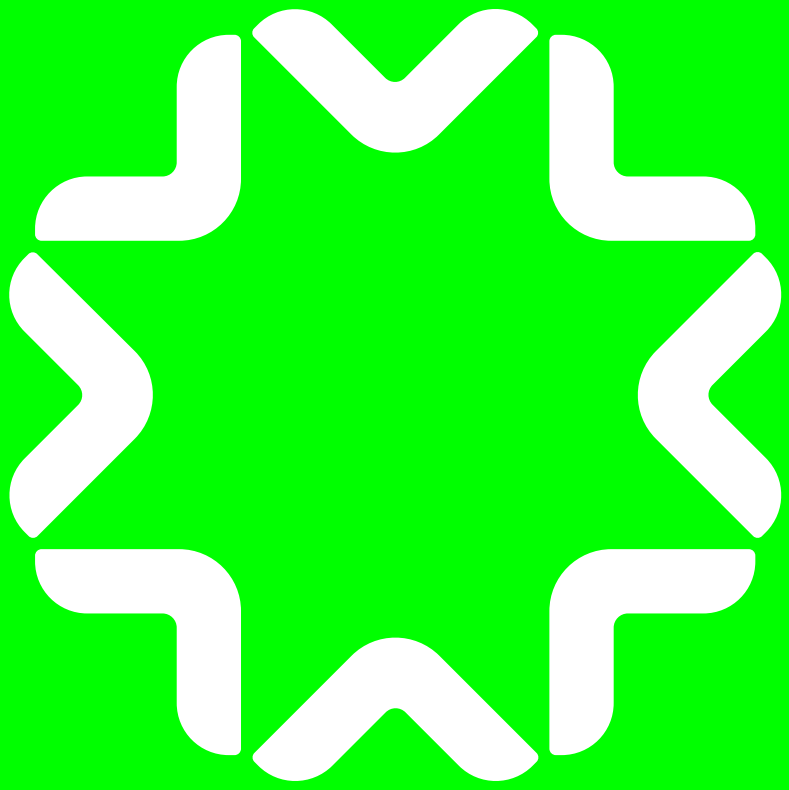
ITALIAN
TECH
ALLIANCE

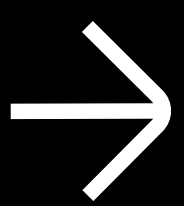


European Digital Strategy

2025

Indice dei contenuti

1 Introduzione e Contesto



AI Act:
L’inizio di una nuova era nella regolamentazione dell’Intelligenza Artificiale

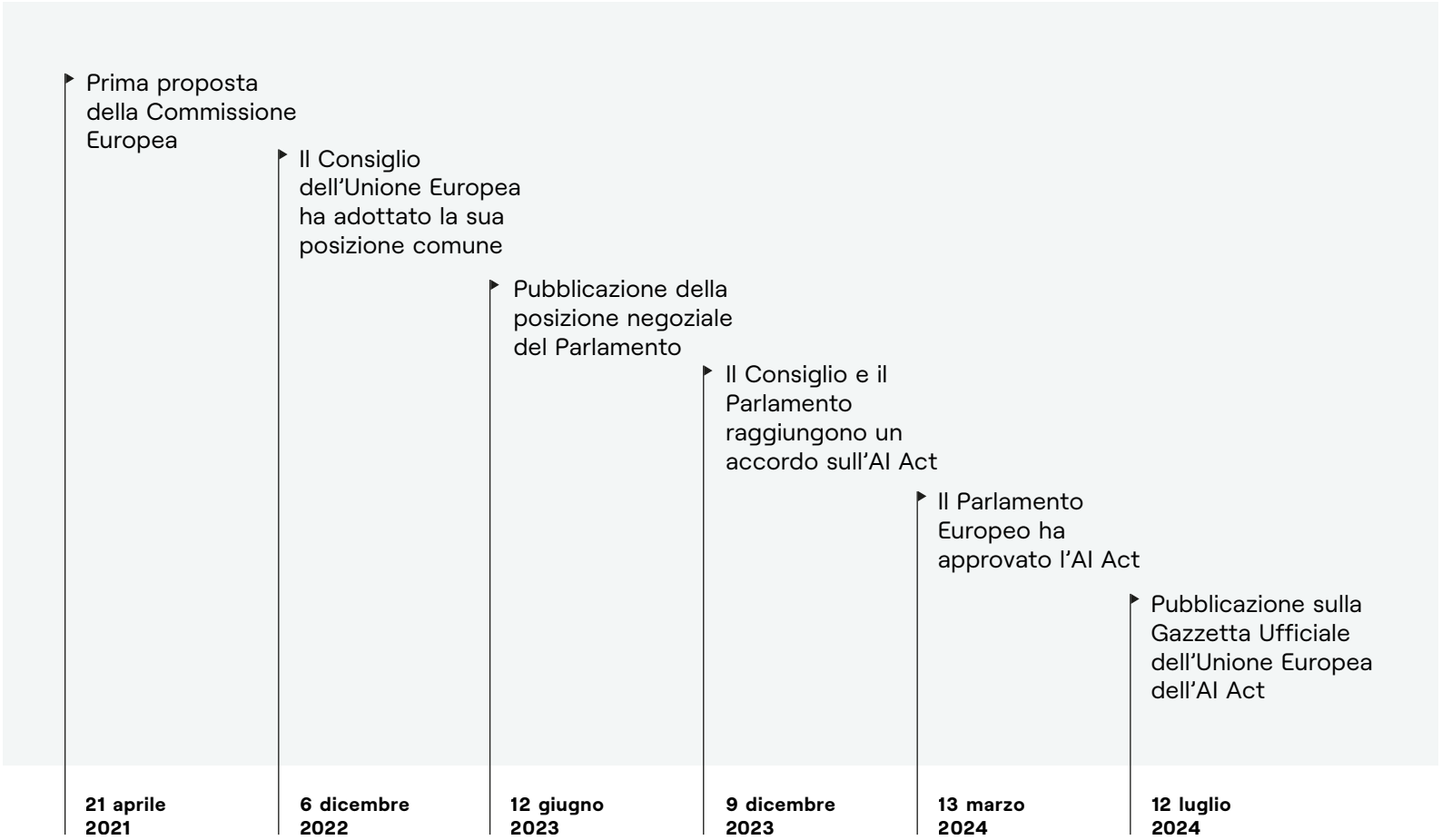
1.1 Introduzione all'AI Act

L'AI Act[1] è la **primissima legge** volta a regolamentare **lo sviluppo, la commercializzazione e l'uso di sistemi di intelligenza artificiale**, che rappresenta un **modello** di ispirazione anche per gli altri regolatori mondiali. Diversi sono stati i passaggi che hanno portato allo stadio attuale:

[1] Ovvero il Regolamento (UE) del 13 giugno 2024

Grafico 1.1

Grafico 1.1
Timeline dello sviluppo dell'AI Act nel corso del tempo



1.2 Obiettivi dell'AI Act

Quali sono gli obiettivi dell'AI Act?

→ Garantire la protezione dei **diritti fondamentali** sanciti dalla Carta dell'Unione Europea quali, ad esempio, la libertà, la non discriminazione, il diritto alla **salute** e alla **sicurezza** dei cittadini dell'Unione Europea, nonché la tutela dell'ambiente, lo Stato di diritto e la democrazia.

→ Assicurare l'adozione di sistemi AI che siano **affidabili**, **trasparenti** e **non lesivi** per l'uomo, al fine di creare fiducia nel loro utilizzo e incentivarne la circolazione in quanto sistemi sicuri.

→ Promuovere l'**innovazione**, creando un mercato unico e facilitando la libera circolazione dei sistemi AI conformi alle norme UE.

1.3 Ambito di Applicazione dell'AI Act

A chi si applica l'AI Act?[2]

→ **Fornitori (provider) di sistemi di IA**, che immettono sul mercato o mettono in servizio modelli AI, sia che siano stabiliti o ubicati nell'UE o in un paese terzo.

→ **Operatori (deployer) e soggetti che utilizzano, sotto la propria autorità, sistemi di AI**, che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione. Esempio: il medico che utilizza una macchina governata da AI per realizzare un'operazione chirurgica.

→ **Provider e deployer di sistemi AI** che hanno lo stabilimento o sono situati al di fuori dell'UE, **quando i sistemi AI producono output in UE.**

→ **Importatori e distributori di sistemi AI.**

→ **Fabbricanti** che immettono sul mercato o mettono in servizio sistemi di AI con il loro prodotto e con il loro marchio;

→ **Rappresentanti** autorizzati di fornitori, non stabiliti nell'UE.

→ **Persone interessate che si trovano in UE.**

Sono **esclusi** dall'applicazione i sistemi di AI utilizzati per: scopi militari, di difesa o sicurezza nazionale e per scopi di ricerca e sviluppo scientifici (ad esempio in ambito accademico).

[2] Art. 2 AI Act

2 Definizioni e Concetti Chiave

Comprendi i fondamentali: Decodificare il linguaggio dell’ Intelligenza Artificiale

2.1 Definizione di “Sistema di Intelligenza Artificiale”

Il “sistema di IA” è un sistema automatizzato progettato per operare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce, dall’input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. [2]

[2] Art 3 AI Act

2.2 Concetto di Rischio nell’AI Act

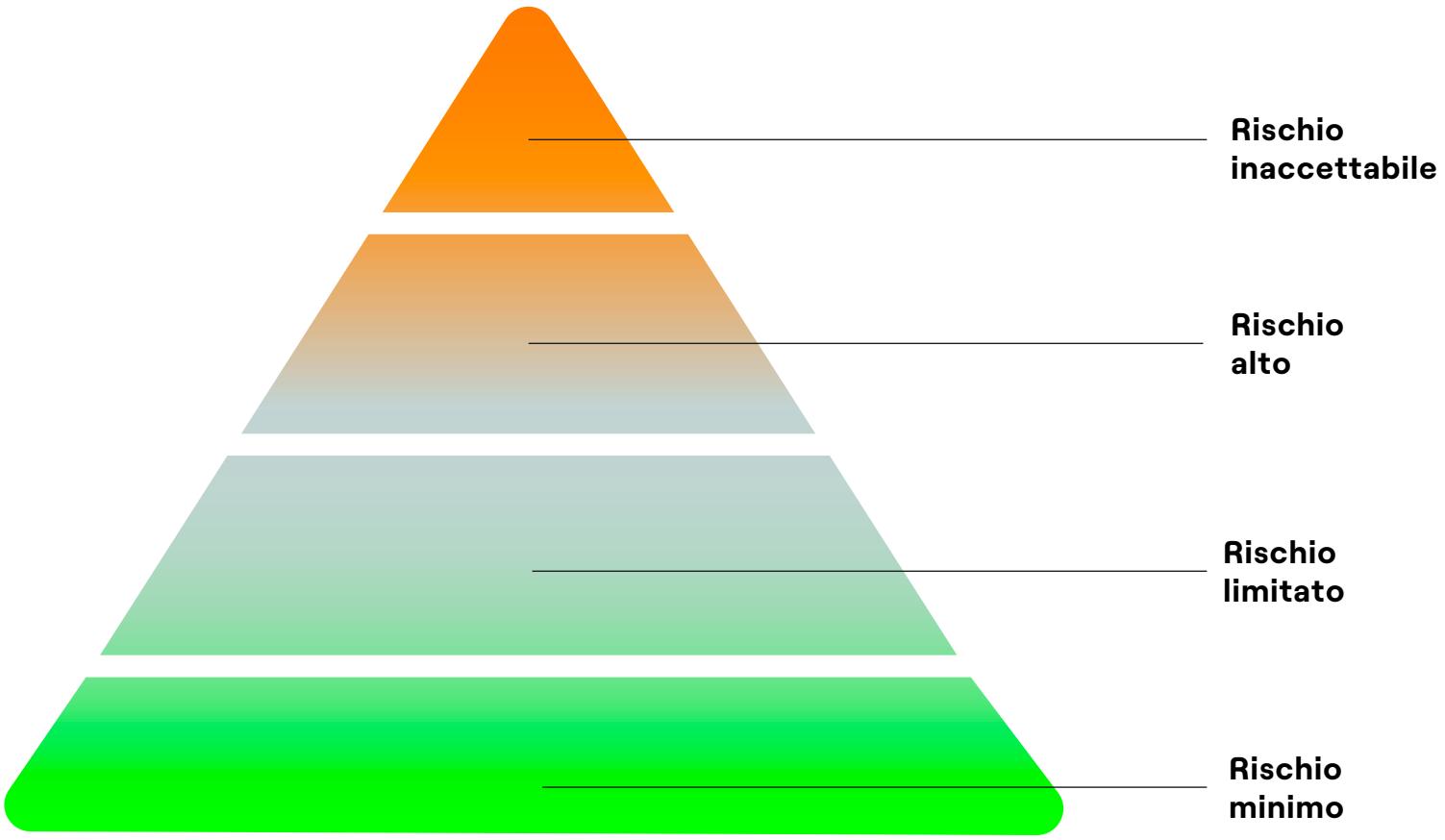
L’AI Act si fonda su un approccio basato sul **rischio** e, in particolare, relativamente al rischio che determinati sistemi di AI possono cagionare ai **diritti fondamentali della persona**. I sistemi di AI vengono quindi classificati in **categorie**, con diversi obblighi e divieti a seconda del livello di rischio individuato:

Grafico 2.1
Schema piramidale di classificazione del rischio nell’AI Act

= rischio inaccettabile/alto

= rischio limitato/minimo

Grafico 2.1



3 Norme e Regolamentazioni

Naviga tra le regole:
Le normative che plasmano il futuro dell’IA

3.1 Pratiche di AI Vietate

Grafico 3.1

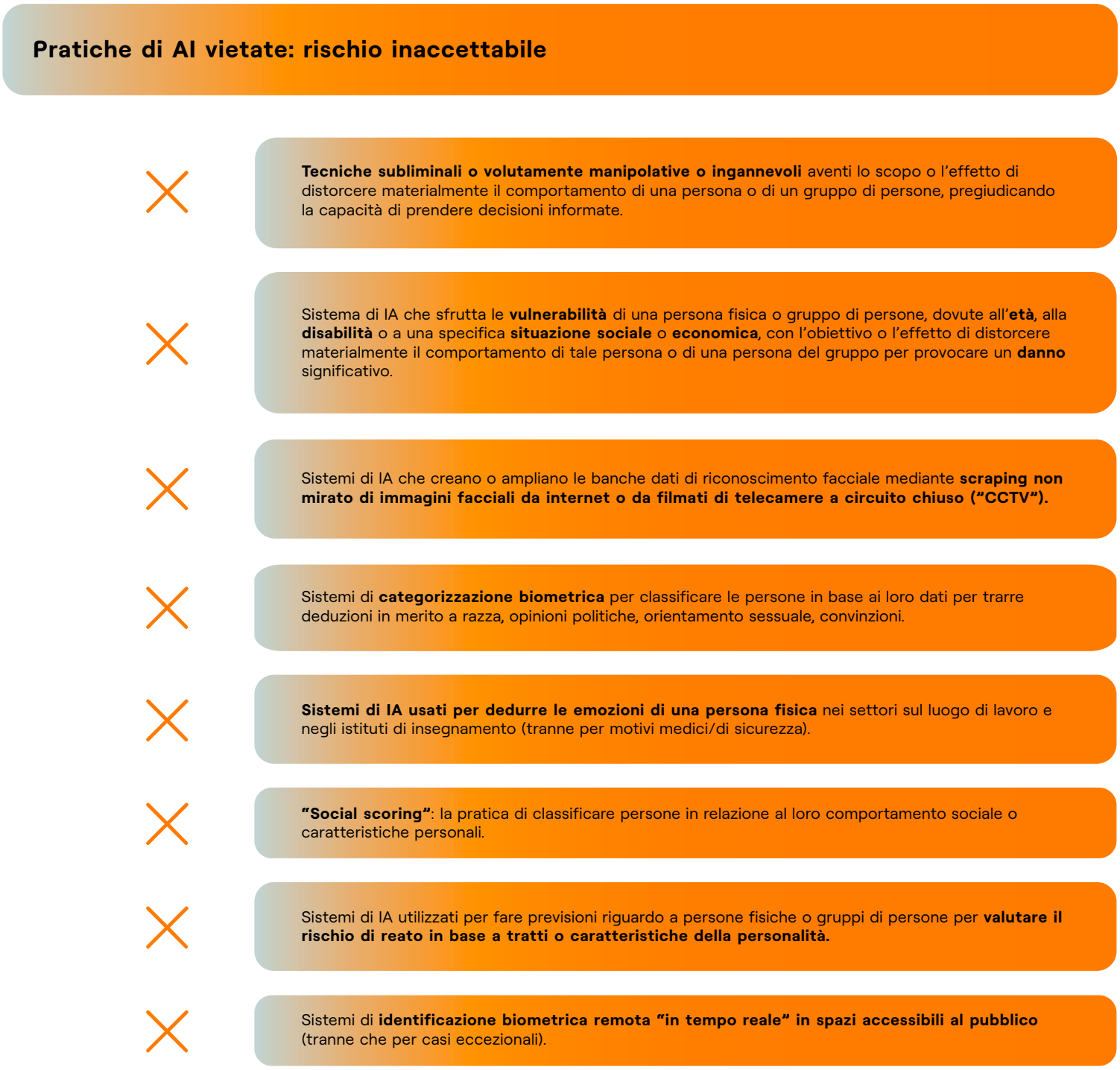


Grafico 3.1
Elenco delle principali pratiche di AI vietate in base all'entità del rischio

= rischio inaccettabile

3.2 Sistemi AI ad Alto Rischio

Grafico 3.2

Grafico 3.2
Schema di definizione dei vari sistemi di AI ad alto rischio.

= rischio alto

3.3 Requisiti e Obblighi per i Sistemi AI ad Alto Rischio

Quali i requisiti e gli obblighi per i sistemi AI ad alto rischio?

Grafico 3.3

Sistema di gestione dei rischi

Implementazione e mantenimento di un **sistema di gestione dei rischi**, finalizzato ad individuare potenziali rischi e adottare azioni finalizzare a mitigarli.

Tracciabilità

Conservazione delle registrazioni degli eventi (“**log**”) durante l’attivazione del sistema.

Accuratezza, robustezza, cybersicurezza

Raggiungimento di adeguati livelli di accuratezza, robustezza, cybersicurezza del sistema.

Sorveglianza Umana

Supervisione tramite misure di sorveglianza umana per minimizzare i rischi e consentire agli utenti di comprendere il sistema.

Registrazione

In determinati casi, prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio, ove applicabile, si registra nella banca dati dell’UE.

Data Governance

Sviluppo del sistema sulla base di **set di dati** che alimentino il sistema, dati di convalida e test, se il sistema prevede l’addestramento di dati.

Documentazione Tecnica

Produzione di **documentazione tecnica** contenente le informazioni necessarie alle autorità per valutare la conformità del sistema AI, da tenere aggiornata.

Trasparenza

Garanzia di trasparenza e fornitura di istruzioni.

Dichiarazione di conformità

Dichiarazione che identifica il sistema AI e la conformità dello stesso ai requisiti, da tenere aggiornata.

Marcatura CE

La marcatura CE apposta sul sistema di AI ad alto rischio in modo visibile, leggibile e indelebile o accessibile per i sistemi digitali.

