FIVERS

Aggiornamento
Data protection, AI, IT and IP

n. 14 / 2024

DATA PROTECTION.

5 Novembre 2024 – Comitato europeo per la protezione dei dati personali: pubblicato il primo rapporto sullo stato di attuazione dell'accordo UE-USA (Data Privacy Framework) per il trasferimento dei dati personali dalla UE verso gli USA.

INTELLIGENZA ARTIFICIALE.

12 Novembre 2024 – Osservatorio Fintech & Insurtech del Politecnico di Milano: i dati dell'IIA Index (Insurtech Investment Index) evidenziano nel 2024 una forte impennata degli investimenti in intelligenza artificiale da parte del comparto assicurativo.

MERCATI DIGITALI

11 novembre 2024 - Commissione europea: adottato gli ulteriori standard tecnici per l'applicazione del Regolamento sulla resilienza operativa digitale per il settore finanziario (regolamento (UE) 2022/2554) (DORA).

---

6 Novembre 2024 - Le AEV (ABE, ESMA ed EIOPA) emanano orientamenti per la cooperazione DORA, concentrandosi sulla comunicazione e sulla supervisione dei fornitori di servizi TIC critici.

---

6 Novembre 2024 – Commissione UE: pubblicato il Regolamento di esecuzione della Legge sui Servizi Digitali per l'attuazione degli obblighi di comunicazione e trasparenza dei VLOP e dei VLOSE.

INFORMATION TECHNOLOGY

7 Novembre 2024 – Corte Suprema di Cassazione: integra il reato di accesso abusivo al sistema informatico anche l'accesso del dirigente che utilizza le credenziali della collaboratrice.

---

6 Novembre 2024 – Corte Suprema di Cassazione: valido l'appello telematico anche se la parte si è costituita con copia analogica di documenti nativi digitali.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

12 Novembre 2024 – Ministero delle Imprese e del Made in Italy (MIMIT): operativa la norma prevista nella Legge Made in Italy per la tutela dei marchi di particolare interesse e valenza nazionale.

---

12 Novembre 2024 – Ministero delle Imprese e del Made in Italy (MIMIT): - transizione green e tech dell'industria della moda, del tessile e degli accessori ai sensi della Legge Made in Italy, dall'11 dicembre invio domande per l'accesso alle agevolazioni.

---

8 Novembre 2024 – Corte di Giustizia della UE: gli Stati membri sono tenuti a tutelare le opere d'arte nel territorio dell'Unione, indipendentemente dal paese d'origine di tali opere o dalla cittadinanza del loro autore.

---

8 Novembre 2024 – Corte di Giustizia UE: la direttiva relativa alla tutela giuridica dei programmi per elaboratore non consente al titolare di tale tutela di impedire la commercializzazione da parte di un terzo di un software che si limiti a modificare il contenuto di talune variabili inserite temporaneamente nella memoria RAM di una consolle per videogiochi.

DATA PROTECTION

5 Novembre 2024 – Comitato europeo per la protezione dei dati personali: pubblicato il primo rapporto sullo stato di attuazione dell'accordo UE-USA (Data Privacy Framework) per il trasferimento dei dati personali dalla UE verso gli USA.

Il Comitato europeo per la protezione dei dati (EDPB) ha adottato una **Relazione sulla prima revisione del quadro UE-USA sulla privacy dei dati (Data Privacy Framework - DPF)** con la quale ha delineato lo stato di attuazione degli accordi dopo l'adozione della decisione di adeguatezza adottata dalla Commissione UE nel luglio 2023.

Per quanto riguarda gli aspetti commerciali, ossia l'applicazione dei requisiti applicabili alle società autocertificate nell'ambito del DPF, l'EDPB osserva che il Dipartimento del Commercio degli Stati Uniti ha adottato tutte le misure pertinenti per attuare il processo di certificazione. Ciò include lo sviluppo di un nuovo sito web, l'aggiornamento delle procedure, il coinvolgimento con le aziende e lo svolgimento di attività di sensibilizzazione.

Inoltre, è stato attuato il meccanismo di ricorso per i cittadini dell'UE e su entrambe le sponde dell'Atlantico sono stati pubblicati orientamenti completi per la gestione dei reclami. Tuttavia, il basso numero di reclami ricevuti finora nell'ambito del DPF evidenzia l'importanza per le autorità statunitensi di avviare attività di monitoraggio relative alla conformità delle aziende certificate DPF con i principi sostanziali del DPF.

L'EDPB incoraggia lo sviluppo di linee guida da parte delle autorità statunitensi, chiarendo i requisiti che le aziende certificate DPF dovrebbero rispettare quando trasferiscono i dati personali che hanno ricevuto dagli esportatori dell'UE. IL Comitato suggerisce – inoltre – l'adozione di una guida da parte delle autorità statunitensi sul trasferimento dei dati del personale.

