto d'autore nell'era digitale

- Le prime regole sulla tutela del diritto d'autore sono formulate con la nascita delle tecnologie che consentono la copia in serie dei libri.

- Il modello tradizionale del diritto d'autore entra in crisi perché è estremamente facile riprodurre e distribuire opere protette.

- L'uso della tecnologia fa evolvere i concetti di opera, di autore e di creatività e ridefinisce le modalità attraverso le quali è possibile remunerare il lavoro degli autori.

- La stessa tecnologia potrebbe fornire strumenti più efficaci delle norme per la tutela degli interessi degli autori.

Comparazione giuridica e nuove tecnologie

Corso di Laurea in Mediazione linguistica per l'impresa internazionale e i media digitali – Lezione 14

Jacopo Fortuna

La normativa UE sui «gatekeepers» delle piattaforme e sugli intermediari di servizi digitali

- Ruolo predominante nella rete da parte di soggetti attraverso la creazione di piattaforme mediante le quali vengono prestati servizi interconnessi.

- Grande potere dei proprietari delle piattaforme verso utenti finali e altri operatori commerciali.

- Parimenti è importante il ruolo degli intermediari dei servizi della società dell'informazione: coloro che assicurano la connessione, coloro che offrono spazi di memorizzazione, coloro che consentono di pubblicare contenuti come un blog o un sito web.

- Gli intermediari dei servizi della società dell'informazione possono teoricamente evitare che vengano commessi abusi ma anche assumere il ruolo di potenziali censori.

- Potenziale bersaglio delle richieste di risarcimento da parte delle vittime degli illeciti

- L'UE è intervenuta per disciplinare tutti questi fenomeni

Regolamento sui mercati digitali (Digital Market Act – Reg. (UE) 2022/1925

- Il Regolamento si propone di contribuire al corretto funzionamento del mercato interno, stabilendo norme armonizzate volte a garantire, per tutte le imprese, che i mercati nel settore digitale nei quali sono presenti gatekeepers (controllori dell'accesso) siano equi e contendibili in tutta l'Unione a vantaggio di utenti commerciali e degli utenti finali.

- L'UE si propone di disciplinare lo strapotere delle piattaforme. Definizione di piattaforma (o più precisamente «servizio di piattaforma di base»: Art. 2, co. 1, n.2 del Digital Market Act).

- Gatekeepers: imprese che forniscono i servizi di piattaforma di base, designate come tali dalla Commissione europea sulla base di alcuni criteri.

Le piattaforme che rientrano nel campo di applicazione del regolamento sono:

- Social network: TikTok, Facebook, Instagram, Linkedin.
- Comunicazione interpersonale indipendenti dal numero: Whatsapp, Messenger.
- Intermediazione: Google Maps, Google Play, Google Shopping, Amazon marketplace, App Store, Booking.com, Meta marketplace.
- Video sharing: YouTube.
- Motori di ricerca: Google Search.
- Browser: Chrome, Safari.
- Servizi Pubblicitari: Google, Amazon, Meta.
- Sistemi Operativi: Google Android, iOS, iPadOS, Windows PC OS.

I soggetti tutelati sono:

- utenti commerciali;
- utenti finali diversi da un utente commerciale;

Obblighi per i gatekeepers

- Rendere i propri servizi interoperabili per i terzi in situazioni specifiche;
- Consentire agli utenti commerciali di accedere ai dati che generano utilizzando la piattaforma;
- Fornire alle imprese che fanno pubblicità sulla piattaforma gli strumenti e le informazioni necessarie per consentire agli inserzionisti e agli editori di effettuare verifiche indipendenti dei messaggi pubblicitari ospitati dalla piattaforma;
- Consentire agli utenti commerciali di promuovere la loro offerta e concludere contratti con clienti al di fuori della piattaforma;

Divieti per i gatekeepers

- Non possono riservare ai propri servizi e prodotti un trattamento favorevole in termini di classificazione rispetto a servizi o prodotti analoghi offerti da terzi sulla loro piattaforma;

- Impedire ai consumatori di mettersi in contatto con imprese al di fuori della piattaforma;

- Impedire agli utenti di disinstallare applicazioni o software preinstallati;

- Tenere traccia per motivi pubblicitari degli utenti finali al di fuori dei servizi essenziali della piattaforma, senza previo consenso dei diretti interessati.