Grafico 3.3
Schema di definizione di rischi e obblighi per i sistemi AI ad alto rischio

= rischio alto

3.4 Sistemi con Rischio Limitato e Minimo

Grafico 3.4

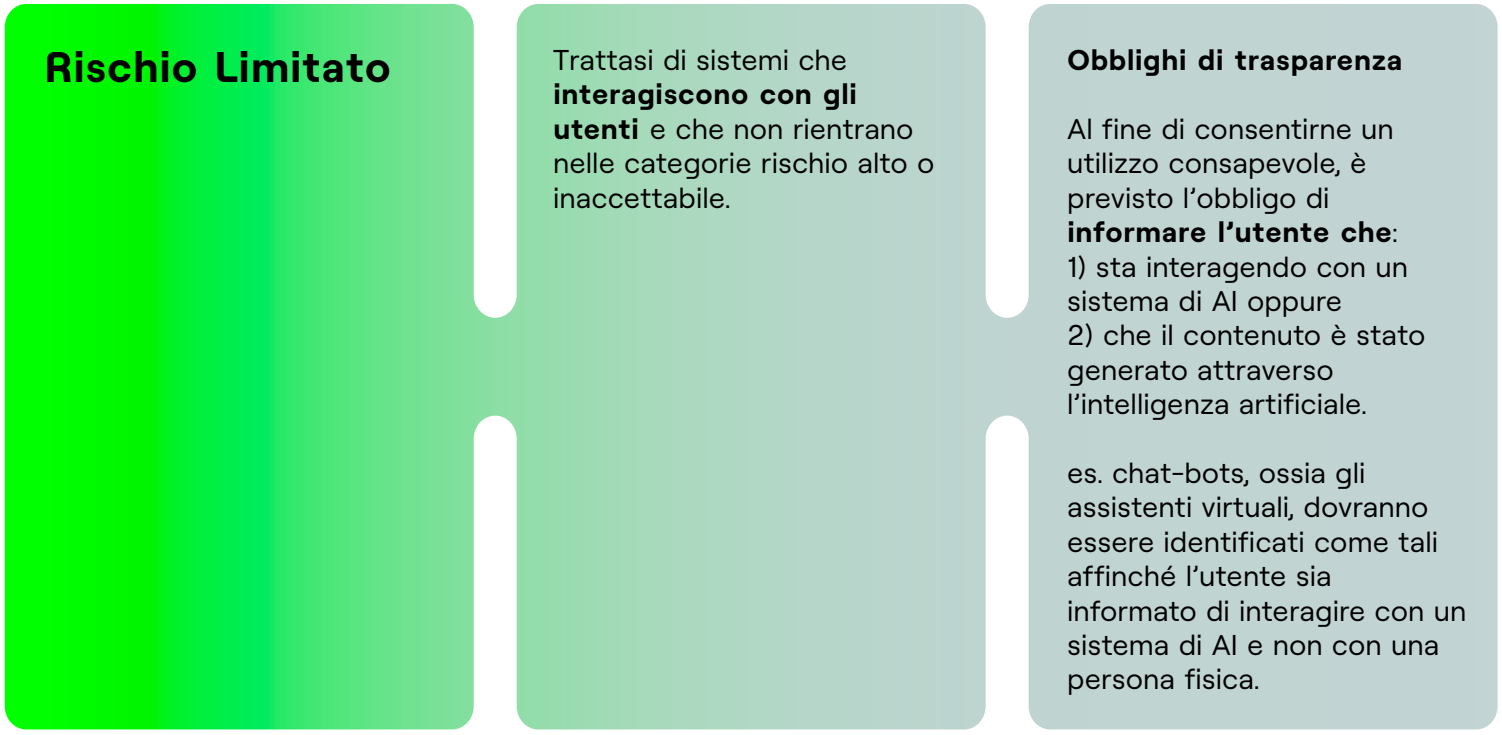


Grafico 3.4
Schema di definizione dei sistemi a rischio limitato

= rischio limitato

Grafico 3.5

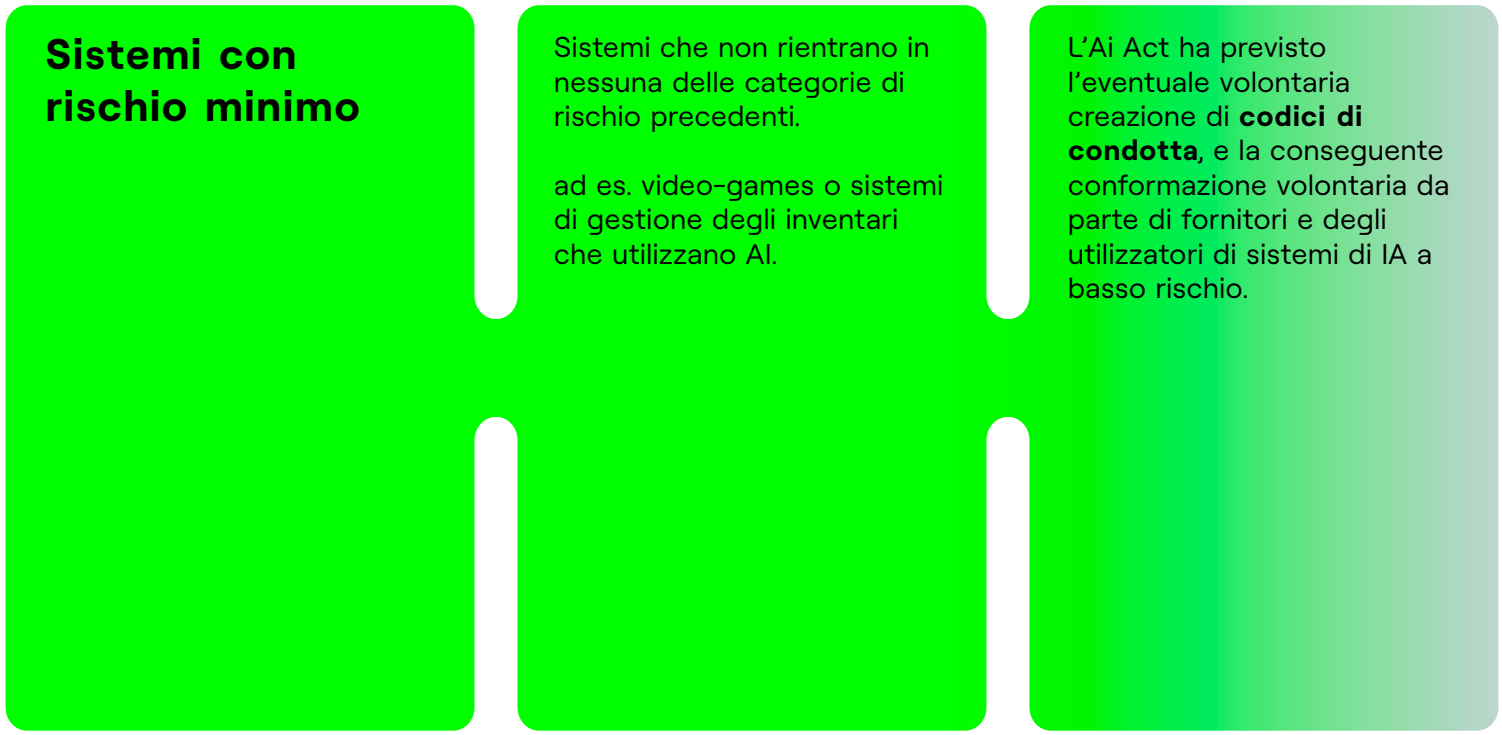


Grafico 3.5
Schema di definizione dei sistemi a rischio a rischio minimo

= rischio minimo

4 Focalizzazioni Specifiche

Focus mirati: Un’occhiata ravvicinata ai sistemi di IA per usi speciali

4.1 Focus sui Sistemi di AI per Finalità Generali (GPAI)

Esempi: sistemi di AI generativa come *ChatGpt; Midjourney.*

Per sistema **GPAI** si intende un sistema di AI per scopi generali, che ha la capacità di servire a una molteplicità di scopi, sia per uso diretto che per l'integrazione in altri sistemi di AI, rispecchiando le capacità cognitive degli esseri umani. Questi sistemi, infatti, operando sulla base del machine learning e deep learning, utilizzando algoritmi per analizzare ampissimi set di dati e apprendendo le informazioni ricevute per elaborare risultati; per loro natura portano con sé molteplici rischi sistemici (es. violazione di diritti fondamentali della persona, diritto d'autore).

La Commissione europea ritiene che, allo stato attuale della tecnologia, i modelli di AI per finalità generali che sono stati addestrati utilizzando una **potenza di calcolo totale superiore a 10^25 FLOPS** comportino rischi sistemici. Tali sistemi devono essere notificati alla Commissione UE.

Al fine di prevenire i potenziali rischi, tutti i fornitori di sistemi GPAI **devono**:

- → Redigere **documentazione tecnica**, compreso il processo di formazione e test e i risultati della valutazione.
- → Raccogliere informazioni e **documentazione da fornire ai fornitori di sistemi** che intendono integrare il sistema GPAI nel proprio sistema di IA in modo tale che quest'ultimo comprenda capacità e limiti e sia in grado di conformarsi.
- → Stabilire una policy per **rispettare la direttiva sul diritto d'autore**.
- → Pubblicare un **riepilogo sufficientemente dettagliato sul contenuto usato per l'addestramento** del sistema GPAI.

Tutti i fornitori di sistemi GPAI possono dimostrare il rispetto dei loro obblighi se aderiscono volontariamente a un codice etico fino alla pubblicazione di norme armonizzate europee, il cui rispetto comporterà una presunzione di conformità. I fornitori che non aderiscono ai codici di condotta devono dimostrare **metodi alternativi adeguati di conformità** per l'approvazione della Commissione.

4.2 Casistica e Sistemi di AI Generativa

→ Sistemi di **AI** specificatamente destinati a generare, con diversi livelli di autonomia, contenuti come testi complessi, immagini, audio o video (“**AI generativa**”):

Grafico 4.1

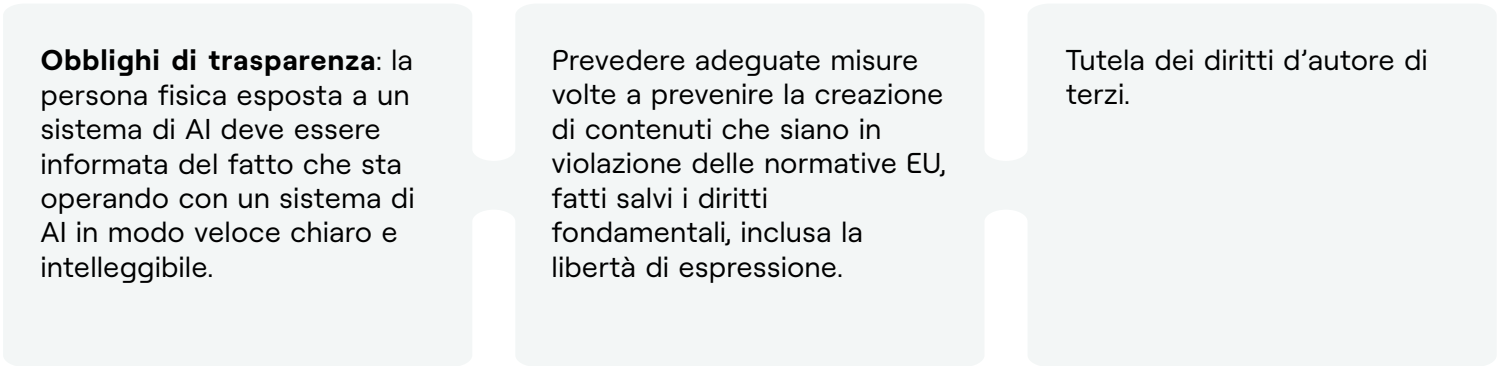


Grafico 4.1
Schema di definizione degli obblighi di trasparenza verso gli utenti di sistemi di AI.

→ Sistemi che riconoscono le **emozioni dei dipendenti** per valutare lo stress sul posto di lavoro sfruttando l’accesso alla *web cam* **vietati**:

→ Sistemi che si occupano di **selezionare Curriculum Vitae di potenziali candidati**:

Grafico 4.2

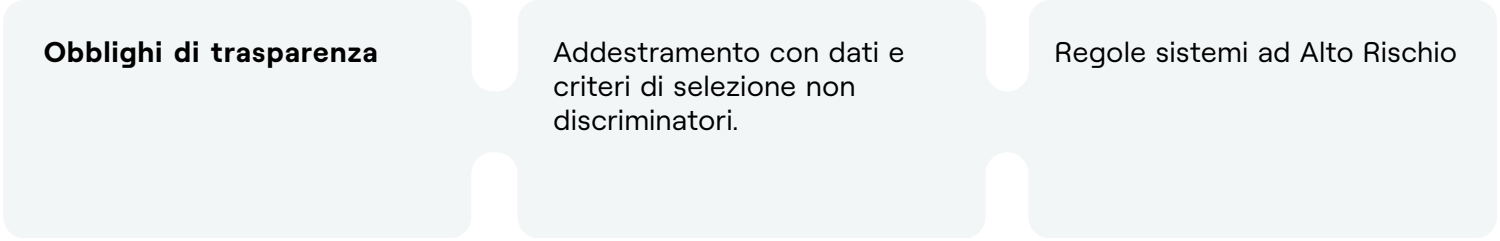


Grafico 4.2
Schema di definizione delle modalità e obblighi di AI di selezione in ambito lavorativo.

5 Conformità e Sanzioni

Essere conformi conviene:
Scopri le sanzioni e
come evitarle

5.1 Sanzioni

L'AI Act prevede sanzioni significative per le violazioni dell'AI Act, fissate in una **percentuale** del **fatturato annuo globale** nell'anno finanziario precedente o in un importo predeterminato (in base al più elevato).

Gli Stati membri dovranno stabilire **sanzioni effettive**, proporzionate e dissuasive, comprese sanzioni amministrative pecuniarie, in relazione alle violazioni, e comunicarle alla Commissione, per i sistemi di IA immessi sul mercato o messi in servizio che non rispettano i requisiti dell'AI Act. Le soglie da tenere in considerazione secondo l'Ai Act vanno da **35 milioni di euro** (o al **7%** del fatturato mondiale totale annuo) a **7,5 milioni di euro** o all'**1% del fatturato mondiale** totale annuo, con l'applicazione della soglia più bassa per la violazione in questione per le sole PMI.

L'AI Act ha istituito il Comitato europeo per l'intelligenza artificiale (EAIB) e l'Ufficio europeo per l'IA, entità che avranno il compito di stabilire linee guida, condividere strategie efficaci e garantire che l'applicazione della normativa venga applicata in modo coerente in tutti gli Stati membri dell'UE.

5.2 Fasi di Entrata in Vigore

Il regolamento sull'IA è entrato in vigore lo scorso **2 agosto**, ovvero venti giorni dopo la sua pubblicazione nella Gazzetta ufficiale dell'Unione Europea, e sarà pienamente applicabile nei **due anni** successivi.

Grafico 5.1
Delineamento cronologico delle fasi di entrata in vigore dell'AI Act.

Grafico 5.1

6 mesi	12 mesi	24 mesi	36 mesi
6 mesi dopo l'entrata in vigore, gli Stati membri devono eliminare i sistemi vietati (già in vigore dallo scorso 2 febbraio 2025).	12 mesi dopo diventano applicabili gli obblighi relativi ai sistemi ad alto rischio e dell'IA per finalità generali.	24 mesi dopo tutte le regole della legge sull'IA diventano applicabili, compresi gli obblighi per i sistemi ad alto rischio definiti nell'allegato III (elenco dei casi d'uso ad alto rischio).	36 mesi dopo si applicano gli obblighi per i sistemi ad alto rischio definiti nell'allegato II (elenco della normativa di armonizzazione dell'Unione).
6 mesi	**12 mesi**	**24 mesi**	**36 mesi**

5.3 To Do List per le aziende

Cosa devono fare le società per assicurarsi di agire in conformità alle regole stabilite dall'AI Act?

Stabilire se esse **utilizzano** o **intendono utilizzare** un sistema di intelligenza artificiale nella propria attività.

Individuare un **livello di rischio** e gli specifici rischi che il proprio sistema di AI può potenzialmente figurare.

Una volta stabilito il livello di rischio, agire di conseguenza:

Grafico 5.2

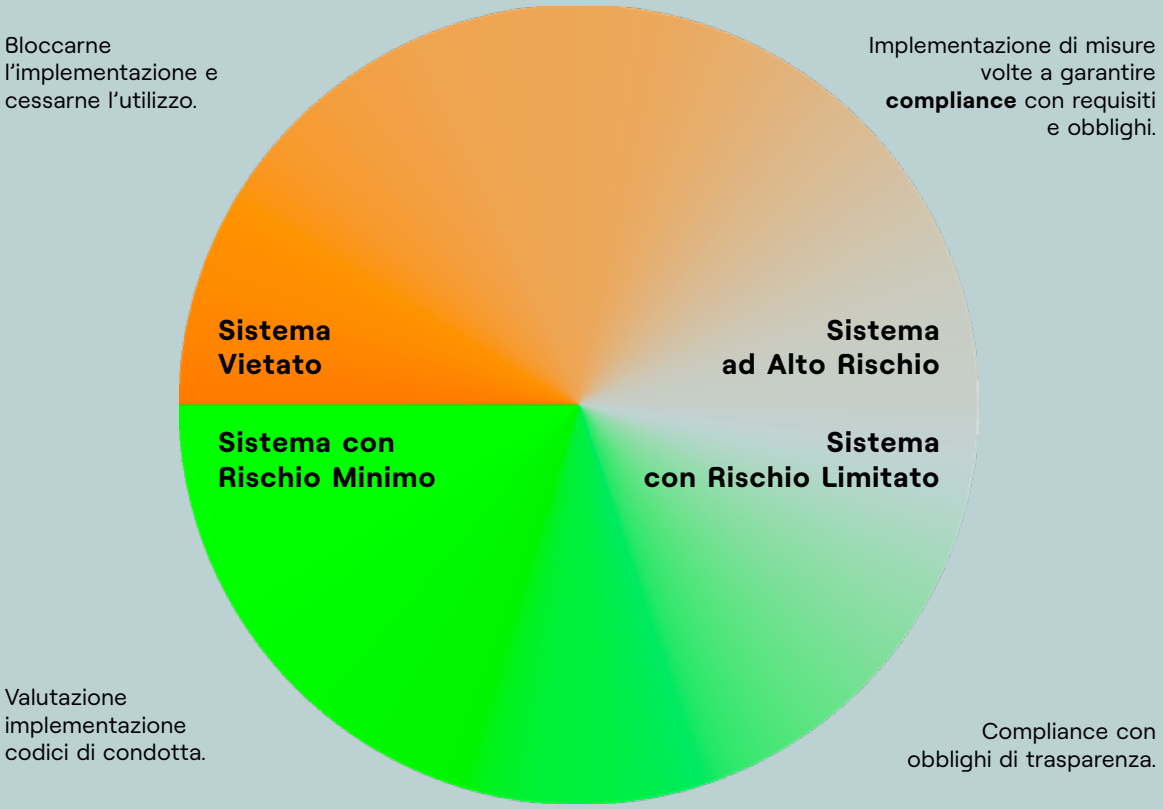
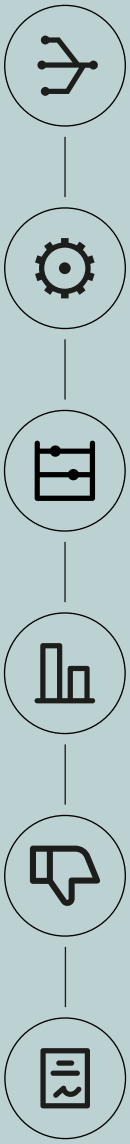


Grafico 5.2
Definizione delle azioni da fare per stabilire la conformità del proprio sistema di AI

= rischio inaccettabile/alto

= rischio limitato/minimo

In linea generale:



Mappare i processi interni, verificando il livello **di conformità** del proprio sistema di AI alle nuove regole.

Implementare policy e **sistemi di governance** dell'AI, con standard di sicurezza e trasparenza, garantendo un **monitoraggio** e una **supervisione** adeguati durante tutto il ciclo di vita del sistema di AI.

Stabilire degli efficaci meccanismi di supervisione umana, **formando** in tal senso il personale interno.

Proteggere adeguatamente il proprio **know-how** e i segreti commerciali; mantenere tutta la **documentazione** necessaria relativa al sistema di AI.

Garantire che il sistema di AI e la sua implementazione siano **privi di meccanismi discriminatori** e non violino norme sulla **privacy** e i **diritti IP** di terzi.

Includere nei contratti con i terzi (in particolare fornitori) l'obbligo di rispettare l'AI Act.

6 Iniziative Nazionali

Italia in prima linea: le iniziative che guidano l’innovazione nell’IA

6.1 Iniziative in Italia

Legge sull'Intelligenza Artificiale (bozza):

Lo scorso 23 Aprile 2024 il Consiglio dei Ministri ha approvato il DDL in materia di Intelligenza Artificiale.

Le norme intervengono in cinque ambiti: la strategia nazionale, le autorità nazionali, le azioni di promozione, la tutela del diritto di autore, le sanzioni penali.
I principi posti alla base della normativa richiamano quelli stabiliti dall'AI Act (es. rispetto dei diritti fondamentali, trasparenza, sicurezza, riservatezza). Sono previste molteplici disposizioni nei seguenti settori:

Sanità e disabilità: I) accessibilità e AI in ambito sanitario e di disabilità; II) ricerca e sperimentazione scientifica in ambito sanitario; III) disposizioni in materia di fascicolo sanitario elettronico; IV) sistemi di sorveglianza nel settore sanitario e governo della sanità digitale.

Lavoro: I) disposizioni sull'utilizzo di AI in materia di lavoro; II) istituzione di un Osservatorio sull'adozione di sistemi di AI nel mondo del lavoro.

Pubblica Amministrazione: regolamentazione dell'utilizzo dell'AI da parte della PA per garantire efficienza e buon andamento.

Attività giudiziaria: utilizzo dell'AI consentito esclusivamente per l'organizzazione e la semplificazione del lavoro giudiziario, per la ricerca giurisprudenziale e dottrinale.

Cybersicurezza nazionale: utilizzo dell'AI come risorsa per rafforzare la cybersicurezza nazionale.

Aumento pena per i reati commessi utilizzando sistemi di AI a determinate condizioni.

Strategia Italiana sull'Intelligenza Artificiale per il 2024-2026 (Agenzia Italiana per il Digitale – AGID)

Settori di intervento:

→ ricerca scientifica;
→ amministrazione pubblica;
→ imprese;
→ educazione.