Per quanto riguarda l'accesso da parte delle autorità pubbliche statunitensi ai dati personali trasferiti dall'UE a organizzazioni certificate, l'EDPB si è concentrato: sull'effettiva attuazione delle garanzie introdotte dall'Executive Order 14086 nel quadro giuridico degli Stati Uniti, quali i principi di necessità e proporzionalità e il nuovo meccanismo di ricorso. Il Comitato ritiene che gli elementi del meccanismo di ricorso siano in essere; al tempo stesso, rinnova l'invito alla Commissione europea a monitorare il funzionamento pratico delle diverse salvaguardie, ad esempio l'attuazione dei principi di necessità e proporzionalità. L'EDPB raccomanda inoltre che la Commissione monitori gli sviluppi futuri relativi alla legge sulla sorveglianza dell'intelligence esterna degli Stati Uniti, in particolare in considerazione dell'estensione della sezione 702 dopo la sua nuova autorizzazione da parte del Congresso degli Stati Uniti all'inizio di quest'anno.

Infine, il Comitato raccomanda che la prossima revisione della decisione di adeguatezza UE-USA abbia luogo entro i prossimi tre anni o entro termini anche più brevi.

INTELLIGENZA ARTIFICIALE.

12 Novembre 2024 – Osservatorio Fintech & Insurtech del Politecnico di Milano: i dati dell'IIA Index (Insurtech Investment Index) evidenziano nel 2024 una forte impennata degli investimenti in intelligenza artificiale da parte del comparto assicurativo.

Il settore insurtech italiano vive un momento di forte crescita, spinto da una forte impennata degli investimenti in intelligenza artificiale, come rivelano i dati aggiornati dell'Insurtech Investment Index. L'indice, ideato dall'Italian Insurtech Association (IIA) e monitorato dall'Osservatorio Fintech & Insurtech del Politecnico di Milano, ha confermato per il 2024 un punteggio di 20 su 30, in crescita rispetto ai 14 punti del 2022, segnalando una maturazione del settore assicurativo verso l'adozione di tecnologie avanzate.

Al centro dell'interesse delle compagnie assicurative italiane troviamo proprio l'intelligenza artificiale, con l'88% delle aziende che ha investito in progetti o partnership in quest'area nei primi sei mesi dell'anno. Le applicazioni principali riguardano la gestione dei sinistri, la sottoscrizione delle polizze e i processi di back-office, ambiti in cui l'AI ha dimostrato di migliorare significativamente l'efficienza e la rapidità delle operazioni.

L'Index mostra anche un'ulteriore crescita delle collaborazioni tra startup e compagnie assicurative: nel 2023, le partnership sono aumentate dell'80% rispetto all'anno precedente, arrivando a quota 45. Questi legami, insieme ai progetti interni delle compagnie, hanno spinto gli investimenti complessivi nel settore a 44,8 milioni di euro, in crescita dell'89% rispetto ai 23,7 milioni del 2022.

Secondo le previsioni dell'IIA, il 2024 potrebbe diventare un anno record per gli investimenti in AI: si stima che entro fine anno verranno stanziati circa 50 milioni di euro, con una proiezione che prevede il raggiungimento dei 90 milioni nel 2025. L'Insurtech ha superato la fase esplorativa e sta consolidando l'ecosistema grazie agli investimenti crescenti, che dimostrano come l'industry abbia colto l'importanza di innovare per migliorare i processi e ampliare il mercato.

Nel 2024, le compagnie assicurative italiane hanno investito soprattutto nell'integrazione dell'AI nella gestione dei sinistri (71%), migliorando la velocità e la qualità delle risposte ai clienti, e nell'amministrazione dei contratti e gestione del cliente (52%), ambiti dove l'automazione ha portato processi più fluidi e personalizzati. L'intelligenza artificiale ha trovato spazio anche nella sottoscrizione delle polizze e nella gestione del rischio (50%), aumentando la precisione delle analisi e la capacità predittiva del settore.

La digitalizzazione dei processi di back-office ha ricevuto un'attenzione particolare: l'88% delle compagnie ha utilizzato l'AI per automatizzare le attività interne, consentendo una gestione più efficace e flessibile. Inoltre, alcune tecnologie specifiche stanno trovando un'ampia adozione: chatbot e assistenti virtuali (78%), AI generativa (76%) per risposte personalizzate, Machine Learning (73%) per l'analisi predittiva dei rischi e Robot Process Automation (45%) per la gestione documentale.