- **Sanzioni**

- **Benefici per i consumatori** (Ad esempio, maggiore controllo sui dati personali e portabilità dei dati)

- **Benefici per gli utenti commerciali** (Ad esempio, poter comunicare direttamente con i clienti senza per forza dover passare dalla piattaforma)

- **Regolamento e disciplina antitrust** (Il regolamento in esame persegue un obbiettivo complementare ma diverso rispetto alle normative in materia di concorrenza).

Regolamento sui servizi digitali (Digital Services Act – Reg. (UE) 2022/2065)

- Regolamento relativo al mercato unico dei servizi digitali: contribuisce al corretto funzionamento del mercato interno dei servizi intermediari.

- Il regolamento prevede regole comuni per contrastare fenomeni deteriori come la diffusione di contenuti illegali e la disinformazione online.

- Propiziare attraverso il comportamento degli intermediari un ambiente online sicuro, prevedibile e affidabile così da garantire i diritti fondamentali.

- Limitare il potere dei grandi player della rete

Ambito di applicazione:

Il DSA si applica a tutti gli intermediari e piattaforme online nell'UE, ad esempio mercati online, social network, piattaforme di condivisione di contenuti, app store e piattaforme di viaggio e alloggio online. Le piattaforme online e i motori di ricerca di dimensioni molto grandi (VLOP e VLOSE) hanno obblighi aggiuntivi.

Il regolamento si applica ai servizi intermediari offerti a destinatari il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione, indipendentemente dal luogo di stabilimento dei prestatori di tali servizi intermediari.

Per **servizio intermediario** si intende uno dei seguenti servizi della società dell'informazione:

1) Servizio di **semplice trasporto** (c.d. mere conduit), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio o nel fornire accesso a una rete di comunicazione.
2) Servizio di **memorizzazione temporanea** (c.d. caching), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite dal destinatario del servizio, che comporta la memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficiente il successivo inoltro delle informazioni ad altri destinatari su loro richiesta.
3) Servizio di **memorizzazione di informazioni** (c.d. hosting), consistente nel memorizzare informazioni fornite da un destinatario del servizio su richiesta dello stesso.

Il DSA prevede obblighi per gli intermediari diversi e via via crescenti in ragione del tipo, delle dimensioni e della natura del servizio intermediario interessato.

La responsabilità dei prestatori di servizi intermediari.

Responsabilità degli intermediari per i contenuti e le attività illegali veicolate (da art. 4 a art. 8).

- Per il semplice trasporto, il prestatore del servizio non è responsabile delle informazioni trasmesse o a cui si è avuto accesso a condizione che non dia origine alla trasmissione, non selezioni il destinatario della trasmissione non selezioni né modifichi le informazioni trasmesse.

Se il prestatore di servizi intermediari non si limita al semplice trasporto ma opera una memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficiente o più sicuro il successivo inoltro delle informazioni ad altri destinatari del servizio su loro richiesta (c.d. caching - art. 5).

In questo caso il prestatore non è responsabile a condizione che non modifichi le informazioni, si conformi alle condizioni di accesso alle informazioni, si conformi alle norme sull'aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore, non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni e agisca prontamente per rimuovere le informazioni che ha memorizzato se necessario.

Art. 6: responsabilità nel caso di memorizzazione delle informazioni.

Il prestatore del servizio consistente nella memorizzazione di informazioni fornite da un destinatario del servizio non è responsabile a condizione che non sia effettivamente a conoscenza delle attività o dei contenuti illegali e, per quanto attiene a domande risarcitorie, non sia consapevole di fatti o circostanze che rendono manifesta l'illegalità dell'attività o dei contenuti; oppure non appena venga a conoscenza di tali attività o contenuti illegali o divenga consapevole di tali fatti o circostanze, agisca immediatamente per rimuovere i contenuti illegali o per disabilitare l'accesso agli stessi.

Ai prestatori di servizi intermediari non è imposto alcun obbligo generale di sorveglianza sulle informazioni che tali prestatori trasmettono o memorizzano. Né di accertare attivamente fatti o circostanze che indichino la presenza di attività illegali (art. 8).

Obblighi in materia di dovere di diligenza per un ambiente online trasparente e sicuro

- Il Regolamento stabilisce obblighi fondamentali applicabili a tutti i prestatori di servizi intermediari nonché obblighi supplementari per i prestatori si servizi di memorizzazione di informazioni.

- Più specificamente, per i prestatori di piattaforme online, di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi.