7 Nuove normative

Le regole dell’AI: la chiave per un futuro sicuro e giusto

7.1 La responsabilità da danno cagionato dai sistemi di Intelligenza Artificiale

L'Unione Europea ha predisposto una serie di norme che combinano "**sicurezza**" (con una protezione *ex ante*) e "**responsabilità**" (con una protezione *ex post*) nell'uso dei sistemi di intelligenza artificiale.
Se al fine di tutelare la sicurezza ex ante si pone l'AI Act, riguardo invece alla protezione ex post è stata adottata la direttiva sulla responsabilità per danno da prodotti difettosi.

→ Tale normativa ha modificato l'attuale quadro della responsabilità civile per danni da danno da prodotto difettoso, adeguando le norme in materia di responsabilità all'era digitale e all'intelligenza artificiale. L'AI Act e la nuova norma promuoveranno l'utilizzo dell'AI e fiducia nei medesimi sistemi, garantendo che le eventuali vittime di danni cagionati dai sistemi siano effettivamente risarcite in caso di danni, nonostante i requisiti preventivi della legge sull'IA e di altre norme di sicurezza.

Diversi, infatti, possono essere i casi in cui l'Intelligenza Artificiale può cagionare un danno e molteplici gli **interrogativi**, in particolare sull'attribuzione di responsabilità:

Grafico 7.01
Esempi di attribuzione di responsabilità al fattore umano/ artificiale in casistiche specifiche.

= la sfumatura indica la linea logica di lettura

Grafico 7.01

Un medico che si avvale di uno strumento di robotica che incorpora un sistema di AI che cagiona un danno al paziente.	Il fallimento di un colloquio di lavoro a causa di un software che valuta le candidature che riveli un effetto discriminatorio.	Un avvocato che perde una causa in quanto cita casi giurisprudenziali inesistenti e inventati da un sistema di AI generativa.
La responsabilità ricade sul produttore? Sul medico? Sulla struttura?	**La responsabilità ricade sul soggetto che ha utilizzato il sistema? Su chi ha raccolto i dati? Sul fornitore?**	**L'avvocato è responsabile?**

7.2 Product Liability Directive (2024/2853)

Lo scorso 8 dicembre 2024 è entrata in vigore la nuova direttiva sulla responsabilità per danno da prodotti difettosi. La revisione della precedente normativa, in vigore dal 1985, ha avuto origine da una proposta presentata lo scorso Settembre 2022, e si è resa necessaria alla luce dell'emersione di molteplici nuove tecnologie e alla diffusione ormai capillare del mercato digitale che hanno determinato il sorgere di nuove problematiche.

Tale nuova normativa avrà certamente un impatto anche sull'operatività e sui potenziali danni cagionati dai sistemi di AI. I punti di innovazione principale di tale normativa si identificano con i seguenti:

Grafico 7.02

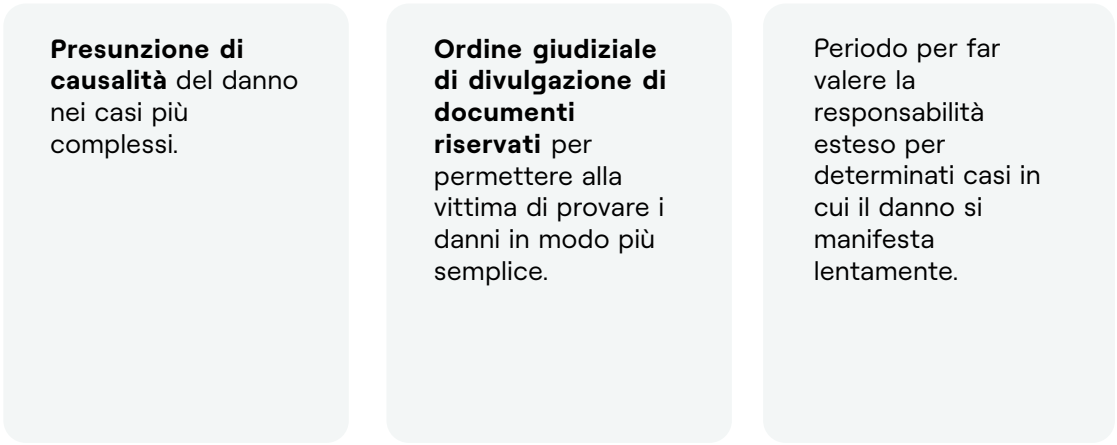


Grafico 7.02
Punti di innovazione della Product Liability Directive.

Richieste di risarcimento facilitate per le vittime

→ La direttiva aggiornata semplifica i requisiti dell'onere della prova per le vittime che richiedono il risarcimento del danno, eliminando la soglia minima di danno di 500 euro.

→ Mentre, normalmente, l'attore avrebbe dovuto dimostrare che il prodotto era difettoso e che tale difetto aveva cagionato il danno, ora viene introdotta una **presunzione di causalità** per cui il tribunale può presumere che il prodotto sia difettoso, salva comunque la possibilità per le aziende di provare il contrario.
Il nesso di causalità è presunto quando:
- il danno è generalmente compatibile con il difetto in questione;
- la complessità tecnica o scientifica causa un'eccessiva difficoltà nel dimostrare la responsabilità (es. sistemi AI "*black box*", ovvero sistemi con meccanismi interni invisibili all'utente, impossibile esaminarne e il codice o la logica sottostante).

→ Il tribunale può altresì ordinare all'azienda di **divulgare le prove**

“necessarie e proporzionate” per aiutare le vittime nelle loro richieste di risarcimento danni, fermo restando il diritto delle aziende a preservare determinate informazioni confidenziali.
Le nuove norme consentono inoltre alle autorità nazionali per la tutela dei consumatori di fornire ai consumatori un aiuto supplementare.

→ I consumatori potranno ottenere un risarcimento non solo per i danni materiali, ma anche per le perdite *immateriali*, compresi i **danni alla salute psicologica** riconosciuti dal punto di vista medico.

→ Infine, la nuova normativa garantisce inoltre che anche coloro che subiscono danni sotto forma di **dati distrutti o corrotti** (ad esempio quando i file vengono cancellati da un disco rigido) abbiano diritto a un risarcimento.

Responsabilità estesa per danni che si manifestano lentamente

→ Secondo la nuova normativa, deve sempre esserci una società avente con sede nell’UE, come un produttore, un importatore o un loro rappresentante autorizzato, che possa essere **ritenuto responsabile per i danni causati da prodotti difettosi**. Tale regola si applica anche ai prodotti acquistati online al di fuori dell’UE, mentre non si applicheranno al *software open source*.

→ Il periodo di responsabilità è esteso a 25 anni in casi eccezionali in cui i sintomi sono lenti a manifestarsi. Se il procedimento giudiziario è stato avviato entro tale periodo, la vittima del danno potrà comunque ottenere un risarcimento dopo tale periodo.

Keypoints

Le nuove norme si applicheranno ai prodotti immessi sul mercato 24 mesi dopo l’entrata in vigore della direttiva.

7.3 Regolamento (UE) 2022/868 relativo alla governance europea dei dati

1. Introduzione

Il Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio relativo alla *governance* europea dei dati e che modifica il Regolamento (UE) 2018/1724, pubblicato sulla Gazzetta Ufficiale dell'Unione europea il 3 giugno 2022 (il "**DGA**") è entrato in vigore il 23 giugno 2022 ed è applicabile in ciascuno Stato membro dal 24 settembre 2023.

Il DGA è parte della strategia digitale della Commissione europea volta all'implementazione di una trasformazione digitale comunitaria modellata sui diritti fondamentali, sui valori e sulle norme dell'Unione europea, che mira, fra l'altro, alla creazione di uno spazio comune europeo dei dati e di una *data economy* efficiente ed innovativa.

Il DGA si pone come obiettivo il miglioramento delle condizioni relative alla condivisione dei dati nel mercato interno tramite la creazione di un quadro armonizzato per gli scambi di dati, l'individuazione dei requisiti di base per la *governance* degli stessi e la facilitazione della cooperazione tra gli Stati membri (*considerando 3*). Le tre aree di regolamentazione oggetto del DGA sono il riutilizzo di determinate categorie di dati detenuti da enti pubblici, i servizi di intermediazione dei dati e l'altruismo dei dati.

Quale premessa generale, i principali responsabili dell'attuazione del DGA sono gli Stati membri, che si impegnano a designare una o più autorità competenti a svolgere i compiti di seguito meglio delineati[3].

2. Riutilizzo di determinate categorie di dati detenuti da enti pubblici

Il DGA stabilisce le condizioni per il riutilizzo, all'interno dell'UE, di determinate categorie di dati detenuti da enti pubblici[4] (art. 1, comma 1, lett. a).
Con il termine "riutilizzo", il DGA intende l'utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti (art. 2(2)). La messa a disposizione di terzi dei dati raccolti dagli enti pubblici non può avvenire sulla base di accordi di esclusiva, se non in casi eccezionali[5], affinché sia rispettato il diritto della concorrenza.

Si evidenzia che il DGA non impone di consentirne il riutilizzo da parte di terzi: tale decisione spetta a ciascuno Stato membro, il quale può scegliere se agevolare l'utilizzo dei dati detenuti dagli enti pubblici per

[3] Si prega di notare che gli Stati membri, ai sensi dell'articolo 26, hanno la facoltà di istituire una o più autorità nuove per tali finalità o avvalersi di autorità esistenti. Tuttavia, sebbene non espressamente stabilito dal DGA, l'articolo 13, comma 3, presuppone che tale compito non possa essere svolto dalle autorità per la protezione dei dati, dalle autorità nazionali garanti della concorrenza, dalle autorità responsabili della *cyber* sicurezza e da altre autorità settoriali pertinenti, con le quali, invero, le autorità competenti ai sensi del DGA si impegnano ad instaurare una forte cooperazione.

[4] La definizione di ente pubblico viene data dall'articolo 2(17), che identifica gli enti pubblici nelle autorità statali, regionali o locali, negli organismi di diritto pubblico - come definiti dal successivo articolo 2(18) - o nelle associazioni formate da una o più di tali autorità oppure da uno o più di tali organismi. Il DGA prosegue, all'articolo 3, comma 2, elencando categorie di dati rispetto ai quali il Capo II non trova applicazione (*i.e.: (i)* i dati detenuti da imprese pubbliche, definite ai sensi dell'articolo 2(19), in quanto utilizzano sempre più spesso modelli imprenditoriali e di mercato; *(ii)* i dati detenuti da emittenti di servizio pubblico e istituti culturali e di istruzione, in quanto le opere e gli altri documenti in loro possesso sono prevalentemente coperti da diritti di proprietà intellettuale di terzi; *(iii)* i dati protetti per motivi di sicurezza pubblica, difesa o sicurezza nazionale, a prescindere dall'ente pubblico che li detiene; e *(iv)* i dati la cui fornitura è un'attività che esula dall'ambito dei compiti di servizio pubblico dall'ente pubblico che li detiene). Essendo i dati un *asset* intangibile, sebbene non si possa parlare propriamente di possesso, significa che l'ente pubblico ha la facoltà effettiva e tecnica di accedere ai dati e al loro contenuto.

[5] Accordi di tale tenore sono possibili solo se giustificati e necessari per la fornitura di un servizio o di un prodotto di interesse generale, ad esempio, nel caso in cui l'utilizzo esclusivo dei dati rappresenti l'unico modo per massimizzare i benefici sociali dei dati in questione (*considerando* 13). Le condizioni

scopi non governativi. In tal caso, si applica il quadro normativo previsto dal Capo II, che mira alla creazione di una cultura *open data* in cui non sussistano accordi di esclusiva e in cui sia facilitato il riutilizzo dei dati.

In particolare, i dati detenuti da enti pubblici disciplinati dal Capo II sono quelli particolarmente "*sensibili*" (*e.g.,* dati commerciali riservati, dati soggetti a segreto statistico, dati protetti da diritti di proprietà intellettuale di terzi - compresi segreti commerciali e dati personali) e, per questo motivo, spesso non a disposizione del pubblico, nemmeno per attività di ricerca o di innovazione nel pubblico interesse (*considerando 6*). Per tali categorie di dati, il legislatore europeo ha individuato l'esigenza di una specifica disciplina relativa al loro riutilizzo, in virtù del fatto che gli stessi, prima di essere messi a disposizione, esigono il soddisfacimento di alcuni requisiti tecnici e giuridici al fine di garantire il rispetto dei diritti di terzi.
L'ente pubblico CHE consente il riutilizzo dei dati, a titolo gratuito o a fronte del pagamento di una tariffa, deve farlo alle condizioni stabilite dall'articolo 5, affinché il riutilizzo sia non discriminatorio, trasparente, proporzionale e oggettivamente giustificato in relazione alla natura, alle categorie di dati e alle finalità del riutilizzo.

L'ente pubblico deve rendere pubbliche le condizioni per consentire il riutilizzo e la procedura di richiesta dello stesso attraverso un c.d. sportello unico, come disciplinato ai sensi dell'articolo 8. Inoltre, l'ente pubblico è soggetto a specifici obblighi relativi alla protezione degli interessati e dei titolari dei dati. Infine, gli artt. 7-9 disciplinano la creazione di un'infrastruttura amministrativa ai fini di facilitare l'effettivo riutilizzo dei dati[6].

3. Servizi di intermediazione dei dati

Il secondo obiettivo del DGA consiste nella facilitazione dello scambio di grandi quantità di dati tra soggetti privati e pubblici, per rendere pienamente utilizzabili le basi di dati già esistenti e contribuire al buon funzionamento di un'economia basata sui dati (*considerando 5*).

Per raggiungere tale scopo, il Capo III introduce i servizi di intermediazione di dati[7], che consentono agli interessati e ai titolari dei dati di condividere i rispettivi dati con potenziali utilizzatori e a quest'ultimi di accedere più facilmente ai dati pertinenti. Il fornitore di servizi di intermediazione dei dati si colloca, dunque, in una posizione tra interessati e titolari, da un lato, e utilizzatori, dall'altro, fungendo da intermediario nelle relazioni commerciali instaurate tra le parti coinvolte e volte alla condivisione di dati. I servizi di intermediazione dei dati includono la condivisione bilaterale o multilaterale, la creazione di piattaforme e banche dati che ne consentano la condivisione o l'utilizzo congiunto, nonché la creazione di un'infrastruttura specifica per l'interconnessione di interessati e titolari dei dati con gli utenti (*considerando 27*).

di tali eccezioni sono previste all'articolo 4 (2-5).

[6] In particolare, l'articolo 7 prevede che gli Stati membri designino uno o più organismi competenti per assistere gli enti pubblici che concedono l'accesso al riutilizzo dei dati, mentre l'articolo 8 disciplina i c.d. sportelli unici, presso i quali siano disponibili e accessibili per i riutilizzatori tutte le informazioni relative al riutilizzo dei dati. Infine, l'articolo 9 dettaglia la procedura per le richieste di riutilizzo.

[7] Ai sensi dell'articolo 2(11), un "servizio di intermediazione di dati" è: "*un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali*".

La fornitura di servizi di intermediazione dei dati è soggetta a una procedura di notifica all'autorità competente in ciascuno Stato membro per i servizi di intermediazione dei dati, al fine di monitorare i fornitori di tali servizi e sanzionare eventuali violazioni. Tale procedura di notifica, il cui contenuto è dettato dall'articolo 11, comma 6, ha lo scopo di garantire una *governance* dei dati basata su uno scambio affidabile. A seguito della ricezione di tale notifica, l'autorità competente informa la Commissione, che pubblica i dettagli rilevanti sul nuovo fornitore di servizi di intermediazione dei dati in un registro pubblico aggiornato ai sensi dell'articolo 11, comma 13.
L'articolo 12 individua taluni requisiti ai quali ogni fornitore di servizi di intermediazione dei dati deve adeguarsi affinché sia assicurata la propria neutralità. In particolare, il fornitore è tenuto a:

- utilizzare i dati per i quali fornisce servizi di intermediazione al solo scopo di metterli a disposizione degli utenti dei dati[8], in modo da garantire una separazione, nell'economia dei dati, tra fornitura, intermediazione e utilizzazione degli stessi;

- fornire servizi di intermediazione attraverso una persona giuridica distinta;

- non subordinare le condizioni commerciali (compreso il prezzo) per la fornitura di servizi al fatto che il titolare dei dati o l'utente dei dati utilizzi altri servizi forniti dallo stesso fornitore o da un'entità collegata;

- non utilizzare i metadati raccolti dalla persona fisica o giuridica che utilizza i servizi di intermediazione dei dati (*e.g.*, data, ora, geolocalizzazione) per scopi diversi dallo sviluppo di tali servizi;

- agevolare lo scambio di dati nel formato in cui li riceve, convertendoli al solo scopo di migliorarne l'interoperabilità, previa richiesta dell'utente dei dati o se prescritto dal diritto comunitario;

- provvedere affinché la procedura di accesso al servizio sia equa, trasparente e non discriminatoria, compresi i prezzi e le condizioni di servizio, così da evitare alterazioni della concorrenza;

- disporre di procedure per prevenire pratiche fraudolente o abusive da parte dei soggetti che utilizzano i suoi servizi;

- adottare misure adeguate per garantire l'interoperabilità con altri servizi di intermediazione dei dati, anche attraverso il rispetto delle vigenti norme di uso comune nel settore in cui opera;

- mettere in atto adeguate misure tecniche, giuridiche e organizzative al fine di impedire l'illecito trasferimento o accesso a dati non personali.

Per i dati personali, un'analoga obbligazione è prescritta dall'articolo 32 GDPR;

- notificare ai titolari dei dati eventuali trasferimenti, accessi o utilizzi

[8] Ciò significa che i fornitori di servizi di intermediazione di dati non possono offrire ulteriori servizi, fatta eccezione per i servizi che servono meramente a facilitare lo scambio di dati (*e.g.*, conservazione temporanea, anonimizzazione e pseudoanonimizzazione).

non autorizzati dei dati non personali che ha condiviso. Per i dati personali, un'analoga obbligazione è prescritta dall'articolo 34 GDPR;

→ adottare le misure necessarie per garantire un adeguato livello di sicurezza in merito alla conservazione, trattamento e trasmissione di dati non personali. Nel caso di informazioni sensibili sotto il profilo della concorrenza, invece, il fornitore si impegna ad assicurare il massimo livello di sicurezza[9];

→ nel caso di servizi offerti agli interessati, agire nell'interesse superiore di questi ultimi, facilitando l'esercizio dei loro diritti;

→ qualora fornisca strumenti per ottenere il consenso degli interessati o le autorizzazioni dei titolari dei dati, specificare la giurisdizione del Paese terzo in cui si intende utilizzare i dati e fornire gli strumenti per dare e revocare il consenso o le autorizzazioni;

→ tenere un registro dell'attività di intermediazione dei dati.

[9] Ai fini di completezza, si evidenzia che i fornitori di servizi di intermediazione di dati non sono sempre in grado di determinare se i dati conservati, trattati o trasmessi attraverso i propri servizi contengano sensibili sotto il profilo della concorrenza e, pertanto, si potrebbe sostenere che tali soggetti siano sempre tenuti ad assicurare il massimo livello di sicurezza.

[10] Di conseguenza, gli interessati ricevono un compenso esclusivamente in relazione ai costi da loro sostenuti nel mettere a disposizione i propri dati per obiettivi di interesse generale.

4. Altruismo dei dati

Il terzo pilastro introdotto dal DGA è l'altruismo dei dati, definito come "*la condivisione volontaria di dati (…) per obiettivi di interesse generale (…) quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale*". Il fine dell'altruismo dei dati si individua, dunque, nella valorizzazione di un'ampia varietà di informazioni condivise e utilizzate volontariamente per ottenere benefici per la società[10].

In particolare, il Capo IV prescrive un quadro per la registrazione volontaria delle entità che raccolgono e trattano i dati messi a disposizione per fini altruistici, nonché per l'agevolazione della messa a disposizione, su base volontaria, di dati personali da parte degli interessati e di dati non personali da parte dei titolari. Per conseguire tale obiettivo, il DGA prevede che gli Stati membri si dotino di disposizioni organizzative e/o tecniche quali, a titolo esemplificativo, la messa a disposizione degli interessati o dei titolari dei dati di strumenti di facile utilizzo per concedere il consenso o l'autorizzazione all'uso altruistico dei loro dati, l'organizzazione di campagne di sensibilizzazione, lo scambio strutturato tra le autorità competenti sui benefici dell'altruismo dei dati per le politiche pubbliche.

Il Capo IV non impone agli Stati membri la creazione di organizzazioni per l'altruismo dei dati, ma si limita a dettare i requisiti che le persone giuridiche che intendono sostenere obiettivi di interesse generale mettendo a disposizione quantità considerevoli di dati sulla base

dell'altruismo dei dati devono soddisfare per potersi registrare in qualità di "organizzazione per l'altruismo dei dati riconosciuta nell'Unione" ed essere riconosciute a livello comunitario con tale titolo, al fine di infondere fiducia circa il fatto che i dati messi a disposizione a fini altruistici servano un obiettivo di interesse generale (*considerando* 46). Al fine di aiutare gli interessati e i titolari ad identificare le organizzazioni riconosciute, l'articolo 17 impone agli Stati membri di tenere e aggiornare un registro pubblico nazionale delle organizzazioni per l'altruismo dei dati riconosciute[11] e alla Commissione di tenere un registro comunitario.