Nonostante i progressi, l'adozione dell'AI in campo assicurativo presenta ancora diverse difficoltà. Tra le principali problematiche riscontrate emergono l'integrazione con le infrastrutture esistenti (62%) e le preoccupazioni etiche (52%), seguite da questioni di privacy (57%) e conformità normativa (48%). "Per superare queste sfide e rimanere competitivi, le compagnie assicurative devono investire non solo in tecnologie, ma anche in nuove competenze", ha commentato Simone Ranucci Brandimarte, Presidente di IIA, anticipando che entro il 2030 oltre la metà delle polizze includerà almeno un elemento di AI.

La spinta verso l'innovazione, alimentata dalla collaborazione tra compagnie e startup, è destinata a crescere, ma resta cruciale garantire finanziamenti adeguati per competere a livello europeo.

MERCATI DIGITALI

11 novembre 2024 - Commissione europea: adottati gli ulteriori standard tecnici per l'applicazione del Regolamento sulla resilienza operativa digitale per il settore finanziario (regolamento (UE) 2022/2554) (DORA).

La Commissione europea ha adottato le ulteriori e attese norme tecniche per integrare il Regolamento 2022/2554 sulla resilienza operativa digitale per il settore finanziario (DORA).

Le norme tecniche comprendono:

- norme tecniche di attuazione (ITS) su moduli, modelli e procedure standard per le entità finanziarie per la segnalazione di un incidente grave connesso alle TIC e per la notifica di una minaccia informatica significativa (Reporting ITS);

- norma tecnica di regolamentazione (RTS) sul contenuto e i termini per la notifica iniziale e la relazione intermedia e finale sugli incidenti gravi connessi alle TIC e il contenuto della notifica volontaria per le minacce informatiche significative (RTS per la segnalazione); e

- RTS sull'armonizzazione delle condizioni che consentono lo svolgimento delle attività di sorveglianza (Harmonisation RTS).

Gli ITS di segnalazione

Il sistema di gestione degli ITS per la segnalazione contiene modelli per la notifica iniziale, la relazione intermedia e la relazione finale sugli incidenti gravi connessi alle Tecnologie dell'Informazione e Comunicazione (TIC) da fornire alle autorità di vigilanza competenti ai sensi dell'articolo 19, paragrafo 4, della DORA. Il sistema di gestione degli ITS per la segnalazione chiarisce inoltre che le entità finanziarie che forniscono informazioni su incidenti ricorrenti non gravi connessi alle TIC che soddisfano cumulativamente le condizioni per un incidente grave connesso alle TIC devono fornire informazioni in forma aggregata. Analogamente, le entità finanziarie che, dopo una valutazione, concludono che l'incidente relativo alle TIC precedentemente segnalato come grave non soddisfa tali criteri devono notificare la riclassificazione alle autorità di vigilanza competenti.

Il Reporting RTS

L'RTS di rendicontazione descrive in dettaglio i contenuti richiesti delle notifiche iniziali, delle relazioni intermedie e finali da fornire ai sensi dell'articolo 19, paragrafo 4, del DORA.

Inoltre, le RTS per la comunicazione delineano i termini per la presentazione della notifica e delle relazioni di cui sopra. La notifica iniziale dovrebbe essere effettuata entro quattro ore dalla classificazione degli incidenti connessi alle TIC come incidenti gravi e non oltre 24 ore dal momento in cui l'entità finanziaria ne viene a conoscenza. Le relazioni intermedie dovrebbero essere presentate entro 72 ore dalla notifica iniziale e una relazione intermedia aggiornata dovrebbe essere presentata senza indebito ritardo qualora siano state ripristinate le normali attività. La relazione finale deve essere presentata entro un mese dalla presentazione della relazione intermedia o dall'ultima relazione intermedia aggiornata.

In particolare, quando un incidente correlato alle TIC non è classificato come grave entro 24 ore dal momento in cui ne è venuto a conoscenza, ma successivamente riclassificato come grave, l'entità finanziaria deve presentare la notifica dell'incidente come grave entro quattro ore dalla riclassificazione.

L'RTS di segnalazione rileva inoltre i contenuti della notifica volontaria di minacce informatiche significative ai sensi dell'articolo 19, paragrafo 2, del DORA.

Le norme tecniche di armonizzazione

Le norme tecniche di armonizzazione riguardano il ruolo dei fornitori terzi di servizi di TIC critici nel settore finanziario ai sensi dell'articolo 31 del DORA. In particolare, i fornitori terzi di servizi ICT critici che presentano una richiesta volontaria di essere designati come critici devono fornire all'Autorità di vigilanza europea (ESA) tutte le informazioni necessarie per dimostrarne la criticità. Le norme tecniche di armonizzazione specificano ciò che deve essere incluso nella presentazione alle AEV da parte dei fornitori terzi di servizi TIC critici, insieme al contenuto, alla struttura e al formato di tali comunicazioni.

Le norme tecniche di armonizzazione comprendono anche le informazioni da presentare all'autorità di sorveglianza capofila necessarie per svolgere i suoi compiti di sorveglianza ai sensi del DORA.