Obblighi validi per tutti gli intermediari

- Obbligo di designazione di un punto di contatto unico che consenta ai prestatori di servizi intermediari di comunicare direttamente con le autorità degli Stati membri e le competenti autorità europee.
- Obbligo di designazione di un punto di contatto per comunicare con i destinatari del servizio (art. 12)
- Obbligo di designazione di un rappresentante legale per i prestatori di servizi intermediari che non sono stabiliti nell'Unione ma che offrono servizi nell'UE (art. 13).
- Obblighi sui contenuti dei termini e delle condizioni del servizio. I prestatori di servizi intermediari devono includere nelle loro condizioni generali informazioni sulle restrizioni che impongono in relazione all'uso dei loro servizi per quanto riguarda le informazioni fornite dai destinatari

- **Tali informazioni riguardano:**

- Politiche, procedure, misure e strumenti utilizzati ai fini della moderazione dei contenuti.

- Processo decisionale algoritmico e verifica umana.

- Regole procedurali del loro sistema interno di gestione dei reclami.

- Redazione in linguaggio chiaro e comprensibile.

- Disponibili al pubblico in formato facilmente accessibile e leggibile meccanicamente.

- Prescrizioni più specifiche sono dettate per i servizi destinati ai minori e per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi (art. 14).
- L'ultimo obbligo comune a tutti gli intermediari riguarda le relazioni di trasparenza per i prestatori di servizi intermediari (art. 15).

Obblighi aggiuntivi applicabili ai prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme online.

Chi eroga servizi di caching e hosting è soggetto ai seguenti ulteriori obblighi:

a) Attivazione di un meccanismo di segnalazione e azione

b) Motivazione delle restrizioni imposte:

Restrizioni:

- Restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio, compresa la rimozione dei contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti;
- Sospensione, cessazione o altra limitazione dei pagamenti in denaro;
- Sospensione o cessazione totale o parziale della prestazione del servizio;
- Sospensione o chiusura dell'account del destinatario;

c) Notifica di sospetti di reati (art. 18).

Obblighi aggiuntivi applicabili ai fornitori di piattaforme online.

- Attivazione di un sistema interno di gestione dei reclami;
- Messa a disposizione di informazioni circa la possibilità di rivolgersi all'organismo di risoluzione extragiudiziale delle controversie;
- Attribuzione di un ruolo significativo ai segnalatori attendibili;
- Adozione di misure di protezione contro gli abusi;
- Comunicazioni aggiuntive;
- Uso di interfacce online che non ingannino o manipolino i destinatari dei loro servizi o falsino o compromettano altrimenti la capacità dei destinatari dei loro servizi di prendere decisioni libere e informate (c.d. divieto di dark patterns - art. 25);

- Diffusione di messaggi pubblicitari solo se in possesso di determinate caratteristiche (ad es. riconoscibilità del messaggio come pubblicità).

- Adozione di sistemi di raccomandazione trasparenti (art. 27).

- Protezione online per i minori (art. 28).

- Obblighi aggiuntivi applicabili ai fornitori di piattaforme online che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali.

- Obblighi supplementari a carico dei fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi per la gestione dei rischi sistemici.

- **Ruolo dei codici di condotta:** La Commissione e il Comitato europeo per i servizi digitali incoraggiano e agevolano l'elaborazione di codici di condotta volontari a livello di Unione per contribuire alla corretta applicazione del DSA.

Comparazione giuridica e nuove tecnologie

Corso di Laurea in Mediazione linguistica per l'impresa internazionale e i media digitali – Lezione 15

Jacopo Fortuna

Cybersecurity e rischio digitale

- La sicurezza dei sistemi informatici è essenziale per garantire la protezione dei dati personali.
- Sicurezza della navigazione in rete specialmente per i minori.
- Sicurezza dei meccanismi di firma.
- Sicurezza delle transazioni sulla rete.

Definizioni

- Il regolamento (UE) 2019/881 (Cybersecurity Act) definisce la «**cybersicurezza**» come l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche.
- La «**minaccia informatica**» è qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli eventi di tali sistemi e altre persone.
- La direttiva (UE) 2022/2555 (Direttiva NIS2) definisce «**incidente**» un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi. Il «rischio» è invece la potenziale perdita o perturbazione causata da un incidente; è espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che l'incidente si verifichi

Alcune tipologie di attacco alla sicurezza informatica

- Attacchi più frequenti:

Malware: software dannoso progettato specificamente per danneggiare o interrompere un sistema, attaccando la riservatezza, l'integrità o la disponibilità (include virus worms, trojan horses, ransomware, spyware, adware, scareware).