Inoltre, al fine di essere ammessa alla registrazione[12], un'entità deve rispettare e mantenere i requisiti previsti: *(i)* dall'articolo 18 e, tra gli altri, svolgere attività di altruismo dei dati, essere una persona giuridica costituita a norma del diritto nazionale per conseguire obiettivi di interesse generale e operare senza scopo di lucro; *(ii)* dall'articolo 20 in materia di obblighi di trasparenza[13]; e *(iii)* dall'articolo 21 in materia di obblighi specifici di tutela dei diritti degli interessati e dei titolari dei dati[14].

Il DGA non intende creare una nuova base giuridica per il trattamento dei dati personali a fini altruistici, ma rimanda alle basi giuridiche per il trattamento degli stessi previste agli articoli 6 e 9 GDPR, tra le quali il consenso dell'interessato. Ai sensi dell'articolo 4 GDPR, il consenso consiste in "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*". Alla luce di ciò, per ogni nuova operazione di trattamento, l'interessato è tenuto a rilasciare un consenso specifico.

Al fine di facilitare l'ottenimento dei consensi e, di conseguenza, la raccolta dei dati basata sull'altruismo, l'articolo 25 prevede che la Commissione istituisca un modulo europeo di consenso all'altruismo dei dati che permetta di raccogliere e revocare il consenso o l'autorizzazione in un formato uniforme in tutti gli Stati membri.

5. Accesso internazionale e trasferimento

Il Capo VII prevede tutele e condizioni per impedire l'illecito trasferimento o accesso internazionale a dati non personali, imponendo a enti pubblici, riutilizzatori dei dati, fornitori di servizi di intermediazione dei dati o organizzazioni per l'altruismo riconosciute, di adottare tutte le ragionevoli misure tecniche, giuridiche e organizzative per impedire il trasferimento internazionale di dati non personali detenuti nell'Unione o l'accesso a questi ultimi da parte delle autorità pubbliche, qualora tale trasferimento o accesso confliggesse con il diritto dell'Unione o il diritto nazionale dello Stato membro pertinente. Per i dati personali si applica, invece, l'articolo 44 GDPR.

[11] Tale compito è svolto da una (o più) autorità competente per la registrazione delle organizzazioni per l'altruismo dei dati, che ciascuno Stato membro si impegna a designare ai sensi dell'articolo 23 e che rispetta i requisiti di cui all'articolo 26. Le autorità competenti per la registrazione delle organizzazioni per l'altruismo dei dati hanno il compito di monitorare e controllare la conformità alle prescrizioni stabilite nel DGA da parte delle organizzazioni per l'altruismo dei dati.

[12] Ai sensi della procedura stabilita dall'articolo 19.

[13] Ad esempio: *(i)* tenere registri accurati concernenti le persone fisiche o giuridiche a cui è data la possibilità di trattare i dati detenuti da tale organizzazione e la data e/o durata e le finalità del trattamento o dell'utilizzo dei dati personali e non personali; *(ii)* elaborare e trasmettere relazioni di attività annuali alle autorità competenti concernenti le attività svolte, le modalità con cui sono stati promossi gli obiettivi di interesse generale, e le fonti di entrate e costi.

[14] Tra questi, l'obbligo di:
- informare in maniera chiara e comprensibile gli interessati o i titolari prima di qualsiasi trattamento dei loro dati in merito agli obiettivi di interesse generale per cui i dati devono essere trattati;
- non utilizzare dati per fini diversi dagli interessi generali dichiarati;
- fornire strumenti per ottenere il consenso degli interessati o le autorizzazioni dei titolari dei dati e gli strumenti per dare e revocare tali consensi o autorizzazioni;
- garantire un livello adeguato di sicurezza per la conservazione e il trattamento dei dati che ha raccolto; e
- specificare, qualora agevoli il trattamento dei dati da parte di terzi, se del caso, la giurisdizione del paese terzo in cui si intende utilizzare i dati.

6. Diritto a un ricorso giurisdizionale effettivo e sanzioni

Il DGA sancisce il diritto ad un ricorso giurisdizionale effettivo in relazione alle decisioni giuridicamente vincolanti adottate dagli organismi competenti in materia di riutilizzo, intermediazione e altruismo dei dati, pur lasciando che le leggi nazionali di ciascuno Stato membro disciplinino la tutela e le sanzioni da applicare in caso di violazione degli obblighi in materia di: *(i)* trasferimento di dati non personali a Paesi terzi, *(ii)* notifica per i fornitori di servizi di intermediazione dei dati, *(iii)* condizioni per la fornitura di servizi di intermediazione dei dati, e *(iv)* condizioni per la registrazione come organizzazione per l'altruismo dei dati riconosciuta. Il DGA non specifica se la colpa debba essere provata ai fini dell'imposizione delle sanzioni e, pertanto, tale circostanza dipende dall'applicazione delle sanzioni a livello nazionale.

7. Comitato europeo per l'innovazione in materia di dati

Il Capo VI stabilisce un quadro per l'istituzione di un Comitato europeo per l'innovazione in materia di dati ad opera della Commissione, che si impegna a designare un gruppo di esperti costituito da rappresentanti *(i)* delle autorità competenti per i servizi di intermediazione dei dati e per la registrazione delle organizzazioni per l'altruismo dei dati di tutti gli Stati membri, *(ii)* del Comitato europeo per la protezione dei dati, *(iii)* del Garante europeo della protezione dei dati, *(iv)* dell'ENISA, *(v)* della Commissione, e *(vi)* di organi pertinenti di settori specifici e dal rappresentante dell'Unione europea per le PMI. Il comitato europeo per l'innovazione in materia di dati svolge, *inter alia*, compiti di consulenza e assistenza alla Commissione[15] e facilitazione della cooperazione tra gli Stati membri e tra le autorità competenti per il riutilizzo, i servizi di intermediazione e l'altruismo dei dati.

[15] In particolare, con riferimento a:
- lo sviluppo di una prassi coerente degli enti pubblici e degli organismi competenti in materia di trattamento delle richieste di riutilizzo di dati, altruismo dei dati e servizi di intermediazione dei dati
- l'elaborazione di orientamenti coerenti sulle modalità per proteggere al meglio i dati commerciali sensibili non personali (e.g., i segreti commerciali) e i dati non personali protetti da diritti di proprietà intellettuale;
- l'elaborazione di orientamenti coerenti sulle prescrizioni in materia di cyber sicurezza per lo scambio e la conservazione dei dati;
- la strategia per far fronte alla frammentazione del mercato interno e dell'economia dei dati nel mercato interno mediante il rafforzamento dell'interoperabilità transfrontaliera e intersettoriale dei dati e dei servizi di condivisione dei dati tra diversi settori e ambiti, anche allo scopo di incoraggiare la creazione di spazi comuni europei di dati; e
- l'elaborazione del modulo europeo di consenso all'altruismo dei dati.

7.4 Regolamento (UE) 2023/2854 del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo

1. Introduzione

Il Regolamento 2023/2854 in materia di accesso equo e uso dei dati ("**Data Act**"), **entrato in vigore** a gennaio 2024, costituisce l'ultimo tassello della strategia attuata dall'Unione Europea in materia di dati.

La sempre maggiore proliferazione di prodotti connessi e dell'*Internet of Things* (IoT) ha aumentato il volume (e, conseguentemente, il valore) dei dati per i consumatori e le imprese: poter disporre di dati interoperabili e di elevata qualità provenienti da diversi settori è divenuto un fattore determinante per innalzare il tasso di competitività e di innovazione dell'intero blocco.

I dati generati dai prodotti connessi e dai servizi correlati possono, infatti, essere utilizzati per potenziare i servizi post-vendita e ausiliari, nonché per creare servizi completamente nuovi, a vantaggio sia dei consumatori (che potrebbero, ad esempio, beneficiare di prezzi più bassi per i servizi di riparazione dei loro oggetti connessi) che delle imprese (ad esempio, dei fornitori dei servizi post-vendita che potrebbero offrire prestazioni maggiormente personalizzate, risultando così in grado di competere con servizi analoghi offerti dai produttori).

L'intento del Data Act è così proprio quello di dare impulso alla *data economy* dell'UE, mediante la definizione di regole armonizzate sull'accesso e l'utilizzo dei dati, e l'eliminazione degli ostacoli alla condivisione in tutti i settori economici dell'Unione.

Affiancato dal *Data Governance Act* (Regolamento (UE) 2022/868[16]), si stima che il Data Act, intervenendo sulle problematiche giuridiche, economiche e tecniche che causano un sottoutilizzo dei dati[17], dovrebbe garantire un aumento del PIL di 270 miliardi di euro per gli Stati membri dell'UE entro il 2028.

2. Ambito di applicazione

Il Data Act ha ad oggetto i dati personali e non personali trattati in tutti i settori economici, derivanti dall'utilizzo di qualsiasi prodotto connesso e servizio correlato immesso sul mercato europeo.

La normativa si rivolge dunque a una vasta platea di soggetti e, nello specifico:

- ai **fabbricanti** di prodotti connessi immessi sul mercato dell'UE e ai fornitori di servizi correlati, indipendentemente dal loro luogo di stabilimento;

- agli **utenti** nell'UE di tali prodotti connessi o servizi;

- ai **titolari dei dati**[18], indipendentemente dal loro luogo di stabilimento, che li mettono a disposizione dei destinatari nell'Unione e, naturalmente, a questi ultimi;

- ai **fornitori di servizi**[19] di trattamento dei dati, indipendentemente dal loro luogo di stabilimento, che forniscono tali servizi a clienti nell'Unione;

- ai **partecipanti agli spazi di dati** e ai **venditori di applicazioni** che utilizzano contratti intelligenti.

Sono, infine, incluse specifiche previsioni indirizzate agli enti pubblici, alla Commissione, alla Banca centrale europea e agli organismi dell'Unione.

3. Le principali novità del Data Act

Con il Data Act, la Commissione persegue l'obiettivo di massimizzare il valore dei dati nell'economia europea, mediante l'introduzione di alcune interessanti novità sul piano normativo.

(A) Diritto di accesso e utilizzo dei dati

Il principale obiettivo del Data Act è quello di creare equità nell'economia dei dati e di consentire agli utenti[20] di un **prodotto connesso** (ad esempio, veicoli connessi, dispositivi medici e sanitari, macchinari industriali o agricoli) o di un **servizio correlato** (ossia tutto ciò che fa sì che un prodotto connesso si comporti in uno specifico modo, come ad esempio un'applicazione che consente di misurare l'impatto ambientale del ciclo di lavaggio di una lavatrice e di regolare il ciclo di conseguenza) di trarre valore dai dati che i medesimi generano utilizzando detti prodotti o i servizi.

Il Regolamento introduce, pertanto, da un lato il **diritto** degli utenti di **accedere** tempestivamente e gratuitamente ai dati (personali e non personali) generati dall'uso del prodotto connesso o del servizio correlato e di **utilizzare** tali dati, anche condividendoli con soggetti terzi di sua scelta.

Per rendere effettivi tali diritti, il Capo II del Data Act prevede una serie di **obblighi** per i **produttori** di beni connessi immessi sul mercato nell'Unione europea e per i fornitori di servizi correlati.

In particolare:

→ *Accesso ai dati by design e by default*
I prodotti connessi e i servizi correlati che raccolgono o generano dati dovranno essere progettati, fabbricati e forniti in modo tale da garantire all'utente l'accesso e la portabilità dei dati, inclusi i metadati necessari ad interpretarli e utilizzarli.
Tali dati dovranno essere, per impostazione predefinita, accessibili all'utente in un formato completo, strutturato, di uso comune e leggibile da un dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo diretto.

→ *Obblighi informativi*
Prima della conclusione dei contratti relativi a prodotti e servizi, l'utilizzatore dovrà essere preventivamente informato, in maniera chiara e comprensibile, di specifici profili attinenti ai dati che potranno essere generati – compresi il tipo, il formato e il volume stimato di tali dati, con quale frequenza, le modalità per accedervi, se il fornitore intende utilizzarli o consentire a terzi l'utilizzo e per quali scopi, l'identità del titolare dei dati, a chi rivolgersi per richieste o reclami.

Condivisione dei dati con soggetti terzi
Il titolare dei dati dovrà inoltre, dietro richiesta dell'utente o di un soggetto che agisce per suo conto, mettere i dati a disposizione di terze parti, a condizioni eque, ragionevoli, non discriminatorie e trasparenti (*fair, reasonable and non discriminatory* - FRAND).

La disciplina generale è accompagnata da una serie di **correttivi** e **limitazioni** volti a riequilibrare il funzionamento del mercato ed evitare che le imprese siano disincentivate dall'investire in prodotti IoT e, tra i più rilevanti:

→ l'applicazione limitata ai soli dati (personali e non personali, inclusi i metadati) grezzi e pre-elaborati generati dall'uso di un prodotto connesso o di un servizio correlato, ossia a dati che sono prontamente disponibili per il titolare dei dati. Sono, pertanto, escluse le informazioni dedotte, inferite o ricavate;

→ l'esclusione dei dati generati dall'utilizzo di prodotti o di servizi connessi forniti da microimprese o piccole imprese;

→ il divieto per l'utente di utilizzare i dati, o di condividerli con un terzo, al fine di sviluppare prodotti connessi che sono in concorrenza con il prodotto da cui provengono i dati;

→ l'esclusione dal novero dei possibili beneficiari della condivisione dei dati delle piattaforme designate come *digital gatekeepers* ai sensi del Regolamento (UE) 2022/1925 (*Digital Market Act* [21]).

È opportuno, infine, evidenziare che il Data Act integra e lascia impregiudicato il GDPR: il considerando 7 ribadisce, infatti, che le previsioni ivi contenute non costituiscono una base giuridica per la raccolta o la generazione di dati personali da parte del titolare dei dati e che se l'utente non è l'interessato, detto Regolamento non costituisce neppure una base giuridica per consentire l'accesso ai dati personali o per metterli a disposizione di terzi.

(B) Maggiore equilibrio nei rapporti tra imprese

Il Data Act introduce altresì una disciplina specifica volta a riequilibrare il potere contrattuale fra le imprese di grandi dimensioni e quelle di piccole dimensioni, al fine di garantire condizioni eque, ragionevoli e non discriminatorie nella condivisione dei dati generati da un prodotto connesso o un servizio correlato.

→ *Clausole contrattuali abusive*
In particolare, viene prevista l'**inefficacia** di un elenco di clausole contrattuali imposte unilateralmente, con una distinzione tra:

- clausole **considerate abusive** – ad esempio, esclusioni o limitazioni della responsabilità della parte che ha imposto unilateralmente la clausola in caso di atti intenzionali o colpa grave, esclusione di rimedi in caso di inadempimento o responsabilità di tale parte, e

- clausole che si **presumono abusive** – ad esempio, clausole che impediscano al contraente cui tali clausole sono state imposte di utilizzare i dati dell'altro contraente o la facoltà di risolvere unilateralmente il contratto entro un periodo ragionevole.

Con analoghi obiettivi di tutela, è previsto che la Commissione elabori e raccomandi **clausole contrattuali tipo** non vincolanti relative all'accesso ai dati e al relativo utilizzo per assistere le parti nella stesura e nella negoziazione di contratti equilibrati dal punto di vista dei diritti e degli obblighi.

→ *Compenso per la condivisione dei dati*
A differenza dell'ipotesi di messa a disposizione dei dati a favore dell'utente/utilizzatore, che deve avvenire a titolo gratuito, il Regolamento prevede che il titolare dei dati possa concordare un compenso con l'impresa terza destinataria dei dati.

Tuttavia, al fine di evitare oneri eccessivi tali da rendere tale condivisione non più commercialmente sostenibile, il compenso dovrà essere ragionevole e non discriminatorio, nonché tenere conto dei costi sostenuti per la messa a disposizione e degli investimenti compiuti per la raccolta e la produzione dei dati[22].

Vincoli più stringenti sono, invece, previsti quando il beneficiario è una micro, piccola o media impresa: in questo caso potrà essere richiesto

soltanto il rimborso dei costi sostenuti per la loro messa a disposizione.

(C) Portabilità dei dati e interoperabilità nei servizi cloud

Per garantire un mercato competitivo nell'Unione, è necessario che i clienti dei servizi di trattamento dei dati - quali i servizi di *cloud* o *edge computing* - possano passare da un fornitore all'altro, mantenendo una funzionalità minima del servizio e senza tempi di inattività. Attualmente, infatti, i clienti si trovano di fronte a una serie di ostacoli, tra cui procedure lunghe e costi elevati associati all'uscita dei dati, nonché mancanza di interoperabilità tra i fornitori che può comportare la perdita di dati.

→ *Passaggio tra fornitori di servizi di trattamento dei dati*
Al fine prevenire fenomeni di *vendor lock-in* e agevolare agli utenti il passaggio a un nuovo fornitore, il Data Act introduce una serie di misure che il fornitore di servizi di trattamento dati è tenuto ad adottare, tra cui l'obbligo di:

- eliminare gli ostacoli (pre-commerciali, commerciali, tecnici, contrattuali e organizzativi) che i clienti possono incontrare quando vogliono passare a un altro fornitore o a un sistema *on-premise*, ovvero utilizzare più servizi contemporaneamente;

- includere, nei relativi contratti con i clienti, determinate condizioni contrattuali (individuate all'articolo 25) volte a disciplinare il passaggio da un fornitore all'altro (o a un sistema *on-premise*);

- informare i clienti sulle procedure disponibili per il passaggio e la portabilità al loro servizio e fornire loro il riferimento al registro online aggiornato del fornitore di servizi, contenente dettagli sulle strutture e sui formati dei dati, nonché sugli standard pertinenti e sulle specifiche di interoperabilità aperta;

- rendere disponibili e mantenere aggiornate sui propri siti *web* le informazioni sulla giurisdizione cui è soggetta l'infrastruttura utilizzata per il trattamento dei dati, nonché una descrizione delle misure adottate per impedire l'accesso o il trasferimento a governi esteri dei dati non personali;

- a seconda della tipologia di servizi erogati, adottare misure tecniche per garantire l'equivalenza funzionale del servizio di destinazione, nonché la compatibilità con le specifiche comuni di interoperabilità che saranno pubblicate ai sensi del Data Act.

Si segnala, inoltre, l'obbligo di eliminare le tariffe di passaggio a partire dal 12 gennaio 2027. I *provider* non potranno quindi più addebitare ai propri clienti i costi delle operazioni necessarie per facilitare il passaggio da un fornitore all'altro o l'accesso ai dati.

Come misura transitoria durante i primi 3 anni dall'entrata in vigore del Data Act – dall'11 gennaio 2024 al 12 gennaio 2027 – i fornitori conserveranno tuttavia la facoltà di imporre ai loro clienti tariffe di passaggio ridotte, in ogni caso non superiori ai costi direttamente connessi al pertinente processo di passaggio[23].

→ *Interoperabilità e smart contract*
Il Data Act mira altresì ad aumentare concretamente l'**interoperabilità** dei servizi di trattamento dei dati attraverso misure che mirano alla standardizzazione. In particolare, il Regolamento identifica, a un livello alto, i requisiti essenziali di interoperabilità per gli spazi dei dati e i servizi di trattamento dei dati, demandando alla Commissione il compito di fornire ulteriori prescrizioni di dettaglio. In tale quadro generale, gli organismi di standardizzazione dell'UE saranno altresì tenuti, su richiesta della Commissione, a individuare standard armonizzati e specifiche tecniche di interoperabilità.

Vengono, infine, stabiliti alcuni requisiti rivolti ai venditori e agli sviluppatori di applicazioni che utilizzano ***smart contract*** nel contesto dell'esecuzione di un accordo per la messa a disposizione dei dati. Questi includono obblighi relativi alla robustezza e al controllo degli accessi, alla sicurezza della cessazione o dell'interruzione del funzionamento dello *smart contract* e alla archiviazione e continuità dei dati.

(D) La Commissione Obbligo di condivisione dei dati con le autorità pubbliche

evidenza come i dati in possesso di soggetti privati possano essere essenziali per un **ente pubblico** per svolgere un compito di interesse pubblico.

Il Data Act introduce, pertanto, specifici meccanismi per consentire agli enti pubblici di accedere, a determinate condizioni, a tali dati in caso di necessità eccezionali, ossia circostanze imprevedibili e limitate nel tempo. Le situazioni di eccezionale necessità possono comprendere sia le emergenze pubbliche (*e.g.*, grandi catastrofi naturali o indotte dall'uomo, pandemie e incidenti di sicurezza informatica), sia le situazioni di non emergenza (*e.g*, la redazione di statistiche ufficiali o la mitigazione o la ripresa dopo un'emergenza pubblica).