Le AEV comprendono l'Autorità bancaria europea (ABE), l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA) e l'Autorità europea degli strumenti finanziari e dei mercati (ESMA).

---

6 Novembre 2024 - Le AEV (ABE, ESMA ed EIOPA) emanano orientamenti per la cooperazione DORA, concentrandosi sulla comunicazione e sulla supervisione dei fornitori di servizi TIC critici.

Il 6 novembre 2024 il Comitato congiunto delle autorità europee di vigilanza (AEV) ha pubblicato gli Orientamenti congiunti sulla cooperazione in materia di sorveglianza e sullo scambio di informazioni tra le AEV e le autorità competenti ai sensi del *Digital Operational Resilience Act* (DORA).

Le AEV costituiscono l'Autorità bancaria europea (ABE), l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA) e l'Autorità europea degli strumenti finanziari e dei mercati (ESMA). Gli orientamenti si applicano solo all'articolo 31 del DORA e non si applicano, tra l'altro, a un'autorità specifica, alle entità finanziarie e ai fornitori di servizi TIC critici e alle disposizioni in materia di governance soggette al regolamento interno delle AEV.

Le linee guida delineano raccomandazioni relative al linguaggio, alla comunicazione e all'accessibilità. In particolare, la comunicazione dovrebbe avvenire per via elettronica, dovrebbe essere utilizzato un punto di contatto unico per lo scambio di informazioni riservate e dovrebbe essere utilizzato uno strumento online dedicato per condividere le informazioni in modo confidenziale e sicuro.

Fornitori terzi di servizi ICT critici

Gli orientamenti riguardano anche la designazione dei fornitori terzi di servizi di TIC critici. Ai fini della loro designazione, quelle che sono essenziali per le entità finanziarie, ai sensi dell'articolo 31, paragrafo 1, lettera a), del DORA, le autorità competenti dovrebbero, senza indebito ritardo dopo il ricevimento del registro delle informazioni ai sensi del DORA, mettere l'intero registro a disposizione delle AEV. Le autorità competenti dovrebbero inoltre mettere a disposizione delle AEV tutte le informazioni quantitative o qualitative necessarie per la valutazione delle criticità di cui all'articolo 31, paragrafo 2, del DORA.

Le AEV dovrebbero mettere a disposizione delle autorità competenti delle entità finanziarie che utilizzano i servizi forniti dai fornitori terzi di servizi di TIC la ragione sociale, il codice di identificazione, il paese della sede legale e, se necessario, il gruppo di impresa madre del soggetto critico entro 10 giorni lavorativi dal ricevimento da parte del fornitore terzo di servizi di TIC. L'autorità di sorveglianza capofila dovrebbe inoltre condividere con le autorità competenti delle entità finanziarie che si avvalgono del servizio di fornitori terzi di servizi di TIC:

- la comunicazione di eventuali modifiche alla struttura della gestione della controllata; e
- la data di inizio a partire dalla quale il fornitore terzo di servizi di TIC sarà soggetto a sorveglianza.

Inoltre, le linee guida descrivono in dettaglio gli scambi di informazioni tra l'autorità di sorveglianza capofila e le autorità competenti. L'autorità di sorveglianza capofila dovrebbe informare le autorità competenti delle entità finanziarie che utilizzano servizi di TIC forniti da un fornitore terzo di servizi di TIC critico in merito a qualsiasi:

- incidenti gravi con impatto diretto o indiretto sulle entità finanziarie; e
- eventi che potrebbero rappresentare un rischio significativo per la continuità e la sostenibilità dell'erogazione dei servizi ICT.

Sospensione dei servizi

Gli orientamenti stabiliscono che le autorità competenti devono informare l'autorità di sorveglianza capofila della loro intenzione di notificare alle entità finanziarie l'eventuale decisione adottata qualora l'entità finanziaria non adotti disposizioni contrattuali adeguate per affrontare i rischi. L'autorità di sorveglianza capofila deve quindi valutare l'impatto di tale decisione sul fornitore terzo di servizi ICT critico.

In particolare, gli orientamenti prendono in considerazione lo scenario in cui due autorità competenti pianificano o adottano decisioni riguardanti entità finanziarie che utilizzano gli stessi fornitori terzi di servizi di TIC critici e il modo in cui le autorità competenti dovrebbero essere informate di approcci di vigilanza incoerenti o divergenti.

Le Linee Guida entreranno in vigore il 17 gennaio 2025.

6 Novembre 2024 – Commissione UE: pubblicato il Regolamento di esecuzione della Legge sui Servizi Digitali per l'attuazione degli obblighi di comunicazione e trasparenza dei VLOP e dei VLOSE.