Web based attacks: attacchi che utilizzano il web e i suoi servizi.

Web application attacks: tentativi diretti o indiretti di sfruttare una vulnerabilità o debolezza nei servizi o nelle applicazioni sul web.

Phishing: meccanismo di elaborazione dei messaggi che utilizza tecniche di ingegneria sociale in modo che il destinatario sia attirato. Tentativo di indurre i destinatari di e-mail e messaggi ad aprire un allegato dannoso, cliccare su un URL non sicuro, ottenere bonifici ecc…

Denial of services: malfunzionamento dovuto a un attacco informatico con il quale si esauriscono le risorse di un sistema in modo che non sia più in grado di erogare i servizi ai clients richiedenti.

Spam: uso abusivo di e-mail e servizi di messaggistica per inondare i destinatari di comunicazioni non richieste.

Botnets: rete di computer infettati da software dannoso in modo da poter essere controllati in remoto.

Data breach: è il risultato di un attacco riuscito che produce la perdita o la diffusione di dati

Insider threat: la minaccia proveniente dall'interno può colpire ogni organizzazione e chiunque abbia avuto accesso alle risorse digitali può abusarne (minaccia dolosa o colposa).

Physical manipulation/damage/theft/loss: si verifica quando c'è una perdita, un furto, un danneggiamento o una manipolazione fisica delle risorse informatiche.

Information leakage: fuga di informazioni (dati personali, informazioni commerciali etc...).

Identity theft: frode perpetrata rubando l'identità di una persona.

Cryptojacking: mira a sfruttare le risorse di un sistema per generare criptovalute all'insaputa del proprietario.

Ransomware: un tipo di malware che limita l'accesso del dispositivo che infetta. Viene richiesto un riscatto (ransom) da pagare se si vuole che la limitazione venga rimossa.

Cyberspionaggio: mira al furto di segreti di Stato e commerciali, di diritti di proprietà intellettuale e di informazioni proprietarie in settori strategici

La strategia europea sulla cybersicurezza

- Nel dicembre 2020 la Commissione europea ha illustrato la strategia dell'UE in materia di cybersicurezza per il decennio digitale.
- La disciplina della materia è affidata alla citata direttiva (UE) 2022/2555 (c.d. Direttiva NIS2), relativa a misure per un livello comune elevato di cybersicurezza nell'Unione.
- La direttiva stabilisce misure volte a migliorare il funzionamento del mercato interno. Essa stabilisce:

- Obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cybersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza e team di risposta agli incidenti di sicurezza informatica (CSIRT);

- Misure in materia di gestione dei rischi di cybersicurezza e obblighi di segnalazione per i soggetti di un tipo di cui agli allegati alla direttiva nonché per i soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557;

- Norme e obblighi in materia di condivisione delle informazioni sulla cybersicurezza;

- Obblighi in materia di vigilanza ed esecuzione per gli Stati membri.

La direttiva si applica a una pluralità di soggetti, di un certo tipo di consistenza, che operano in settori critici (energia, trasporti, settore bancario, infrastrutture del mercato finanziario, settore sanitario, acque, infrastrutture digitali, pubblica amministrazione etc...).

- Ogni Stato membro deve adottare una strategia nazionale per la cybersicurezza che prevede gli obbiettivi strategici e le risorse necessarie per conseguirli, nonché adeguate misure strategiche normative al fine di raggiungere e mantenere un livello elevato di cybersicurezza.

- Ogni Stato deve istituire una o più autorità competenti responsabili della cybersicurezza e dei compiti di vigilanza e deve istituire un team di risposta agli incidenti di sicurezza informatica (c.d. CSIRT).

- Altro tassello importante nella strategia europea è il Cybersecurity Act, relativo all'ENISA e istitutivo della stessa, l'Agenzia dell'UE per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione ed ella comunicazione.

- Il Cybersecurity Act istituisce anche il sistema di europeo di certificazione della cybersicurezza. Il certificato europeo di cybersicurezza è rilasciato dall'organismo competente e attesterà che un determinato prodotto TIC, servizio TIC o processo TIC (TIC: Tecnologie dell'informazione e della comunicazione) è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cybersicurezza.