Il Capo V prevede, in particolare, che un ente pubblico, la Commissione, la Banca centrale europea o un organismo dell'Unione possa richiedere al titolare dei dati di mettere a disposizione, senza ritardi ingiustificati:

→ dati personali (i quali, ove possibile, devono essere resi anonimi dal titolare) e non personali per rispondere a un'**emergenza pubblica**. Tale condivisione deve avvenire a titolo gratuito, salvo nel caso in cui i titolari dei dati siano microimprese o piccole imprese, ferma in ogni caso la possibilità per il titolare dei dati di richiedere un riconoscimento pubblico;

→ dati non personali per adempiere a un **compito** specifico di **interesse pubblico** e previsto dalla legge, se l'ente pubblico è in grado di dimostrare di non essere riuscito ad accedere ai dati con altri mezzi. In tale caso il titolare dei dati ha diritto a un compenso equo, in ogni caso non superiore ai costi tecnici e organizzativi sostenuti per soddisfare la richiesta e a un margine ragionevole.

(E) Tutele contro il trasferimento illegale di dati in Stati Terzi

Il Data Act introduce regole volte a garantire maggiore **trasparenza** e **certezza** per quanto riguarda il processo e le condizioni in cui i dati non personali detenuti nell'Unione possono essere lecitamente consultati o trasferiti a enti governativi non appartenenti all'UE.

In particolare, il Capo VII prevede che in assenza di accordi internazionali, il trasferimento o l'accesso a dati non personali detenuti nell'Unione possano essere consentiti solo in presenza delle specifiche condizioni[24] previste all'articolo 32 a tutela dei diritti europei (quali, i diritti fondamentali delle persone o gli interessi di sicurezza nazionale).

Al fine di prevenire l'accesso illecito a dati non personali da parte di autorità di paesi terzi, sarà infine opportuno che i fornitori di servizi di trattamento dei dati *(i)* adottino tutte le misure ragionevoli per impedire l'accesso ai sistemi in cui sono archiviati dati non personali (ad esempio, mediante la cifratura dei dati, la frequente sottoposizione ad *audit*, l'adesione ai pertinenti sistemi di certificazione della sicurezza e la modifica delle politiche aziendali), e *(ii)* informino i consumatori prima di consentire l'accesso ai loro dati.

(F) Tutela dei diritti di proprietà industriale e intellettuale

I dati oggetto del Data Act potrebbero contenere o costituire diritti di proprietà industriale e intellettuale, la cui circolazione potrebbe ledere gli interessi e i diritti dei relativi titolari.

A tale riguardo, il Regolamento non pregiudica le normative applicabili in materia di protezione dei diritti di proprietà industriale e intellettuale e introduce una serie di disposizioni a tutela di tali tipologie di dati, ivi inclusa l'adozione di misure di sicurezza a protezione dei segreti commerciali e la possibilità per il titolare dei dati di sospenderne la condivisione o impedirne l'accesso al ricorrere di talune circostanze.

Viene chiarito, inoltre, che il diritto *sui generis* di cui alla Direttiva 96/9/CE sulle banche dati[25] non trova applicazione con riferimento alle banche dati contenenti dati ottenuti o generati dall'utilizzo di un prodotto connesso o di un servizio correlato, rimuovendo così ogni incertezza che la condivisione di tale tipologia di dati possa costituire una violazione di diritti di proprietà intellettuale.

Si segnala, in ogni caso, che entro il 12 settembre 2028 la Commissione

dovrà effettuare una valutazione iniziale degli impatti del Data Act sui diritti di proprietà intellettuale e sui segreti commerciali.

4. Applicazione e Attuazione

Il Data Act è stato concepito come regolamento ad applicazione differita: la maggior parte delle sue disposizioni, infatti, si applicherà a partire dal **12 settembre 2025**, con eccezioni per:

- gli obblighi per la progettazione, la produzione e la fornitura di dispositivi connessi e servizi correlati, che si prevede si applicheranno a partire dal 12 settembre 2026;

- le disposizioni sulle clausole contrattuali abusive per l'accesso ai dati tra imprese, che si prevede si applicheranno a partire dal 12 settembre 2027 per i contratti di lunga durata o a tempo indeterminato che sono stati conclusi il, o anteriormente al, 12 settembre 2025.

Responsabili dell'applicazione e dell'esecuzione del Regolamento saranno, inoltre, le autorità nazionali appositamente designate dagli Stati membri, i quali dovranno altresì stabilire le norme relative alle sanzioni da applicare in caso di violazione e i meccanismi per la gestione dei reclami.

5. Conclusioni

Il Data Act appare aprire opportunità rilevanti nel contesto della *data economy*, mettendo a disposizione strumenti potenzialmente in grado di riequilibrare il funzionamento del mercato e di aumentare la concorrenza e l'innovazione.

Affinché gli strumenti messi a disposizione dalla Commissione siano effettivamente in grado di dare un impulso significativo all'economia europea dei dati nel suo complesso, sarà tuttavia necessario che le imprese mettano ancora una volta in conto importanti oneri di adeguamento, sia a livello tecnico (*e.g.*, implementando adeguati presidi di *cybersecurity* e infrastrutture per il *data sharing*) che organizzativo e contrattuale (*e.g.*, predisponendo nuove procedure e modelli contrattuali).

7.5 European Health Data Space

1. Introduzione

Nell'ambito della Strategia europea per i dati, un ruolo decisamente rilevante è ricoperto dal regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari (European Health Data Space o "**EHDS**" o "Regolamento") pubblicato sulla Gazzetta Ufficiale dell'Unione europea in data 5 marzo 2025. Il Regolamento, in vigore dal 25 marzo 2025, diventerà applicabile in diverse fasi in base ai tipi di dati e ai casi d'uso.

Il Regolamento è considerato un pilastro fondamentale nell'ambito della creazione di una forte "*Unione europea della salute*" da parte della Commissione europea e costituisce il primo testo di normativa relativa a un settore specifico, ovvero quello sanitario. Inoltre, può essere considerata *lex specialis* rispetto al *Data Governance Act* che fissa le regole sulla circolazione intersettoriale di dati nell'ambito della strategia europea dei dati.

A tal fine, occorre considerare il contesto in cui l'EHDS si colloca. La pandemia da Covid-19 ha, infatti, messo in luce l'importanza di avvalersi di un sistema condiviso, sicuro e affidabile per l'accesso e la condivisione, all'interno dell'Unione, di dati sanitari elettronici per lo sviluppo di una strategia in risposta alle emergenze sanitarie, garantendo, allo stesso tempo, il controllo delle persone fisiche sui propri dati sanitari. L'obiettivo perseguito tramite l'utilizzo e la regolamentazione di un sistema condiviso di dati è, quindi, quello di consentire agli operatori di sfruttare appieno il potenziale dei dati sanitari per orientare la ricerca scientifica nell'interesse pubblico, basandosi sullo sviluppo tecnologico e sull'interoperabilità dei sistemi di cartelle cliniche elettroniche.

Un esempio formulato proprio dai co-legislatori, nel comunicato stampa del 15 marzo 2024, delinea in maniera chiara l'obiettivo dell'EHDS: "*l'obiettivo delle nuove norme è consentire a un turista spagnolo di ritirare una ricetta in una farmacia tedesca, oppure permettere ai medici di accedere alle informazioni sanitarie di un paziente belga sottoposto a cure in Italia*".

2. Gli obiettivi perseguiti dall'EHDS

L'EHDS si prepone così di istituire lo spazio europeo dei dati sanitari prevedendo diposizioni, norme, prassi comuni, infrastrutture e un quadro di *governance* dell'ecosistema sanitario europeo con l'obiettivo di:

- disciplinare l'uso primario, sia a livello nazionale sia a livello europeo, dei dati sanitari elettronici delle persone fisiche, responsabilizzandole attraverso un maggiore accesso digitale all'interno dell'Unione e un controllo dei loro dati sanitari elettronici personali;

- promuovere un mercato unico per i sistemi di cartelle cliniche elettroniche, i dispositivi medici pertinenti e i sistemi di intelligenza artificiale ad alto rischio;

- fornire un sistema affidabile ed efficiente per l'uso secondario dei dati sanitari per finalità, quali, la ricerca, l'innovazione, la definizione delle politiche e le attività di regolamentazione.

Inoltre, le previsioni del Regolamento si basano, a livello europeo e nazionale, su specifiche normative settoriali, come il Regolamento 2017/745 sui dispositivi medici e il Regolamento 2014/910 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche; sulla normativa in materia di protezione dei dati personali, disciplinata dal Regolamento 2016/679 ("**GDPR**") nonché su normative recenti o in corso di approvazione, quali il Data Act, il Data Governance Act e l'AI Act.

Assume altresì particolare rilevanza l'interazione tra le disposizioni relative all'uso primario e secondario dei dati sanitari elettronici e le previsioni del GDPR (nonché della normativa nazionale in materia di protezione dei dati personali, quindi il Codice Privacy).

La disciplina relativa all'uso primario dei dati sanitari, infatti, rafforza e integra i diritti previsti dal GDPR e le relative norme riguardano tutte le categorie di dati sanitari, indipendentemente dal modo in cui sono stati raccolti o da chi li ha forniti, dal fondamento giuridico del trattamento o dallo status del titolare del trattamento come organizzazione pubblica o privata. Quanto, invece, all'uso secondario, il Regolamento si pone l'obiettivo di disciplinare nel dettaglio l'uso lecito di dati per finalità ulteriori (e secondarie) rispetto a quelle per i quali i dati sono stati raccolti. Tale aspetto costituisce un aspetto cruciale che oggi incontra spesso limiti all'interno della normativa, soprattutto nazionale, nonché un generale "timore" connesso all'utilizzo di dati personali in assenza di una lecita base giuridica del trattamento, determinando, così, una potenziale violazione della normativa in materia di protezione dei dati personali.

A Uso primario dei dati sanitari elettronici

Come sopra menzionato, il Capo II dell'EHDS introduce specifici diritti delle persone fisiche in relazione al trattamento dei loro dati sanitari elettronici.

In particolare, la normativa si basa sui diritti riconosciuti dal GDPR e integra ulteriormente alcuni di essi, previsti dall'articolo 3 del Regolamento, con l'obiettivo di sostenere l'attuazione coerente di tali

diritti applicati ai dati sanitari elettronici, indipendentemente dallo Stato membro in cui sono trattati tali dati, dal tipo di prestatore di assistenza sanitaria, dalle fonti dei dati o dallo Stato membro di affiliazione della persona interessata.

Assumono particolare rilievo le previsioni in merito al diritto di accesso ai dati sanitari elettronici e al diritto alla portabilità dei dati, finalizzati a garantire un maggior controllo delle persone fisiche sui loro dati.

Quanto al diritto di accesso, pur rimanendo fermo quanto previsto dall'articolo 15 del GDPR, l'EHDS prevede un meccanismo che consente alla persona fisica di accedere immediatamente, gratuitamente e in un formato facilmente leggibile, accessibile e di uso comune a una serie di dati sanitari elettronici (definite categorie prioritarie di dati sanitari elettronici, quali le prescrizioni elettroniche, i documenti relativi all'anamnesi dei pazienti, i risultati di laboratorio) superando soluzioni tutt'ora comunemente previste in alcuni Stati membri che prevedono, ad esempio la fornitura dei dati solamente in formato cartaceo o scannerizzati.

Il diritto alla portabilità è altresì previsto come elemento fondamentale per garantire la continuità dell'assistenza ed evitare duplicazioni ed errori. In ragione di ciò, i dati sanitari elettronici dovranno essere resi disponibili in un formato interoperabile, trasmissibili tra applicazioni, dispositivi e operatori sanitari. Inoltre, per supportare la condivisione dei dati tra operatori sanitari, l'EHDS introduce requisiti obbligatori di interoperabilità, sicurezza, protezione e privacy, nonché un'autocertificazione obbligatoria delle cartelle cliniche elettroniche che copra l'interoperabilità e la sicurezza. A tal fine, è stata istituita un'infrastruttura web comune denominata MyHealth@EU, dedicata proprio all'interscambio di dati tra i punti di contatto nazionali.

Fatta salva la precisazione contenuta Considerando 8 dell'EHDS che tali diritti "*non devono pregiudicare i diritti di accesso e portabilità stabiliti dal GDPR*", occorre, tuttavia, considerare che il rapporto tra il diritto alla portabilità del GDPR e quello dell'EHDS non sarà facile né, al momento, pare chiara la loro sovrapposizione e convivenza, risultando, in ogni caso, adempimenti previsti alle strutture sanitarie quali titolari del trattamento.

Inoltre, ai sensi del Regolamento, ai pazienti è riconosciuto il potere di controllare e condividere i propri dati sanitari elettronici con un operatore sanitario di loro scelta, nonché di aggiungere dati al proprio fascicolo sanitario elettronico per sé o per le persone di fiducia. In ogni caso, il Regolamento prevede che le scelte degli interessati siano reversibili e modificabili a loro discrezione.

Infine, tra le modifiche introdotte dall'accordo provvisorio raggiunto tra il Consiglio e il Parlamento di marzo 2024, è inclusa la possibilità, per gli Stati membri, di prevedere un diritto di *opt-out* sia all'uso primario dei loro dati da parte degli operatori sanitari sia, come meglio si dirà nel prosieguo, da parte degli altri soggetti legittimati ad accedere ai dati per l'uso secondario (sebbene, in questo caso, il diritto sia soggetto a una

serie di condizioni più rigorose).

Nell'ambito dell'attuazione di tali diritti, gli Stati membri saranno tenuti a designare le autorità sanitarie digitali che avranno un ruolo fondamentale nel far rispettare i diritti sopra menzionati.

B Sistemi di cartelle cliniche elettroniche e applicazioni per il benessere

Al fine di garantire il rispetto dei diritti delle persone fisiche e la libera e sicura circolazione dei dati sanitari elettronici, principio essenziale dello spazio europeo dei dati personali, è necessario prevedere un'accelerazione dal punto di vista puramente tecnico che consenta di creare un sistema condiviso e sicuro.

L'EHDS prevede, a tal fine, un schema di autocertificazione obbligatoria per i sistemi di cartelle cliniche (c.d. "*sistemi EHR*", "*Electronic Health Records*") utilizzate per il trattamento di una o più categorie specifiche di dati sanitari elettronici. Attraverso tale schema, è possibile dimostrare la conformità dei sistemi EHR ai requisiti di interoperabilità, sicurezza e registrazione per la comunicazione di dati sanitari elettronici personali stabiliti dalle due componenti EHR obbligatorie armonizzate dalla proposta di Regolamento, vale a dire la "*componente europea di interoperabilità per lo scambio di sistemi EHR*" e la "*componente europea di registrazione per i sistemi EHR*".

Ne derivano specifiche regole indirizzate a fabbricanti e i loro rappresentanti autorizzati, importatori, distributori finalizzate a garantire e dimostrare la conformità delle predette cartelle cliniche alle specifiche del formato europeo di interscambio delle cartelle cliniche elettroniche.

Assume particolare rilevanza, inoltre, l'articolo 14 dell'EHDS che disciplina altresì gli obblighi dei fornitori di sistemi di AI ad alto rischio, come definiti dall'articolo 6 dell'AI Act. Tali soggetti che dichiarano l'interoperabilità dei sistemi di IA con i componenti armonizzati dei sistemi EHR saranno tenuti a dimostrare la conformità ai requisiti essenziali relativi al componente europeo di interoperabilità per i sistemi EHR e al componente europeo di registrazione per i sistemi EHR.

Una delle novità rilevanti rispetto al testo della proposta della Commissione, previsto dall'articolo 40 dell'EHDS, attiene, inoltre, alla creazione di un ambiente digitale europeo di *testing* da sviluppare, sia da parte della Commissione, a livello europeo, sia da parte degli Stati membri, a livello nazionale, proprio al fine di valutare la conformità dei componenti dei sistemi EHR. I risultati della fase di *testing* dovranno essere inclusi dai produttori nella documentazione tecnica che gli stessi sono tenuti a produrre ai fini della dimostrazione della conformità dei sistemi.

Da ultimo, l'EHDS precisa che, mentre i sistemi EHR specificamente

destinati a essere utilizzati per il trattamento di una o più categorie specifiche di dati sanitari elettronici dovrebbero essere soggetti all'autocertificazione obbligatoria, i software di tipo generico non dovrebbero essere considerati sistemi EHR, anche se utilizzati in scenari di assistenza sanitaria, e non dovrebbero quindi essere tenuto a conformarsi alle disposizioni del Capitolo III del Regolamento. Ciò riguarda casi come il software di elaborazione del testo utilizzato per la stesura di rapporti che diventerebbero poi parte delle cartelle cliniche elettroniche narrative, il *middleware* per scopi generici o il software di gestione dei database utilizzato come parte di soluzioni di archiviazione dei dati.

Oltre agli obblighi che verranno introdotti dall'EHDS, occorre considerare che in merito alla sicurezza informatica e delle infrastrutture, rimane ferma l'applicazione della Direttiva NIS 2 (n. 2022/2555) sulle misure per un livello comune elevato di cybersicurezza in tutta l'Unione. Inoltre, a livello nazionale, occorrerà comprendere come armonizzare quanto previsto dall'EHDS in merito alle caratteristiche tecniche e di interoperabilità rispetto alla disciplina del Fascicolo Sanitario Elettronico 2.0 e dell'Ecosistema Dati Sanitari, ufficialmente introdotto con la pubblicazione nella Gazzetta Ufficiale del 5 marzo 2025 del Decreto 31 dicembre 2024 del Ministero della Salute.

C Uso secondario dei dati sanitari elettronici

Il terzo aspetto rilevante dell'EHDS consiste nella regolamentazione dell'uso secondario dei dati sanitari elettronici.

Lo Spazio europeo dei dati sanitari istituisce, infatti, un quadro comune dell'UE che consente l'utilizzo di una lista di categorie minime di dati sanitari (quali, elencati all'articolo 51, cartelle cliniche; dati genetici, genomici e proteomici umani; dati sanitari elettronici provenienti da studi clinici e da registri medici) per una serie di finalità individuate, tra cui la ricerca, l'innovazione, la sanità pubblica, l'elaborazione delle politiche, le attività di regolamentazione e la medicina personalizzata. Inoltre, è previsto che i dati sanitari elettronici possano essere utilizzati anche per attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, sistemi di IA e applicazioni di sanità digitale.

Non mancano specifiche previsioni volte a regolare i casi in cui è fatto divieto accedere e trattare dati per uso secondario: ad esempio quando l'accesso ai dati comporta l'adozione decisioni pregiudizievoli per una persona fisica anche al fine di escluderle dal beneficio di un contratto di assicurazione o di modificare i loro contributi e premi assicurativi; oppure per svolgere attività pubblicitarie o di marketing rivolte a professionisti sanitari, organizzazioni sanitarie o persone fisiche. Inoltre, in caso di uso secondario dei dati, resta ferma la necessità di tutelare i dati personali nonché i diritti di proprietà intellettuale e i segreti commerciali.

Quanto alle modalità di accesso per l'uso secondario dei dati sanitari, il Regolamento si basa sulla creazione di una nuova infrastruttura UE decentralizzata (*HealthData@EU*) che consentirà di collegare gli organismi di accesso ai dati sanitari che dovrebbero essere istituiti in tutti gli Stati membri. Sul punto, risulta chiara l'impostazione data dal legislatore europeo nell'ambito della strategia europea dei dati dove assumono rilevanza nel nuovo contesto gli organismi istituti per dare accesso ai dati, come i fornitori di servizi di condivisione dei dati nell'ambito del *Data Governance Act*.

L'EHDS istituisce, inoltre, regole in materia di *governance* e meccanismi per l'uso secondario. In particolare, coloro che desiderano riutilizzare i dati sanitari (c.d. "*health data users*" ovvero ricercatori, aziende o istituzioni pubbliche) dovranno, quindi, richiedere un permesso all'organismo di accesso ai dati sanitari competente, istituito a livello nazionale, ai sensi dell'articolo 55 dell'EHDS. Il permesso stabilisce modalità, finalità e tempistiche per l'utilizzo dei dati, fermo restando che sarà necessario trattare i dati solo in ambienti chiusi e sicuri in cui gli organismi di accesso ai dati sanitari devono fornire standard chiari per la sicurezza informatica. Inoltre, il permesso potrà essere richiesto solo per poter accedere e trattare dati in forma anonimizzata. Solo qualora l'utilizzatore dei dati abbia sufficientemente dimostrato che le finalità del trattamento non possono essere raggiunte con dati anonimizzati, l'organismo di accesso ai dati sanitari competente può fornire l'accesso a dati in forma pseudonimizzata, cioè dati che offrono informazioni sulla malattia, sui sintomi e sui farmaci, senza rivelare all'utente l'identità della persona.

La normativa prevede, quindi, che occorre dare prevalenza all'accesso a dati non personali (o anonimizzati) qualora ciò sia sufficiente per raggiungere le finalità perseguite. In alternativa, è necessario fornire dati solamente in forma pseudonimizzata, applicando nella catena di messa a disposizione dei dati per l'uso secondario sia da parte degli organismi di accesso dei dati sanitari sia da parte dei *data holders* tecniche di pseudonimizzazione il prima possibile.

La normativa, in ogni caso, pone un divieto a coloro che accedono ai dati di tentare di identificare nuovamente gli interessati.