La Commissione europea ha pubblicato il Regolamento di esecuzione, che stabilisce i modelli relativi agli obblighi di comunicazione della trasparenza dei fornitori di piattaforme online. Il regolamento di esecuzione stabilisce modelli e periodi uniformi di comunicazione per i fornitori di piattaforme online di dimensioni molto grandi (Very Large On Line Platform – VLOP), motori di ricerca online di dimensioni molto grandi (Very Large Online Search Engines – VLOSE), fornitori di servizi intermediari e prestatori di servizi di hosting ai sensi della legge sui servizi digitali.

Comunicazione ai sensi della legge sui servizi digitali.

L'articolo 15, paragrafo 1, della legge sui servizi di intermediazione dei servizi impone ai prestatori di servizi intermediari di mettere a disposizione del pubblico, in un formato leggibile meccanicamente e in modo facilmente accessibile, almeno una volta all'anno, relazioni chiare e facilmente comprensibili su qualsiasi attività di moderazione dei contenuti da essi intrapresa durante il periodo di riferimento. L'articolo 15, paragrafo 1, della legge sui servizi digitali stabilisce inoltre i contenuti richiesti di tali relazioni, tra cui:

- informazioni sulla moderazione dei contenuti intrapresa di propria iniziativa dai fornitori, compreso l'uso di strumenti automatizzati, e sulle misure adottate per fornire formazione e assistenza alle persone incaricate della moderazione dei contenuti; e
- per i prestatori di servizi intermediari, il numero di reclami ricevuti attraverso i sistemi interni di gestione dei reclami e, per i fornitori di piattaforme online, la base di tali reclami e le decisioni adottate in merito.

L'articolo 24, paragrafo 1, della legge sui servizi digitali delinea le informazioni supplementari richieste che devono essere incluse nelle relazioni di cui all'articolo 15, paragrafo 1, della legge sui servizi digitali.

Comunicazione ai sensi dei regolamenti di esecuzione.

Il regolamento di esecuzione stabilisce un periodo di rendicontazione annuale dal 1° gennaio al 31 dicembre. I VLOP e i VLOSE devono pubblicare i loro rapporti sulla trasparenza ogni sei mesi per il periodo dal 1° gennaio al 30 giugno e dal 1° luglio al 31 dicembre. Le relazioni devono essere pubblicate al più tardi due mesi dopo la conclusione di ciascun periodo di riferimento.

Le relazioni sulla trasparenza devono essere conservate per almeno cinque anni dopo la loro pubblicazione e rimanere disponibili al pubblico durante tale periodo. Quando i rapporti sulla trasparenza vengono aggiornati, devono essere chiaramente indicati che si tratta di una versione aggiornata insieme alle modifiche apportate.

L'allegato II del regolamento di esecuzione fornisce le istruzioni per la compilazione dei modelli di relazione di trasparenza. I modelli includono un modello quantitativo, per contenere informazioni quantitative leggibili dalla macchina sulla moderazione dei contenuti, e un modello qualitativo per fornire informazioni significative sulla moderazione dei contenuti. L'allegato II chiarisce che, poiché gli obblighi di comunicazione non sono gli stessi per i VLOP, i VLOSE, o i prestatori di servizi intermediari, tra gli altri, non tutti i campi dei modelli si applicheranno a tutti i tipi di prestatori di servizi.

Periodo di transizione

L'allegato II rileva inoltre che il 31 dicembre 2025 termina un periodo di transizione, per allineare le tempistiche di segnalazione dei prestatori di servizi intermediari, dei prestatori di servizi di hosting e dei fornitori di piattaforme online con le scadenze dei VLOP e dei VLOSE. L'allegato II chiarisce le scadenze applicabili per i due diversi gruppi di fornitori di servizi di cui sopra durante il periodo di transizione che termina il 31 dicembre 2025.

INFORMATION TECHNOLOGY

7 Novembre 2024 – Corte Suprema di Cassazione: integra il reato di accesso abusivo al sistema informatico anche l'accesso del dirigente che utilizza le credenziali della collaboratrice.

Il dirigente di una struttura alberghiera acquisiva da una collaboratrice le credenziali di accesso al sistema informatico protetto aziendale per l'archiviazione e la gestione a fini promozionali del parco clienti comprensivo di circa 90mia schede individuali, accedendovi per scopi estranei al mandato ricevuto.

Sulla questione è intervenuta la Suprema Corte. Il ricorrente sostiene che in veste di direttore e superiore della dipendente era legittimato a chiedere le credenziali, anche al fine di controllarne il lavoro, inoltre, precisa che poco tempo prima egli aveva accesso in prima persona a quei dati. Per la Corte tale dato è irrilevante.

La Corte precisa che nel caso di un sistema informatico protetto da credenziali, ogni soggetto abilitato ha la sua "chiave" personale. Ciò perché si tratta di dati che, semplicemente, il titolare reputa debbano essere protetti, sia limitando l'accesso a chi venga dotato delle dette credenziali, sia, nel contempo, facendo sì che sia lasciata, in tal modo, traccia digitale dei singoli accessi e di chi li esegua.