- L'UE ha elaborato anche il c.d. Cyber Resilience Act, cioè una proposta di regolamento relativa a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali, con l'obbiettivo di definire un quadro giuridico uniforme per i requisiti essenziali di cybersicurezza per l'immissione su mercato dell'UE di prodotti con elementi digitali.

- L’UE sintetizza la propria strategia in materia di cybersicurezza in quattro principi: prevenire, rilevare, rispondere, scoraggiare.

STRATEGIA ITALIANA. AGENZIA PER LA CYBERSICUREZZA NAZIONALE.

- Il d.l. 82/2021 ha ridefinito l’architettura nazionale di cybersicurezza, con l’obbiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.
- Lo stesso d.l. ha istituito l’Agenzia per la cybersicurezza nazionale (ACN), che ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico nonché di prevenire e mitigare il maggior numero di attacchi cibernetici e di favorire il raggiungimento dell’autonomia tecnologica.

- Tra i principali compiti dell'Agenzia c'è l'attuazione della Strategia nazionale di cybersicurezza.

RISCHIO DIGITALE

- Il 19 luglio 2024 si è verificato un crash informatico globale per effetto di un malfunzionamento dell'aggiornamento di un software di cybersicurezza per ambienti Windows. A causa del malfunzionamento dei server sono stati cancellati migliaia di voli, sono stati rinviati interventi chirurgici e sono risultatati non più operativi anche sistemi di pagamento e di trading online.
- Il rischio digitale è sistemico a causa dell'interconnessione e uno dei settori in cui è maggiormente avvertito il pericolo è il settore finanziario.

- A fronte di ciò, l'UE ha emanato il regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario, comunemente conosciuto come DORA (Digital Operational Resilience Act).

- Il regolamento si rivolge a tutti gli operatori del sistema finanziario, favorisce un migliore allineamento delle strategie di gestione dei rischi ITC da parte delle entità finanziarie, migliora e armonizza le regole per la gestione del rischio, introduce specifici obblighi in materia di gestione degli incidenti e prevede dei test cui le entità finanziarie dovranno essere sottoposte periodicamente per accertarne il grado di sicurezza raggiunto, disciplina le responsabilità delle c.d. terze parti e favorisce lo scambio di informazioni e dati sulle minacce informatiche, al fine di rafforzare la cooperazione tra gli Stati membri.

Metodi alternativi di risoluzione delle controversie

- Incompatibilità dei tempi della giustizia con la necessità di dirimere controversie legate ai contratti conclusi sulla rete.

- Direttiva comunitaria sul commercio elettronico (Dir. 2000/31/CE) e Digital Services Act: spingono per il ricorso a strumenti extragiudiziali di composizione delle controversie.

- Alternative Dispute Resolution e Online Dispute Resolution.

- ADR: regole di rito (contraddittorio, diritto di difesa etc...) e regole di merito.

- I sistemi di risoluzione alternativa delle controversie online sono guardati con favore dall'UE poiché aumentano la fiducia nel commercio elettronico.

- Raccomandazione 4 aprile 2001 della Commissione europea sui principi applicabili agli organi extragiudiziali che partecipano alla risoluzione consensuale delle controversie in materia di consumo. La procedura deve essere:

- Imparziale;
- Trasparente;
- Efficace;
- Equa;

- L’UE ha istituito la piattaforma ODR (Online Dispute Resolution) che costituisce l’unico punto di accesso per i consumatori e i professionisti che desiderano risolvere in ambito extragiudiziale le controversie oggetto del Reg. UE 2013/524. Ha le seguenti funzioni:

- Mettere a disposizione un modulo di reclamo elettronico;

- Informare del reclamo la parte convenuta;

- Individuare l’organismo o gli organismi ADR competenti;

- Proporre uno strumento elettronico di gestione dei casi che consenta alle parti e all'organismo ADR di condurre online la procedura di risoluzione della controversia mediante la piattaforma ODR;

- Fornire alle parti e all'organismo ADR la traduzione delle informazioni che sono necessarie per la risoluzione della controversia e che sono scambiate tramite la piattaforma ODR.

- Mettere a disposizione un modulo elettronico tramite il quale gli organismi ADR trasmettono le informazioni necessarie;

- Mettere a disposizione un sistema di commenti che consenta alle parti di esprimere il proprio punto di vista sul funzionamento della piattaforma.

ALCUNE CONCLUSIONI SUL DIRITTO NELL'ERA DIGITALE