Inoltre, una delle modifiche più rilevanti introdotte dall'accordo sul testo raggiunto tra il Consiglio e il Parlamento a marzo 2024 attiene proprio all'impostazione relativa all'uso secondario dei dati sanitari elettronici. Infatti, in linea con la posizione del Consiglio, in tutti gli Stati membri verrà introdotto il diritto di *opt-out*, ovvero il diritto, riconosciuto ai pazienti, di opporsi all'uso dei loro dati sanitari ai quali viene effettuato l'accesso, sia da parte dell'operatore sanitario curante sia per un uso secondario, in questo caso a condizioni rigorose, ovvero ad eccezione delle ipotesi in cui sia previsto un uso secondario per fini di interesse pubblico, elaborazione di politiche, statistiche e ricerca nell'interesse pubblico.

Non è, quindi, previsto quale requisito necessario un *opt-in*, ovvero un consenso, dell'interessato, con tutte le necessarie caratteristiche ad esso connesse, per consentire l'utilizzo secondario dei dati sanitari elettronici.

Tuttavia, è prevista la possibilità per gli Stati membri di prevedere meccanismi per l'attuazione di eccezioni giustificate per le finalità sopra menzionate e per la ricerca scientifica svolta per importanti motivi di interesse pubblico da enti del settore pubblico, compresi i terzi che agiscono per conto di tali enti o da essi incaricati.

La previsione di un diritto di *opt-out* e non di *opt-in* avrà particolare rilevanza nell'ambito dell'implementazione di tali modifiche a livello nazionale. La normativa nazionale italiana prevede, infatti, regole particolarmente più stringenti, previste dagli articolo 110 e 110-bis del Codice Privacy. Nel dettaglio, ad oggi, l'articolo 110 prevede che il consenso dell'interessato per il trattamento di dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico possa essere escluso solo qualora la ricerca sia effettuata sulla base di disposizioni di legge in conformità con l'articolo 9(2) lett. j) del GDPR, oppure, a determinate condizioni – ad esempio qualora la richiesta del consenso possa risultare impossibile o implicare uno sforzo sproporzionato – previa consultazione del Garante Privacy. Su quest'ultimo aspetto, occorre precisare che, a livello nazionale, proprio negli ultimi giorni, ci sono stati segnali di apertura rispetto al trattamento di dati sanitari nell'ambito della ricerca medica, biomedica ed epidemiologica. In particolare, il DDL n. 1110 di conversione in legge, con modificazioni, del D.L. n. 19/2024, recante ulteriori disposizioni urgenti per l'attuazione del piano nazionale di ripresa e resilienza (PNRR), approvato dal Senato lo scorso 23 aprile, ha modificato l'articolo 110 del Codice Privacy, eliminando l'obbligo di consultazione preventiva del Garante Privacy in caso di studi clinici (c.d. retrospettivi) per i quali sia impossibile raccogliere il consenso, determinando così il passaggio da un regime di autorizzazione preventiva ad un regime privo di autorizzazione.

Ne deriva, quindi, che a livello nazionale il consenso o il coinvolgimento del Garante Privacy vengono considerati elementi essenziali, determinando così un accesso a tali dati meno "immediato". Alla luce, invece, del Regolamento in esame, il testo normativo potrebbe costituire la disposizione di legge prevista dall'articolo 9(2) lett. j) del GDPR idonea a costituire la base giuridica dei trattamenti dei dati sanitari ai fini di ricerca.

3. Conclusioni e conseguenze

L'istituzione dello Spazio Europeo dei Dati Sanitari – a seguito dell'adozione formale del nuovo Regolamento EHDS – comporterà senza dubbio importanti vantaggi nonché un impatto significativo nell'ambito della ricerca scientifica e del settore sanitario. E a tal fine, risulta chiara l'impostazione prevista dai legislatori europei – basata sulla possibilità di un *opt-out* da tale riutilizzo, e non di un *opt-in* degli interessati – che consente di riconoscere un'intenzione a "sfruttare" le potenzialità di un sistema diffuso (e regolamentato) di dati sanitari elettronici per una maggior utilità sociale all'interno dell'Unione.

È quindi, necessario che tutti i soggetti coinvolti – cittadini, *data holders* e *data users* – conoscano e comprendano nel dettaglio le opportunità che tale normativa presenta nonché le regole che disciplinano l'accesso e l'uso a tali dati sanitari. Non possono, infatti, essere tralasciati i rischi connessi all'accesso e all'utilizzo di dati sanitari, in particolare per le persone fisiche ma anche per gli operatori sanitari (si pensi ad esempio ai segreti commerciali): quali i rischi connessi a un utilizzo di dati non corretti, precisi e aggiornati, ad accessi abusivi, alla perdita di dati o a un utilizzo non lecito o per finalità discriminatorie. Se da una parte le istituzioni nonché gli Stati membri giocheranno un ruolo fondamentale nel valutare tali rischi e definire le misure di protezione e sicurezza più idonee da implementare quali requisiti per l'accesso e l'utilizzo, dall'altra un utilizzo corretto e consapevole dei dati sanitari da parte degli operatori potrà determinare l'effettivo raggiungimento degli obiettivi posti dalla normativa.

7.6 Digital Services Act

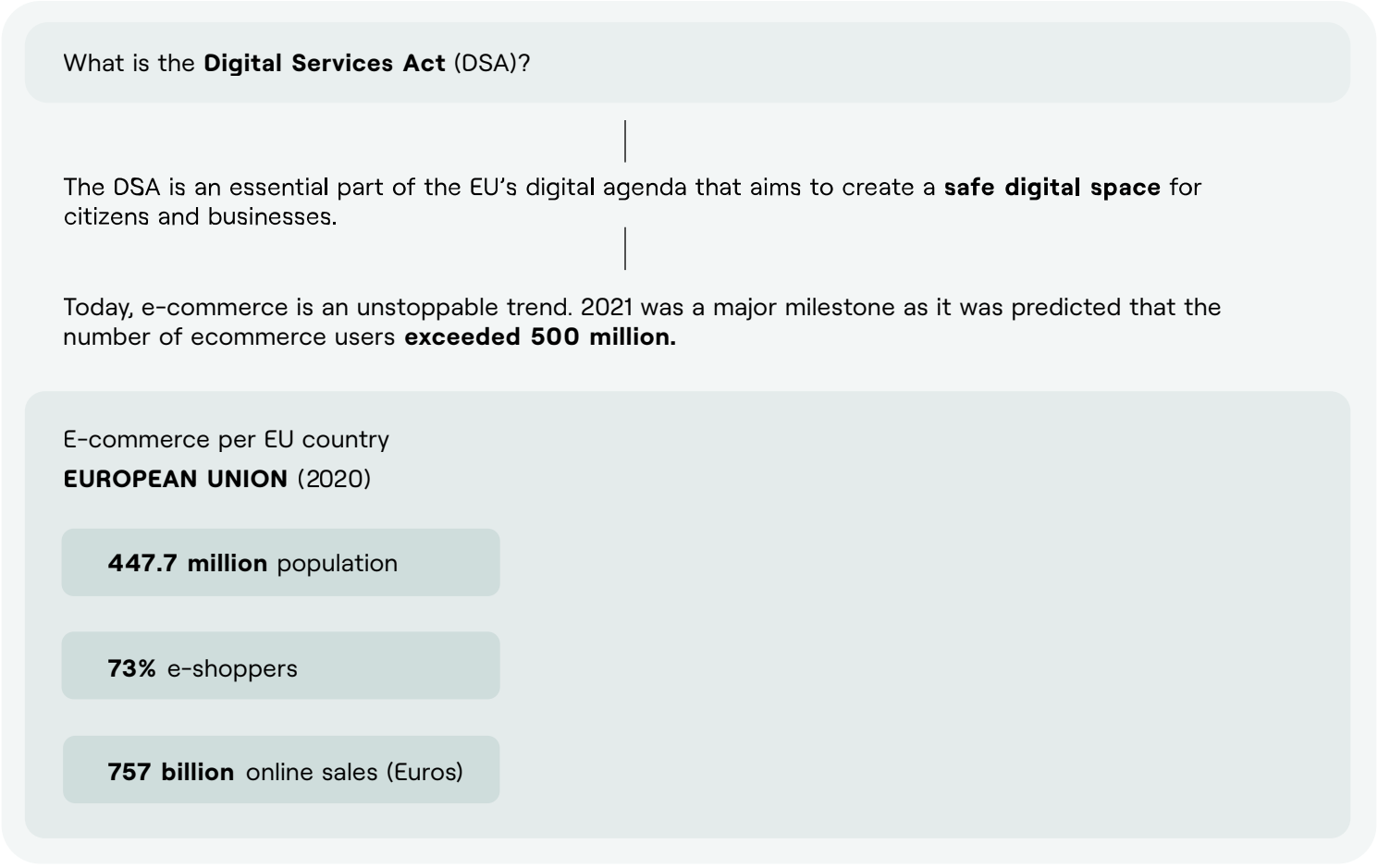
1. Introduzione

Nel corso degli ultimi dieci anni, l'Unione europea si è impegnata nel perseguire una "**sovranità digitale**", orientata sia verso gli Stati membri sia verso gli altri attori internazionali. Questo percorso si è concretizzato attraverso una serie di provvedimenti legislativi volti a regolamentare vari aspetti dell'innovazione e della tecnologia con l'obiettivo di definire norme e principi di rilevanza globale e spesso di ispirazione per altri ordinamenti giuridici.

In questo contesto, il Digital Services Act ("**DSA**") costituisce, insieme al Digital Markets Act ("**DMA**"), un ulteriore strumento per la realizzazione di un quadro **solido, unico ed uniforme** in materia di trasparenza e responsabilità degli intermediari di servizi online, incluse le piattaforme digitali.

Grafico 7.06
Grafico eplicativo del funzionamento del DSA rispetto alla popolazione.

Grafico 7.06

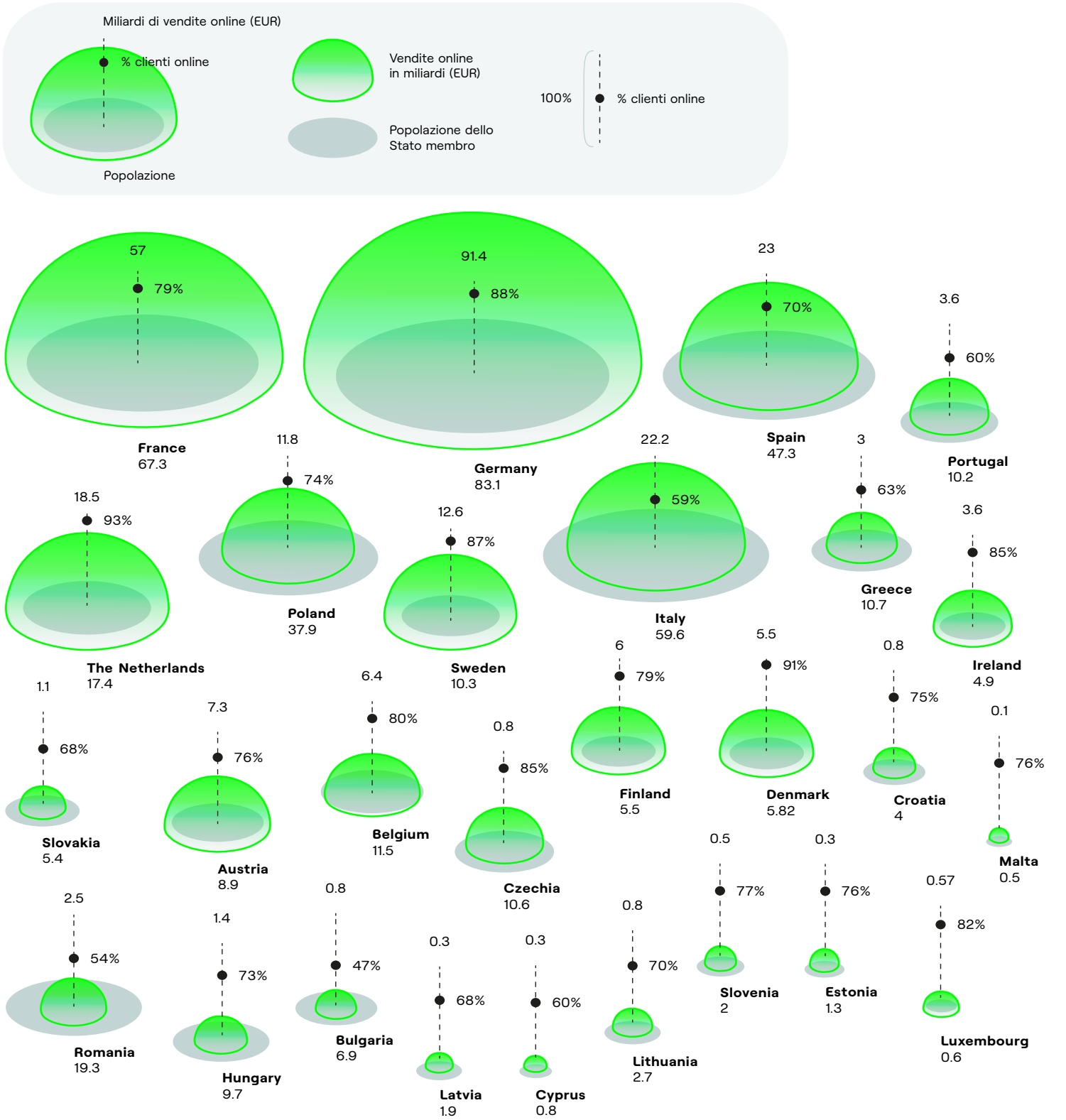


Il DSA non comporta solo l'introduzione di nuovi obblighi in capo piattaforme digitali, ma offre loro anche l'opportunità di migliorare significativamente la loro **reputazione sul mercato**, accrescendo così la **fiducia degli utenti**. L'obiettivo ultimo del DSA è infatti quello di

rafforzare la sicurezza e la responsabilità nel mercato digitale europeo in cui, oggi, è attivo in media il 73% della popolazione.

Grafico 7.07
Visualizzazione vendite *online* in rapporto alla popolazione.
Fonte: Statista e https://www.consilium.europa.eu/it/infographics/digital-services-act/

Grafico 7.07



source: Statista

The new rules will re-shape the rights and obligations of digital service providers, online users, customers and business users in the EU, in line with EU's fundamental rights and values.

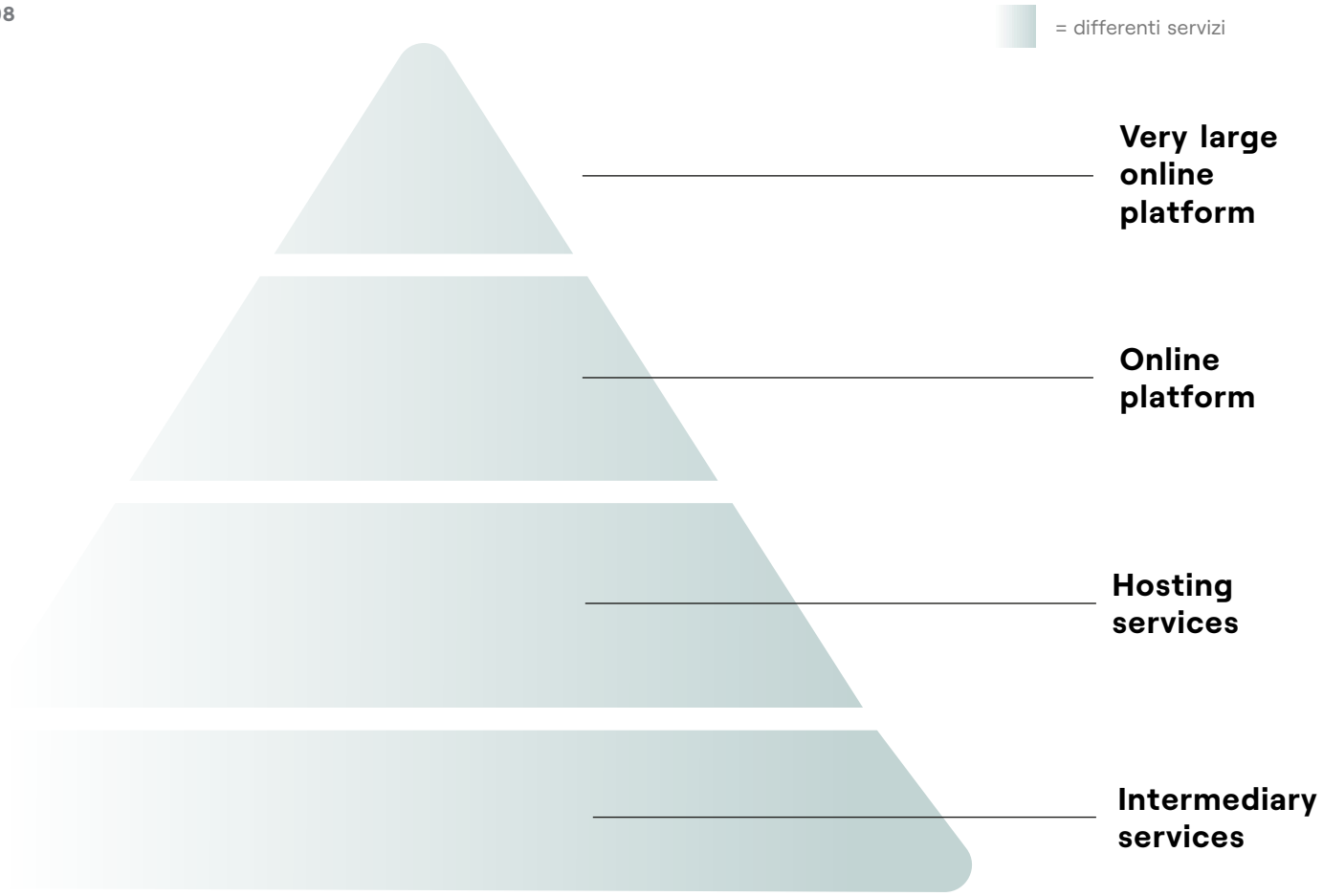
1. Il contesto normativo

Il DSA non comporta solo l'introduzione di nuovi obblighi in capo piattaforme digitali, ma offre loro anche l'opportunità di creare un ambiente online più sicuro e trasparente, stabilendo una serie di obblighi a carico dei fornitori di servizi digitali che fungono da intermediari e, di conseguenza, collegano i consumatori a **merci, servizi e contenuti**.

In una prima fase, la Commissione europea ha designato le piattaforme online di dimensioni molto grandi (*very large online platforms* o "**VLOP**") e i motori di ricerca online di dimensioni molto grandi (*very large online search engines* o "**VLOSE**"), che raggiungono almeno **45 milioni di utenti** nell'UE (ovvero il 10% della popolazione europea). Le VLOP e i VLOSE sono così stati assoggettati, già a partire dal 23 agosto 2023, a norme specifiche in virtù dei particolari rischi che possono comportare nella diffusione di contenuti illegali e disinformazione, prevedendo, ad esempio, sin da subito l'obbligo di pubblicare relazioni di trasparenza sulla loro attività. Le restanti di sposizioni del DSA, invece, sono divenute **pienamente applicabili a partire dal 17 febbraio 2024**.

Grafico 7.08
Classificazione delle differenti tipologie di intermediari.

Grafico 7.08



Il DSA aggiorna ed estende le previsioni normative della Direttiva sul commercio elettronico n. 31 del 2000 (**"Direttiva e-Commerce"**), che aveva posto le prime regole per la regolamentazione dei servizi digitali nell'UE. Le norme esistenti non erano infatti più sufficienti per tenere il passo della rapida evoluzione della tecnologia e dall'aumento esponenziale della digitalizzazione.

In sintesi, il nuovo quadro normativo impone:

→ **obblighi generali a carico di tutti** i fornitori di servizi di intermediazione a destinatari situati o stabiliti nell'UE, indipendentemente dal fatto che il fornitore di servizi di intermediazione sia costituito o situato nell'UE; tali obblighi includono, ad esempio, l'obbligo di fornire un punto di contatto dedicato alle autorità pubbliche e ai destinatari del servizio, l'obbligo di fornire, nei propri termini e condizioni contrattuali, informazioni rispetto alle policy applicate (sui contenuti, restrizioni, moderazione, ecc.) nonché l'obbligo di assicurare un sistema interno di gestione dei reclami;

→ **obblighi supplementari** ai fornitori di servizi di intermediazione che rientrano nella definizione di *(i)* servizi di hosting; *(ii)* piattaforme e *marketplace*; e *(iii)* VLOP e VLOSE, con misure specifiche per contrastare i contenuti e i prodotti illegali, assicurare un processo di *accountability* interno attraverso l'adozione di modelli di valutazione del rischio, rafforzare la tutela dei diritti degli utenti e garantire un approccio più equilibrato tra libertà di espressione e sicurezza online.

La scelta di modificare le regole previste dalla Direttiva e-Commerce con l'adozione di un regolamento, che per definizione è **direttamente applicabile in tutti gli Stati membri**, assicura uniformità delle norme in tutta l'UE, eliminando le fisiologiche discrepanze che si verificano nelle normative nazionali di recepimento delle direttive.