È sbagliato ritenere che, nella specie, il direttore solo per via le sue mansioni, avesse automaticamente il potere di accedere a dati che, per contro, secondo la discrezionale valutazione del datore di lavoro, dovevano restare nella disponibilità di solo alcuni dipendenti, per quanto subordinati al ricorrente. Quest'ultimo ha effettuato l'accesso ad una banca dati di cui non aveva le credenziali, facendo, per giunta, risultare falsamente che l'accesso fosse stato operato dalla dipendente che, incautamente, gli aveva rivelato le sue credenziali.

In conclusione, la Suprema Corte afferma che «viola le direttive (quand'anche implicite, ma chiare) del datore di lavoro il dipendente che, pur in posizione gerarchicamente sovraordinata rispetto al titolare delle credenziali di accesso ad un sistema informatico aziendale, se le faccia rivelare per farvi ingresso senza averne specifica autorizzazione: essendo sufficiente a rendere manifeste tali direttive la stessa protezione dei dati mediante credenziali di accesso».

---

6 Novembre 2024 – Corte Suprema di Cassazione: valido l'appello telematico anche se la parte si è costituita con copia analogica di documenti nativi digitali.

La Corte d'Appello dichiarava l'appello principale improcedibile sul rilievo che: «*dall'esame degli atti non risulta la tempestiva prova della notifica dell'appello alle controparti e, con essa, la dimostrazione della stessa tempestiva costituzione degli appellanti».*

La controversia giunge in Cassazione. Secondo i ricorrenti, il deposito della copia su supporto analogico del messaggio di posta elettronica certificata, dei suoi allegati e della ricevuta di accettazione e di avvenuta consegna con la relativa attestazione di conformità sostituiva a tutti gli effetti il deposito dell'originale telematico. Inoltre, vi era da considerare che tale atto non era stato contestato dalle controparti, né era stata proposta la querela di falso; ragion per cui doveva essere considerata illegittima la dichiarazione di improcedibilità dell'appello.

La Corte di Cassazione, sez. II Civile, con ordinanza del 4 novembre 2024, n. 28207 ritiene il motivo fondato. Il Giudice di secondo grado, spiega la Suprema Corte, aveva accertato che «il difensore degli appellanti principali, che aveva notificato l'atto d'appello in forma telematica, si è costituito nel giudizio secondo le tradizionali forme cartacee, depositando copie analogiche di documenti nativi digitali (della citazione, della relazione di notificazione, delle ricevute di accettazione e di avvenuta consegna del messaggio di posta elettronica certificata, munite di attestazione di conformità), senza depositare telematicamente gli originali o i duplicati informatici di tali atti». E con la comparsa conclusionale la difesa degli appellanti aveva provveduto al deposito della relazione di notifica dell'appello corredata dalle ricevute di accettazione e di consegna in formato digitale.

La Cassazione non condivide «*il rigore formale della Corte d'appello*» secondo cui nel caso di costituzione telematica dell'appellante la prova della notificazione mediante posta elettronica certificata della citazione

introduttiva del processo d'appello deve essere fornita, entro l'udienza di cui all'art. 350 c.p.c., unicamente con modalità telematiche.

Non vi è infatti l'obbligo di produrre la notifica in modalità telematica. Per questi motivi, accoglie il ricorso con ordinanza n. 28207 del 4 novembre 2024.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

12 Novembre 2024 – Ministero delle Imprese e del Made in Italy (MIMIT): operativa la norma prevista nella Legge Made in Italy per la tutela dei marchi di particolare interesse e valenza nazionale.

Il Ministero delle Imprese e del Made in Italy, con apposito decreto del Capo Dipartimento per le politiche per le imprese, rende operativa, con la pubblicazione in Gazzetta Ufficiale, il D.M. 3 luglio 2024, con il quale il MIMIT ha emanato le disposizioni di attuazione dell'art. 7 del cosiddetto "Collegato Made in Italy" (legge 27 dicembre 2023, n. 206).

La disposizione ha come obiettivo quella di non disperdere il patrimonio rappresentato dai marchi del Made in Italy con almeno 50 anni di storia, che godono di una rilevante notorietà e sono utilizzati per la commercializzazione di prodotti o servizi realizzati da un'impresa produttiva nazionale di eccellenza collegata al territorio nazionale.

A partire dal prossimo 2 dicembre 2024, le imprese che intendono terminare l'attività collegata ad un marchio di particolare interesse e valenza nazionale (non oggetto di cessione a titolo oneroso) potranno inviare, attraverso apposito format definito dal Ministero, il proprio progetto di cessazione alla Direzione Generale per la politica industriale, la riconversione e la crisi industriale, l'innovazione, le PMI e il made in Italy (DGIND) del MIMIT.

La Direzione Generale, entro tre mesi dalla ricezione del progetto, nel caso manifesti l'interesse a subentrare nella titolarità, procederà all'avvio dei lavori per la predisposizione dell'atto di cessione gratuita del marchio da parte dell'impresa.

L'impresa nazionale o estera che intende investire in Italia o trasferire in Italia attività produttive ubicate all'estero e interessata a utilizzare uno o più marchi di titolarità del MIMIT, potrà poi presentare apposita richiesta all'Unità di missione attrazione e sblocco degli investimenti (UMASI).

Il contratto di licenza d'uso con il quale il MIMIT mette a disposizione il marchio si risolve qualora l'impresa licenziataria cessi l'attività o delocalizzi gli stabilimenti produttivi al di fuori del territorio nazionale.

---

12 Novembre 2024 – Ministero delle Imprese e del Made in Italy (MIMIT): - transizione green e tech dell'industria della moda, del tessile e degli accessori ai sensi della Legge Made in Italy, dall'11 dicembre invio domande per l'accesso alle agevolazioni.

Il Ministero delle Imprese e del Made in Italy, in attuazione del decreto interministeriale 8 agosto 2024 ha fissato con apposito provvedimento direttoriale i termini e le modalità di apertura delle domande di accesso alle agevolazioni per la realizzazione degli investimenti finalizzati alla transizione ecologica e digitale delle imprese del settore tessile, della moda e degli accessori, sull'intero territorio nazionale.

La misura, introdotta dall'art. 11 della Legge Made in Italy (206/2023), ha una dotazione economica di 15 milioni di euro.

Dalle ore 12.00 dell'11 dicembre 2024 e fino al 31 gennaio 2025, le PMI interessate (identificate con gli specifici codici ATECO) potranno presentare le domande di agevolazione esclusivamente tramite lo sportello online Invitalia, gestore della misura per conto del Ministero.

Le agevolazioni alle imprese saranno concesse sotto forma di contributo a fondo perduto, nella misura massima del 50% delle spese ammissibili e nel limite massimo di 60mila euro, per l'acquisizione di prestazioni specialistiche, quali attività di formazione del personale dipendente dell'impresa, implementazione di una o più tecnologie abilitanti finalizzate a favorire lo sviluppo dei processi aziendali o i prodotti innovativi (cloud computing, big data e analytics, intelligenza artificiale, blockchain, robotica avanzata e collaborativa, manifattura additiva e stampa 3D, Internet of Things, realtà aumentata, soluzioni di manifattura avanzata, piattaforme digitali per condivisione di competenze, sistemi di tracciabilità digitale della filiera produttiva), ottenimento di certificazioni di sostenibilità ambientale, servizi di analisi di Life Cycle Assessment (LCA).

---

8 Novembre 2024 – Corte di Giustizia della UE: gli Stati membri sono tenuti a tutelare le opere d'arte nel territorio dell'Unione, indipendentemente dal paese d'origine di tali opere o dalla cittadinanza del loro autore.

La Vitra, una società svizzera che fabbrica mobili di design, è titolare di diritti di proprietà intellettuale su talune sedie concepite dai coniugi, nel frattempo deceduti, Charles e Ray Eames, cittadini degli Stati Uniti d'America. Tra tali mobili, figura in particolare la Dining Sidechair Wood, realizzata nell'ambito di un concorso di progettazione di mobili organizzato dal Museum of Modern Art di New York (Stati Uniti) ed esposta in tale museo a partire dal 1950.

La società Kwantum, che gestisce, nei Paesi Bassi e in Belgio, una catena di negozi di mobili per interni, ha commercializzato una sedia, denominata «sedia Paris», in asserita violazione dei diritti d'autore della Vitra sulla Dining Sidechair Wood. Quest'ultima ha adito i giudici dei Paesi Bassi al fine, in particolare, di far cessare tale commercializzazione. In tale contesto, la Corte suprema dei Paesi Bassi ha deciso di sottoporre questioni pregiudiziali alla Corte di giustizia relative alla tutela, ai sensi della direttiva europea sulla tutela del diritto d'autore n. 2001/29 di cui può godere, all'interno dell'Unione, un'opera delle arti applicate proveniente da un paese terzo e il cui autore non è un cittadino di uno Stato membro.