2. Esempi pratici

L'approccio regolatorio del DSA si colloca tra il tradizionale modello di *hard law* e quello dell'autoregolazione, prevedendo da un lato obblighi chiari e vincolanti e dall'altro promuovendo la cooperazione volontaria e la responsabilità interna attraverso l'adozione di codici di condotta e lo svolgimento di attività di audit e reportistica interna.

Tutte le piattaforme online, escluse quelle di dimensioni più piccole (ovvero quelle che contano meno di **50 dipendenti** ed hanno un fatturato annuo e/o un bilancio complessivo annuo **non superiore a 10 milioni di euro**), sono tenute a:

- → istituire, a norma dell'**art. 20**, **meccanismi di reclamo e di ricorso**, fornendo agli utenti l'accesso a un sistema interno che consenta di presentare per via elettronica e gratuitamente reclami contro le decisioni prese dal fornitore della piattaforma online e meccanismi di risoluzione extragiudiziale delle controversie (**art. 21**); e

- → cooperare con segnalatori attendibili, ovvero soggetti che, a norma dell'**art. 22**, dispongono di capacità e competenze particolari ai fini dell'individuazione e della notifica di contenuti illegali e che svolgono le proprie attività al fine di presentare le segnalazioni in modo diligente, accurato e obiettivo in posizione di indipendenza da qualsiasi fornitore di piattaforme online;

- → adottare misure contro le segnalazioni abusive, gestire i reclami, verificare le credenziali di fornitori terzi e garantire agli utenti la trasparenza degli annunci online (**art. 20-23**);

- → rendere pubbliche, ai sensi dell'**art. 15**, le **relazioni annuali** sulla moderazione dei contenuti, che devono includere informazioni sulle iniziative di moderazione, comprese quelle relative ai contenuti illegali, all'uso di strumenti automatizzati, alle misure di formazione e ai reclami ricevuti nell'ambito dei sistemi di gestione dei reclami – solo per VLOP e VLOSE tali relazioni devono essere pubblicate ogni sei mesi (**art. 42**);

- → per i servizi di *marketplace*, intensificare le verifiche sull'**identità dei venditori** e sull'**autenticità dei prodotti** offerti. Questo include l'obbligo di verificare periodicamente la conformità dei prodotti tramite database esistenti, contribuendo così a ridurre la vendita di merci contraffatte o non conformi alle normative vigenti (**artt. 31 e 32**). Oltre a queste misure, il DSA impone ai *marketplace* di adottare processi di *'know your business customer'*, che richiedono la verifica delle informazioni aziendali dei venditori per assicurarsi che siano soggetti affidabili. Questo meccanismo serve a proteggere i consumatori da prodotti contraffatti o pericolosi e a promuovere un ambiente di mercato online più sicuro e affidabile;

- → **garantire la privacy e la protezione dei dati personali**, rispettando le limitazioni alla raccolta e all'utilizzo dei dati personali, soprattutto riguardo alla pubblicità mirata e alla profilazione degli utenti, con particolare attenzione alla protezione dei minori online (**art. 28**).

Grafico 7.10

Grafico 7.10
Riassunto dei principali nuovi obblighi previsti dal DSA

Riassunto dei principali nuovi obblighi previsti dal DSA

Tra gli obblighi supplementari vi è quello di instaurare processi efficaci per la rimozione o il blocco dell'accesso ai **contenuti illegali**, quali materiali di estremismo violento, incitamento all'odio, o informazioni palesemente false e dannose. Tali misure devono essere rapide, trasparenti e devono rispettare i diritti fondamentali degli utenti, inclusa la libertà di espressione. Il regolamento impone alle VLOP e ai VLOSE di adottare sistemi che permettano agli utenti di segnalare contenuti illegali in modo semplice e diretto, e richiede che tali segnalazioni siano trattate in maniera equa e tempestiva (**art. 35**).
Le violazioni del DSA possono comportare **sanzioni fino al 6% del fatturato annuo totale** del fornitore di servizi intermediari interessato nell'esercizio finanziario precedente e i destinatari dei servizi digitali hanno il diritto di richiedere un risarcimento per eventuali danni o perdite subite a causa delle violazioni commesse dalle piattaforme.

3. Impatto e suggerimenti operativi

L'introduzione del DSA implica all'interno delle aziende investimenti sia in termini di strategia sia in termini di compliance - in particolare, delle VLOP che, come visto, devono adeguarsi a una serie di obblighi supplementari articolata.
In generale, le piattaforme online devono:

→ **Investire in tecnologie di moderazione**, in quanto l'adozione di soluzioni tecnologiche avanzate, come l'intelligenza artificiale e il *machine learning*, è fondamentale per monitorare, rilevare e gestire i contenuti in maniera efficiente e conforme ai nuovi standard normativi. Queste tecnologie possono aiutare a identificare automaticamente contenuti potenzialmente illegali o problematici, riducendo il rischio di violazioni e migliorando la reattività alle segnalazioni degli utenti.

→ **Investire nella compliance**, dal momento che sarà sempre più essenziale disporre di team specializzati in grado di interpretare il quadro regolatorio europeo. Per esempio, è fondamentale che le piattaforme digitali rendano le proprie interfacce online sufficientemente chiare, intelligibili e prive di ambiguità - specialmente nel descrivere le modalità con cui vengono mostrati annunci pubblicitari e di profilazione degli utenti - e tali da non compromettere scelte consapevoli da parte dei consumatori.

D'altro canto, il DSA ha un impatto significativo su tutte tipologie di imprese digitali, comprese le piccole e medie imprese (PMI), le startup e le scale-up. In termini di costi, questo impatto varia in base alle dimensioni, alle risorse e alle capacità delle imprese di conformarsi alle nuove regolamentazioni, con la possibilità di accedere a risorse e supporto per attenuare le spese associate alla compliance.

Allo stesso tempo, l'implementazione delle nuove regole previste dal DSA può rappresentare un'opportunità per elevare i servizi, gli standard etici e il posizionamento nel mercato unico digitale, garantendo a PMI, startup e scale-up di poter crescere in un contesto più equo e trasparente.

7.7 Digital Markets Act

1. Introduzione

Il Regolamento (UE) 2022/1925 (detto anche "Digital Markets Act" o "**DMA**") – adottato il 14 settembre 2022 e applicabile dal 2 maggio 2023 – stabilisce norme volte a garantire **contendibilità**[26] ed **equità** nei mercati digitali, imponendo obblighi generali *ex ante* sulle piattaforme *online* di grandi dimensioni che ne controllano l'accesso (i "***gatekeeper***") e che forniscono i cosiddetti servizi di piattaforma di base ("***core platform services***" o "**CPS**"). Insieme al Digital Services Act ("**DSA**"), il DMA rappresenta parte fondamentale della strategia digitale dell'Unione europea e si affianca alla già esistente disciplina *antitrust* di cui agli articoli 101 e 102 TFUE.

Dal momento che le piattaforme digitali che operano nell'UE sono più di 10.000 e il 90% di queste sono piccole e medie imprese, il DMA – insieme al DSA – punta a creare condizioni di parità sui mercati digitali che consentiranno alle PMI digitali innovative di crescere e competere nell'UE e nel mondo: l'obiettivo finale del DMA, dunque, è quello di offrire più scelta per i consumatori, e meno ostacoli per i concorrenti di minori dimensioni.

[26] I mercati si definiscono contendibili quando non presentano né barriere all'entrata, né barriere all'uscita (a causa di costi irrecuperabili, c.d. "*sunk cost*", e costi di uscita). La contendibilità viene definita dunque come la capacità delle imprese di superare efficacemente le barriere all'ingresso e all'espansione e può risultare limitata dagli effetti di rete, forti economie di scala e vantaggi derivanti dai dati delle imprese già presenti sul mercato in maniera consolidata. La scarsa contendibilità incide negativamente sul potenziale di innovazione dell'economia delle piattaforme *online* nel suo complesso.

2. Il contesto normativo

(a) Quali sono i servizi interessati dalla normativa (i c.d. CPS)?

In base all'art. 2 del DMA, le nuove norme si applicano ad una categoria circoscritta di CPS specificamente individuati, ossia: **servizi di intermediazione online; motori di ricerca; servizi di *social network*; servizi di piattaforma per la condivisione di video; servizi di comunicazione interpersonale; sistemi operativi; *browser*; assistenti virtuali; servizi di *cloud computing*; servizi pubblicitari *online***. Questi servizi sono contraddistinti e accomunati da economie di scala estreme, forti effetti di rete, capacità di connettere numerosi utenti commerciali con un gran numero di utenti finali, dipendenza significativa da parte di entrambi gli utenti, effetti di *lock-in*, impossibilità per gli utenti finali di utilizzare più piattaforme per uno stesso scopo e integrazione verticale. Tali caratteristiche, insieme alle potenziali pratiche sleali delle grandi piattaforme, possono avere un impatto significativo sulla competitività e l'equità nei mercati e ridurre ampiamente le scelte disponibili per gli utenti finali.

(b) Chi sono i *gatekeeper*?

A norma dell'art. 3 del DMA, sono designate come *gatekeeper* le imprese che:

I) hanno un **impatto significativo sul mercato interno**: il fatturato annuo deve superare i 7,5 miliardi di euro in ciascuno degli ultimi tre esercizi oppure la capitalizzazione di mercato o il valore equo di mercato equivalente deve essere superiore a 75 miliardi di euro nell'ultimo esercizio e devono fornire lo stesso CPS in almeno tre Stati membri dell'Unione europea;

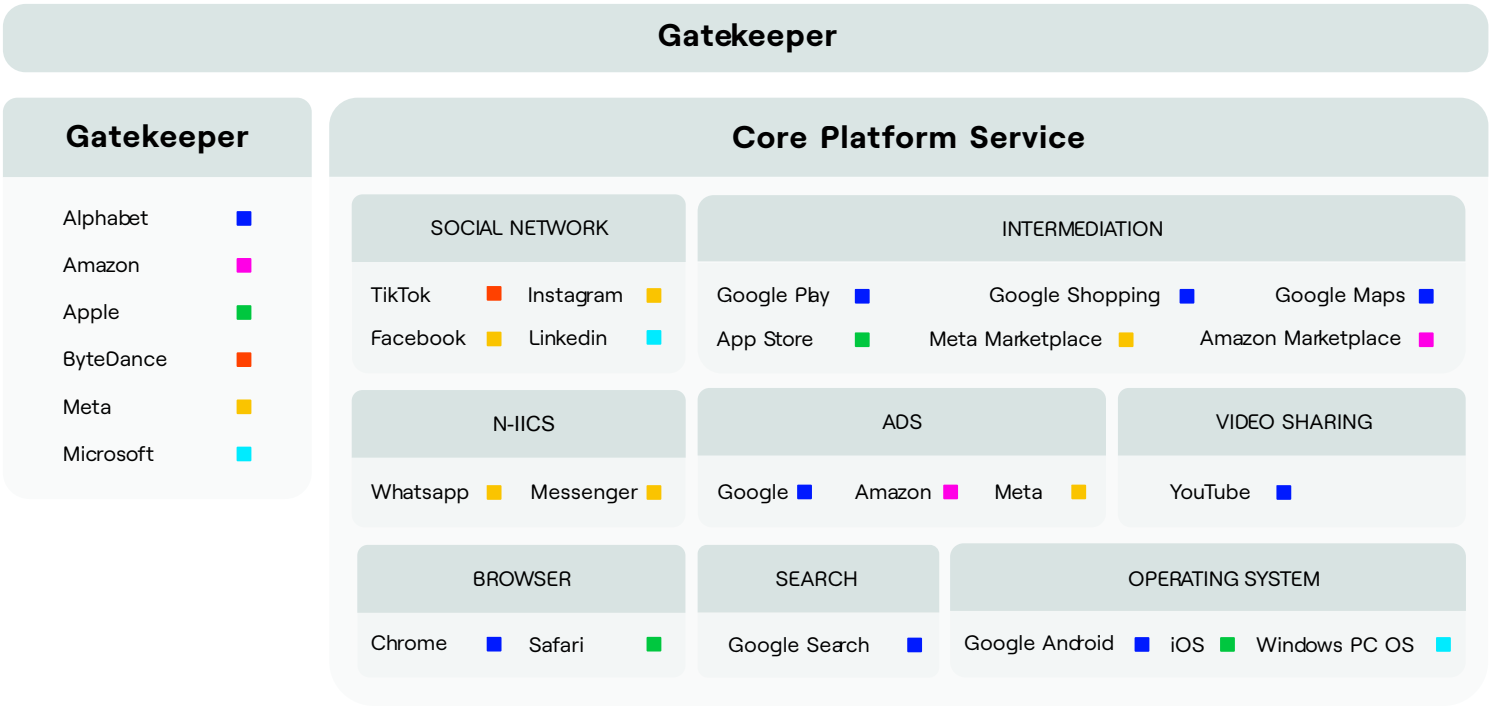
II) forniscono un CPS che costituisce un **punto di accesso importante** affinché gli utenti commerciali raggiungano gli utenti finali: il CPS deve registrare almeno 45 milioni di utenti finali attivi mensili o 10.000 utenti commerciali attivi su base annua con sede o stabilimento nell'UE;

III) detengono una **posizione consolidata e duratura** (attuale o prevedibile in un prossimo futuro): hanno avuto un impatto significativo sul mercato interno e fornito un CPS che costituisce un punto di accesso importante, come precisato ai punti precedenti, per tre esercizi finanziari consecutivi.

I 6 settembre 2023, la Commissione europea ha designato quali gatekeeper Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft in relazione a 22 CPS da loro forniti, tra cui social network, piattaforme di condivisione video, motori di ricerca, browser, sistemi operativi, servizi di intermediazione e servizi di messaggistica (**N-IICS** o Number-Independent Interpersonal Communication Service).

Grafico 7.12
Fonte: https://digital-markets-act.ec.europa.eu/gatekeepers_en
Schema di suddivisione a seconda di piattaforme e servizi dei principali *gatekeepers*.

Grafico 7.12



(c) Quali sono i principali obblighi dei *gatekeeper*?

Il DMA può influenzare e modificare il *business model* delle grandi piattaforme, incidendo *ex ante* sulle loro condotte commerciali. Infatti, i *gatekeeper* dovranno:

- garantire l'interoperabilità delle proprie piattaforme con altri servizi e applicazioni;

- consentire l'installazione, l'utilizzo e l'accesso ad app di terze parti concorrenti o app store sul proprio sistema operativo;

- fornire agli utenti commerciali l'accesso ai dati generati dalle loro attività sulla piattaforma;

- consentire agli utenti commerciali di promuovere offerte e concludere contratti con clienti al di fuori della piattaforma del *gatekeeper*;

- fornire alle imprese che fanno pubblicità sulla piattaforma gli strumenti e le informazioni necessarie (prezzo, commissioni, remunerazione percepita dall'editore e parametro di calcolo) per consentire agli inserzionisti e agli editori di effettuare verifiche indipendenti dei messaggi pubblicitari ospitati dalla piattaforma.

(d) Quali sono i principali divieti imposti ai *gatekeeper*?

Il *gatekeeper* non può:

- riservare ai propri servizi e prodotti un trattamento favorevole in termini di posizionamento, indicizzazione e *crawling* rispetto a servizi o prodotti offerti dai concorrenti sulla loro piattaforma;

- impedire agli utenti di *(I)* disinstallare facilmente applicazioni sul proprio sistema operativo, *(II)* modificare facilmente le configurazioni predefinite sul sistema operativo, assistente virtuale e *browser* del *gatekeeper* e *(III)* omettere, al momento del primo utilizzo, di presentare all'utente le opzioni di scelta circa il motore di ricerca, l'assistente virtuale o il *browser* che intendono utilizzare di *default*;

- imporre clausole volte a impedire agli utenti commerciali di offrire gli stessi prodotti o servizi agli utenti finali tramite altre piattaforme o propri canali di vendita diretta *online* a prezzi o condizioni diversi da quelli offerti attraverso i servizi di intermediazione *online* del *gatekeeper*;

- tenere traccia per finalità pubblicitarie degli utenti finali al di fuori dei servizi essenziali della piattaforma, senza previo consenso dei diretti interessati;

- combinare dati personali ricavati da un CPS con dati personali provenienti da altro servizio offerto dal *gatekeeper* o da terzi, a meno che l'utente finale non abbia prestato il proprio consenso a tale operazione.

(e) Sanzioni

Il DMA consentirà alla Commissione di comminare sanzioni fino al **10%**

del fatturato globale del *gatekeeper*, che possono salire al **20%** in caso di reiterazione della condotta.

3. Esempi pratici - la schermata di scelta dei *browser*

Un *gatekeeper* potrebbe favorire i propri servizi o prodotti, o quelli di terzi, sul suo sistema operativo a discapito di servizi concorrenti di cui gli utenti finali potrebbero usufruire. Ciò può, per esempio, verificarsi quando determinati servizi o applicazioni *software* siano stati **preinstallati** da un *gatekeeper*, ad esempio su un dispositivo con sistema operativo del *gatekeeper* stesso.

Per rimediare a tale situazione, l'art. 6, comma 3, DMA, prevede che gli utenti debbano potere modificare facilmente le impostazioni predefinite del sistema operativo quando tali impostazioni predefinite favoriscono gli stessi servizi e applicazioni del *gatekeeper* come, ad esempio, un *browser*. Al momento del primo utilizzo, nel momento in cui il sistema operativo del *gatekeeper* dirige l'utente verso il suo *browser* (designato come CPS), il *gatekeeper* deve attivare una **schermata di scelta** che consenta all'utente di selezionare un servizio predefinito alternativo. In altre parole, il fornitore di un sistema operativo non può impostare come *browser* predefinito il proprio *browser*. Inoltre, è importante che il *design* dello schermo di scelta del *browser* non impedisca agli utenti di esercitare concretamente la loro scelta all'interno dell'ecosistema del *gatekeeper*, tramite pratiche di manipolazione.

Tale norma sta avendo già i primi impatti significativi sul mercato, stimolando la concorrenza e aiutando fornitori di *browser* meno affermati a guadagnare quote di mercato o, perlomeno, attrarre maggiore attenzione. Da quando i *gatekeeper* designati hanno dovuto conformarsi al DMA, diversi fornitori di *browser* alternativi hanno effettivamente registrato un aumento di *download* dei propri *software*[27].

[27] Fonti: https://techcrunch.com/2024/04/10/eu-dma-browser-choice-screen-early-impact/ e https://www.theverge.com/24040543/eu-dma-digital-markets-act-big-tech-antitrust.

3. Suggerimenti operativi

Grazie al DMA, le piccole e medie imprese e le *start-up* potranno innovare e competere maggiormente con i servizi delle grandi piattaforme *online*. Le PMI e le *start-up* dovrebbero dunque:

- monitorare l'implementazione del DMA e dei requisiti imposti ai *gatekeeper* per comprendere appieno come potrebbero influenzare il loro settore e le loro attività;

- valutare attentamente le nuove opportunità di mercato che potrebbero emergere su mercati precedentemente dominati da *gatekeeper*;

→ partecipare attivamente alle consultazioni pubbliche e alle discussioni sull'implementazione concreta del DMA, facendo sentire la propria voce e contribuendo a plasmare il futuro del settore digitale.

In definitiva, le piccole e medie imprese innovative dovrebbero essere proattive nell'affrontare le sfide e sfruttare le opportunità create dal DMA, mantenendo il focus sulla competitività, sull'innovazione e sull'adattamento alle nuove regole del gioco.

7.8 Regolamento DORA

1. Introduzione

Il Regolamento *Digital Operational Resilience Act*, cd. DORA (il "Regolamento" o "DORA"), è un regolamento dell'Unione Europea (UE) che stabilisce un framework vincolante e completo riguardante la gestione del rischio delle tecnologie di informazione e comunicazione (ICT) per il settore finanziario dell'UE.

I principali obiettivi di DORA sono:

- Gestione del rischio ICT: DORA si concentra sull'individuazione e sulla gestione preventiva dei rischi informatici e di cybersicurezza. L'obiettivo è raggiungere un elevato livello di resilienza operativa digitale.

- Armonizzazione delle normative: Prima di DORA, le norme sulla gestione del rischio ICT per le istituzioni finanziarie dell'UE variavano tra gli Stati membri. DORA mira a eliminare le lacune e le sovrapposizioni armonizzando le regole di gestione del rischio in tutta l'UE..

2. Quando?

Il Regolamento si applicherà a partire dal **17 gennaio 2025.**
DORA è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri dell'UE.

3. Chi? Ambito di applicazione

La nuova regolamentazione si applicherà a tutte le istituzioni finanziarie dell'UE (ivi incluse entità finanziarie tradizionali, quali banche, società di investimento e istituti di credito, assicurazioni ed entità non tradizionali, come fornitori di servizi legati a criptovalute e piattaforme di crowdfunding).