Nel diritto internazionale, la Convenzione di Berna sul diritto d'autore prevede che gli autori che siano cittadini dei paesi firmatari godono, negli altri paesi firmatari, in linea di principio, degli stessi diritti degli autori nazionali. Un'eccezione a tale principio riguarda tuttavia la tutela delle opere delle arti applicate. A tal riguardo, le parti contraenti hanno stabilito una clausola di reciprocità sostanziale secondo cui le opere delle arti applicate originarie dei paesi nei quali simili opere sono protette unicamente in quanto disegni o modelli non possono rivendicare, negli altri paesi firmatari, il cumulo di tale protezione con la tutela del diritto d'autore. A tal riguardo, la questione sottoposta dalla Corte suprema dei Paesi Bassi alla Corte di giustizia è se gli Stati membri siano ancora liberi di applicare, alle opere delle arti applicate originarie dei paesi terzi, la clausola di reciprocità sostanziale, contenuta nella Convenzione di Berna, che protegge tali opere soltanto in forza di un regime speciale, sebbene il legislatore dell'Unione non abbia previsto una tale limitazione.

Nella sua sentenza, la Corte di giustizia risponde in senso negativo: nell'ambito di applicazione della direttiva 2001/29, gli Stati membri non sono più competenti ad attuare le disposizioni pertinenti della Convenzione di Berna. Innanzitutto, la Corte chiarisce a tal riguardo che una situazione in cui una società rivendica una tutela in forza del diritto d'autore di un oggetto delle arti applicate commercializzato in uno Stato membro, purché un siffatto oggetto possa essere qualificato come «opera», ai sensi della direttiva 2001/29, rientra nell'ambito di applicazione materiale del diritto dell'Unione.

La Corte constata poi che il legislatore dell'Unione, adottando tale direttiva, ha necessariamente preso in considerazione tutte le opere per le quali viene richiesta la tutela nel territorio dell'Unione, dato che, peraltro, detta direttiva non include criteri relativi al paese d'origine di tali opere o alla cittadinanza dei loro autori. La Corte aggiunge che l'applicazione della clausola di reciprocità sostanziale contenuta nella Convenzione di Berna rimetterebbe in discussione l'obiettivo della direttiva 2001/29, che consiste nell'armonizzazione del diritto d'autore nel mercato interno, poiché, in applicazione di detta clausola, le opere delle arti applicate originarie dei paesi terzi potrebbero essere trattate in maniera diversa in differenti Stati membri.

8 Novembre 2024 – Corte di Giustizia UE: la direttiva relativa alla tutela giuridica dei programmi per elaboratore non consente al titolare di tale tutela di impedire la commercializzazione da parte di un terzo di un software che si limiti a modificare il contenuto di talune variabili inserite temporaneamente nella memoria RAM di una consolle per videogiochi.

La Sony commercializza consolle per videogiochi PlayStation e giochi per tali consolle. Fino al 2014, essa vendeva tra l'altro la consolle PlayStationPortable nonché il videogioco «MotorStorm: Arctic Edge». La Sony ha convenuto in giudizio dinanzi a organi giurisdizionali tedeschi la società Datel, la quale distribuisce taluni software e un dispositivo che sono compatibili con tale PlayStation e offrono all'utilizzatore opzioni di gioco non previste nell'attuale fase del videogioco da parte della Sony. La Sony ritiene che questi prodotti della Datel abbiano l'effetto di modificare i software su cui si basa il suo videogioco e pertanto violino il suo diritto esclusivo di autorizzare modifiche di questo tipo. Essa ha dunque chiesto a tali organi giurisdizionali di vietare alla Datel la commercializzazione dei prodotti in questione e di condannarla al risarcimento del danno asseritamente subito.

La Corte federale di giustizia tedesca (BGH) ha chiesto alla Corte di giustizia di interpretare la direttiva relativa alla tutela giuridica dei programmi per elaboratore. Il BGH osserva che il software della Datel è installato dall'utilizzatore sulla PlayStation ed è eseguito contemporaneamente al software di gioco. Esso non modifica o non riproduce né il codice oggetto, né il codice sorgente, né la struttura interna e l'organizzazione del software della Sony, ma si limita a modificare il contenuto delle variabili temporaneamente inserite dai videogiochi della Sony nella memoria RAM della consolle, che sono utilizzate durante l'esecuzione del videogioco. Pertanto, il videogioco viene eseguito sulla base di tali variabili dal contenuto modificato.

Con la sentenza nella causa *C-159/23 | Sony Computer Entertainment Europe,* la Corte dichiara che non rientra nell'ambito della tutela conferita dalla direttiva il contenuto dei dati variabili inseriti da un programma per elaboratore nella memoria RAM di un elaboratore e utilizzati da detto programma durante la sua esecuzione, nei limiti in cui questo contenuto non consenta la riproduzione o la realizzazione di tale programma in una fase successiva. Infatti, la direttiva tutela soltanto la creazione intellettuale quale essa si riflette nel testo del codice sorgente e del codice oggetto del programma per elaboratore. Per contro, la direttiva non tutela le funzionalità di tale programma né gli elementi mediante i quali gli utilizzatori sfruttano tali funzionalità, se questi ultimi non consentono una riproduzione o una realizzazione di detto programma in una fase successiva.