A queste istituzioni, si accosteranno alcune entità generalmente escluse dalla regolamentazione finanziaria (ad esempio, i fornitori di servizi di terze parti che forniscono a ditte finanziarie sistemi e servizi ICT, come fornitori di servizi cloud e data center)(i "Soggetti").

L'articolo 2 di DORA descrive nel dettaglio l'ambito di applicazione.

4. Cosa? Obblighi

Il Regolamento prevede numerosi obblighi a carico dei Soggetti, tra cui:

→ **Adozione di un sistema di governance e gestione del rischio ICT:**
Le istituzioni finanziarie devono identificare e gestire i rischi informatici e di cyber-sicurezza in modo proattivo. Ciò include la valutazione dei rischi, la pianificazione della continuità operativa e la definizione di procedure di risposta agli incidenti.

In tale ambito, l'obiettivo del regolamento è quello di favorire il coordinamento ed allineamento delle strategie di gestione dei rischi ICT da parte dei Soggetti. È attribuito un ruolo fondamentale all'organo di gestione che dovrà (i) assegnare ruoli e responsabilità per tutte le funzioni ICT; (ii) controllare e monitorare la gestione dei rischi ICT e, (iii) allocare adeguatamente investimenti e formazione in ambito ICT.

I Soggetti dovranno adottare procedure di gestione dei rischi connessi alle tecnologie ICT, volte all'individuazione e alla qualificazione del rischio stesso per ridurre gli effetti negativi degli incidenti. Dovranno, a tal fine, mappare i propri sistemi ICT, identificare e classificare funzioni e *asset* critici.

→ **Classificazione degli incidenti e delle minacce informatiche:**

Il Regolamento prevede che le organizzazioni di settore debbano implementare un sistema di mappatura che classifica i vari incidenti sulla base dei criteri descritti nel Regolamento e ulteriormente definiti dalle AEV (Autorità Europee di Vigilanza) per specificare le soglie di rilevanza.

→ **Creazione di sistema di segnalazione degli incidenti informatici:**

Si richiede ai Soggetti di attuare un processo di monitoraggio registrazione e gestione costante degli incidenti connessi alle tecnologie ICT, al fine di notificarli alle autorità competenti.
I Soggetti devono, inoltre, stabilire specifiche procedure per identificare, tracciare, registrare, categorizzare e classificare gli incidenti connessi alle tecnologie ICT in base alla loro priorità, gravità e criticità dei servizi colpiti.

→ **Test di resilienza:**

I Soggetti devono condurre test di resilienza ICT regolari per verificare la loro capacità di resistere a interruzioni operative gravi e per accertarne il grado di maturità, identificarne punti deboli e definire eventuali misure correttive.

Questi test dovrebbero includere scenari di attacco informatico, guasti di sistema e altre minacce.

5. Rischi di terze parti

I Soggetti devono condurre test di resilienza ICT regolari per verificare la loro capacità di resistere a interruzioni operative gravi e per accertarne il grado di maturità, identificarne punti deboli e definire eventuali misure correttive.

6. Condivisione di informazioni

È prevista, a determinate condizioni, la possibilità per le organizzazioni finanziarie di scambiarsi reciprocamente informazioni e analisi delle minacce informatiche, tra cui indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cyber sicurezza e strumenti di configurazione.

7. Sanzioni

Il regolamento, pur dettando criteri di calcolo delle sanzioni, affida alle autorità di vigilanza l'identificazione e la scelta di quest'ultime (tra cui sanzioni amministrative o misure di riparazione per violazioni che, ai sensi del rispettivo diritto nazionale, siano passibili di sanzioni penali). Alle autorità competenti sono conferiti tutti i poteri di vigilanza, di indagine e sanzionatori.

8. Suggerimenti operativi

Il Regolamento DORA pone in capo ai soggetti rientranti nell'ambito di applicazione del regolamento l'obbligo di documentare adeguatamente le proprie scelte per la gestione della resilienza operativa secondo il principio di ***accountability***.

Inoltre il Regolamento si basa sul principio di **proporzionalità**. Le entità finanziarie devono adempiere alle disposizioni del Regolamento proporzionalmente alla propria dimensione, al profilo di rischio, alla natura e alla complessità dei loro servizi. Ciò implica che ciascuna entità finanziaria possa conformarsi al Regolamento in funzione delle proprie caratteristiche.

I soggetti possono quindi adottare una strategia proattiva che include le seguenti azioni:

- **Valutazione dei rischi:** Effettuare una valutazione completa dei rischi informatici per identificare le vulnerabilità e le minacce potenziali. Considerare anche i rischi derivanti dai fornitori di servizi ICT.
- **Pianificazione della resilienza digitale:** Creare un piano dettagliato per garantire la resilienza operativa digitale. Questo dovrebbe includere procedure di risposta agli incidenti, test di resilienza e procedure di comunicazione.
- **Monitoraggio continuo:** Monitorare costantemente gli indicatori chiave di rischio (KRI) e adotta misure correttive tempestive.

I Soggetti dovranno procedere con:

I) Gap analysis del quadro generale dell'ICT risk management, confrontando la situazione attuale e gli obiettivi da raggiungere per conformarsi al Regolamento;

II) effettuare una valutazione completa dei rischi informatici per identificare le vulnerabilità e le minacce potenziali, considerando anche i rischi derivanti dai fornitori di servizi ICT;

III) creare un piano dettagliato per garantire la resilienza operativa digitale. Questo dovrebbe includere procedure di risposta agli incidenti, test di resilienza e procedure di comunicazione;

IV) gestione dei fornitori: Applicare criteri rigorosi nella selezione e nella gestione dei fornitori di servizi ICT. Valutare regolarmente la loro conformità alle normative e ai requisiti di sicurezza e compiere una valutazione dei fornitori che potrebbero essere qualificati come critici e rinegoziazione dei contratti con quest'ultimi;

V) implementazione dei controlli di sicurezza sulla propria infrastruttura generale;

VI) assicurarsi che il personale sia adeguatamente formato sulla sicurezza informatica e consapevole delle minacce;

VII) adozione di piano che sia adeguato alle esigenze per garantire la business continuity.

9. Grafico esplicativo

Ambito di applicazione:

Tutte le istituzioni finanziarie dell'UE (ivi incluse entità finanziarie tradizionali, quali banche, società di investimento e istituti di credito, ed entità non tradizionali, come fornitori di servizi legati a criptovalute e piattaforme di crowdfunding. A queste istituzioni, si accosteranno alcune entità generalmente escluse dalla regolamentazione finanziaria (ad esempio, i fornitori di servizi di terze parti che forniscono a ditte finanziarie sistemi e servizi ICT, come fornitori di servizi cloud e data center).

Principali obblighi:

- → Adozione di un sistema di governance e organizzazione interna
- → Classificazione degli incidenti e le minacce informatiche
- → Creazione di sistema di segnalazione degli incidenti informatici
- → Test di resilienza
- → Condivisione di informazioni

Suggerimenti operativi per conformarsi al Regolamento:

- → Gap analysis del quadro generale dell'ICT risk management, confrontando la situazione attuale e gli obiettivi da raggiungere per conformarsi al Regolamento;
- → revisione del report degli incidenti;
- → valutazione dei fornitori che potrebbero essere qualificati come critici e rinegoziazione dei contratti con quest'ultimi;
- → predisposizione di un piano di risposta agli incidenti;
- → implementazione dei controlli di sicurezza sulla propria infrastruttura generale;
- → adozione di un piano che sia adeguato alle esigenze per garantire la *business continuity*.

7.9 Cyber Resilience Act

1. Introduzione

Il Cyber Resilience Act (il "CRA") è il regolamento europeo relativo alla sicurezza informatica dei prodotti connessi.

Il Regolamento stabilisce:

a) norme per l'immissione sul mercato di prodotti con elementi digitali per garantire la cyber sicurezza di tali prodotti;

b) requisiti essenziali per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali e obblighi per gli operatori economici in relazione a tali prodotti per quanto riguarda la cyber sicurezza;

c) requisiti essenziali per i processi di gestione delle vulnerabilità messi in atto dai fabbricanti per garantire la cyber sicurezza dei prodotti con elementi digitali durante l'intero ciclo di vita e obblighi per gli operatori economici in relazione a tali processi;

d) norme sulla vigilanza del mercato e sull'applicazione delle norme e dei requisiti di cui sopra.

2. Quando?

Il CRA è entrato in vigore il 10 dicembre 2024. Tuttavia, l'applicazione completa del CRA avverrà a partire dall'11 dicembre 2027.
Alcune misure specifiche seguiranno scadenze differenziate: gli obblighi di segnalazione delle vulnerabilità attivamente sfruttate entreranno in vigore l'11 settembre 2026 mentre il il Capo IV, relativo alla notifica degli organismi di valutazione della conformità, si applicherà dall'11 giugno 2026.

3. Chi? Ambito di applicazione

Ambito oggettivo

La portata del CRA risulta essere molto ampia: si applica ai prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete.

La definizione di "prodotto con elementi digitali" comprende qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati

da remoto, compresi i componenti software o hardware da immettere sul mercato separatamente.
Il CRA tuttavia non si applicherà a quei prodotti per i quali è già prevista una normativa specifica.

Ambito soggettivo

Il regolamento si applica a diversi operatori economici che sono coinvolti nella produzione, distribuzione e gestione dei prodotti con elementi digitali.
Il CRA fa riferimento agli "operatori economici" includendo il *"fabbricante, il rappresentante autorizzato, l'importatore, il distributore o qualsiasi altra persona fisica o giuridica soggetta agli obblighi stabiliti dal presente regolamento".*
Gli operatori economici coinvolti dovranno procedere ad una valutazione dei rischi legati alla cybersicurezza, in tutte le fasi del ciclo produttivo e di vita, dei singoli prodotti con elementi digitali.

4. Cosa?

Gli obiettivi del CRA sono quelli di creare le condizioni (i) per lo sviluppo di prodotti sicuri con elementi digitali garantendo che i prodotti hardware e software siano immessi sul mercato con meno vulnerabilità e sensibilizzare i produttori riguardo la sicurezza durante tutto il ciclo di vita di un prodotto; (ii) che consentano agli utenti di tenere conto della sicurezza informatica nella scelta e nell'utilizzo di prodotti con elementi digitali.

Il CRA prevede obblighi dettagliati e specifici per ciascun operatore economico.

Tra questi ricordiamo l'obbligo del fabbricante di:

→ verificare la conformità del prodotto con gli elementi essenziali descritti nell'allegato del CRA stesso;

→ effettuare una valutazione dei rischi di cyber sicurezza associati a un prodotto con elementi digitali tenendoi conto dei risultati di tale valutazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto con elementi digitali, allo scopo di ridurre al minimo i rischi di cyber sicurezza, prevenire gli incidenti di sicurezza e ridurre al minimo l'impatto di tali incidenti, anche in relazione alla salute e alla sicurezza degli utilizzatori;

→ documentare sistematicamente, in modo proporzionato alla natura e ai rischi di cyber sicurezza, gli aspetti pertinenti di cyber sicurezza relativi al prodotto con elementi digitali, comprese le vulnerabilità di cui viene a conoscenza e qualsiasi informazione pertinente fornita da terzi e, se del caso, aggiornare la valutazione dei rischi del

prodotto;

→ all'atto dell'immissione sul mercato di un prodotto con elementi digitali, includere una valutazione dei rischi di cyber sicurezza nella documentazione tecnica;

→ all'atto dell'immissione sul mercato di un prodotto con elementi digitali e per la durata prevista del prodotto o per un periodo di cinque anni dall'immissione sul mercato del prodotto, a seconda di quale sia il periodo più breve, garantire che le vulnerabilità di tale prodotto siano gestite in modo efficace;

→ segnalare all'Agenzia dell'Unione europea per la cyber sicurezza ("ENISA") entro 24 ore dalla scoperta di una vulnerabilità attivamente sfruttata, includendo una descrizione della vulnerabilità e le misure correttive adottate o proposte.

L'operatore dovrà altresì comunicare all'ENISA eventuali incidenti informatici che abbiano un impatto diretto sul prodotto digitale rientrante nel campo applicativo del CRA.

Gli importatori e i distributori hanno responsabilità meno onerose rispetto ai fabbricanti, ma comunque cruciali per garantire la sicurezza dei prodotti digitali. Le loro azioni includono obblighi di verifica del corretto adempimento da parte del fabbricante; se ritengono o hanno motivo di ritenere che un prodotto con elementi digitali o i processi messi in atto dal fabbricante non siano conformi al CRA, devono evitare di immettere il prodotto sul mercato ed informare il fabbricante e l'autorità di vigilanza; analogamente nel caso in cui il prodotto sia già stato immesso sul mercato, devono adottare misure correttive o, se necessario, ritirare o richiamare il prodotto.

È importante notare che un importatore o distributore potrebbe essere considerato un fabbricante ai fini del CRA se immette sul mercato un prodotto con elementi digitali con il proprio nome o marchio commerciale o apporta una modifica sostanziale a un prodotto con elementi digitali già immesso sul mercato.

5. Sanzioni

Gli Stati membri fissano le norme sulle sanzioni applicabili in caso di violazione del Regolamento da parte degli operatori economici e prendono tutti i provvedimenti necessari per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive.

L'art. 53 del CRA prevede che:

→ la non conformità ai requisiti essenziali di cyber sicurezza è soggetta a sanzioni amministrative pecuniarie fino a 15.000.000 di EURO, o se l'autore del reato è un'impresa, fino al 2,5 % del

fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

→ Le violazioni relative ad altri obblighi comportano una sanzione amministrativa pecuniaria fino a 10.000.000 EUR. Se l'autore è un'impresa, la sanzione può arrivare fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

→ Se un operatore fornisce informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità di vigilanza del mercato, può incorrere in una sanzione amministrativa pecuniaria fino a 5.000.000 EUR. Se l'autore della violazione è un'impresa, la sanzione potrà arrivare fino all'1% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Nel decidere l'importo della sanzione amministrativa pecuniaria in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e si tiene quanto segue in debita considerazione:

a) la natura, la gravità e la durata della violazione e delle sue conseguenze;

b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per una violazione analoga;

c) le dimensioni e la quota di mercato dell'operatore che ha commesso la violazione.

6. Suggerimenti

Con l'approvazione del CRA, gli operatori economici interessati devono iniziare a prepararsi ed intraprendere alcune azioni, tra cui:

→ Revisione approfondita dei prodotti

→ Identificazione delle vulnerabilità di sicurezza

→ Creazione di un ciclo di vita dello sviluppo della sicurezza (SDL)

→ Implementazione di un processo di gestione delle vulnerabilità

→ Rispetto degli obblighi di segnalazione degli incidenti

9. Grafico esplicativo

Ambito oggettivo:

Tutti i prodotti (hardware e software) con componenti connessi, direttamente o indirettamente, con altri dispositivi o reti. In particolare rientra nell'ambito di applicazione il software free e open-source nel caso in cui sia reso disponibile sul mercato nell'ambito di un'attività commerciale.

Classificazione dei prodotti:

→ prodotti non critici;

→ critici di classe I;

→ critici di classe II;

→ altamente critici, individuati caso per caso dalla Commissione Europea.

Ambito soggettivo:

"*operatori economici*" che include indistintamente il "*fabbricante, il rappresentante autorizzato, l'importatore, il distributore o qualsiasi altra persona fisica o giuridica soggetta agli obblighi stabiliti dal presente regolamento*".

7.10 Direttiva Nis 2

1. Introduzione

La "Direttiva UE n. 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione" ("Direttiva Nis2" o "Direttiva") rafforza l'obiettivo di raggiungere un livello comune di cybersicurezza tra gli Stati Membri. La normativa impone obblighi di cybersicurezza stringenti in capo a un'ampia platea di organizzazioni operanti in settori ritenuti critici per il funzionamento della società europea.

2. Quando?

La Direttiva Nis 2 è entrata in vigore il 18 ottobre 2024. Gli Stati membri dell'Unione Europea hanno avuto tempo fino al 17 ottobre 2024 per recepire le disposizioni della Direttiva nel diritto nazionale.

3. Chi? Ambito di applicazione

Una delle novità di maggior interesse della Direttiva Nis 2 è l'ampio novero dei soggetti a cui si applica. In particolare ad:

→ organizzazioni pubbliche e private

→ operanti in settori compresi nelle tipologie "alta criticità" o "altri settori critici" (indicati negli Allegati 1 e 2 della Direttiva) e che soddisfano specifici criteri dimensionali

→ operatori che prestano i loro servizi o svolgano le loro attività all'interno dell'Unione.

Tra i settori qualificati come ad Alta Criticità rientrano il settore (i) dell'energia, (ii) dei trasporti, (iii) bancario, (iv) infrastrutture dei mercati finanziari, (v) sanitario, (vi) acqua potabile, (vii) acque reflue, (viii) infrastrutture digitali, (ix) gestione dei servizi TIC, (x) pubblica amministrazione e (xi) spazio.

Mentre, invece, rientrano negli Altri Settori Critici (i) servizi postali e di corriere; (ii) gestione dei rifiuti; (iii) Fabbricazione, produzione e distribuzione di sostanze chimiche; (iv) produzione, trasformazione e distribuzione di alimenti; (v) fabbricazione; (vi) fornitori di servizi digitali; (vii) ricerca (i "Soggetti").

Per quanto riguarda il criterio dimensionale, rientrano nell'ambito di applicazione:*

I) tutte le grandi imprese appartenenti ai settori sopra individuati con più di 250 dipendenti o un fatturato annuo maggiore di 50 milioni di euro o un totale di bilancio annuo superiore a 43 milioni di euro;

II) le medie imprese appartenenti ai settori sopra individuati con un numero di dipendenti compreso fra 50 e 250 o un fatturato annuo o un totale di bilancio compreso fra 10 e 50 milioni di euro o con un totale di bilancio annuo non superiore a 43 milioni di euro;

III) alcune categorie specifiche di soggetti, anche piccole imprese specificati nell'art. 2 della Direttiva (ad esempio qualora il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali).

*L'elenco sopra riportato è esemplificativo e non esaustivo. E' opportuno compiere una verifica mirata per accertarsi di appartenere ai soggetti che rientrano nell'ambito di applicazione della Direttiva.

4. Cosa? Obblighi e doveri

I Soggetti che rientrano nel perimetro della Direttiva dovranno adottare misure di gestione del rischio di cybersicurezza e obblighi di segnalazione. Tra questi rilevano:

Obblighi di governance: Le aziende devono adottare misure tecniche ed organizzative adeguate e proporzionate per gestire i rischi cyber e prevenire/minimizzare gli impatti degli incidenti di sicurezza.
La Direttiva prevede che gli organi di gestione dei Soggetti (ad esempio il consiglio di amministrazione) (i) approvino le misure di gestione dei rischi di cybersicurezza adottate dai Soggetti; (ii) sovraintendano alla sua attuazione e possano essere ritenuti responsabili di violazione da parte dei Soggetti; (iii) seguano una formazione periodica su tematiche di cybersicurezza e offrano una formazione analoga ai loro dipendenti.

Risk Management: la Direttiva prevede l'obbligo di valutare i rischi e attuare le necessarie misure tecniche e organizzative fornendo un elenco, nell'art. 21, di requisiti cui i soggetti debbono uniformarsi come, ad esempio, politiche di analisi dei rischi e di sicurezza dei sistemi informatici, gestione degli incidenti e politiche e procedure relative all'uso della crittografia. Viene poi citata, tra le misure di gestione del rischio, la capacità di garantire la continuità operativa e con riferimenti ad aspetti quali il backup, il ripristino in caso di disastro e la gestione delle crisi, finalizzati a ridurre al minimo l'impatto di eventuali interruzioni dei servizi erogati.

Sicurezza della catena di approvvigionamento: La NIS 2 richiede una maggiore attenzione alla sicurezza dei fornitori e dei partner commerciali.

I Soggetti dovranno garantire la sicurezza della propria catena di approvvigionamento, presidiando gli aspetti di sicurezza dei rapporti con i propri fornitori, considerandone le vulnerabilità specifiche nonché la qualità complessiva di prodotti e pratiche di cybersicurezza.

Obblighi di segnalazione: le entità coinvolte devono segnalare gli incidenti di sicurezza alle autorità competenti e collaborare nella gestione delle minacce. È previsto il dovere di notificare ai rispettivi *Computer Security Incident Response Team* ("CSIRT") o all'autorità nazionale competente qualsiasi incidente che abbia un impatto significativo sulla fornitura dei loro servizi.

Se opportuno, i Soggetti interessati notificano senza indebito ritardo anche ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.

Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

L'iter di notifica prevede la trasmissione di (i) un preallarme entro il termine di 24 ore da quando si è venuti a conoscenza dell'incidente; (ii) una notifica entro il termine di 72 ore dalla conoscenza dell'incidente, che aggiorni le informazioni del preallarme; (iii) una relazione intermedia sugli aggiornamenti di stato pertinenti su richiesta del CSIRT; (iv) una relazione finale entro un mese dalla trasmissione della notifica, il cui contenuto minimo sarà dettagliato dal legislatore dello stato membro in fase di recepimento.

5. Sanzioni

La Direttiva NIS 2 prevede sanzioni di diversa natura in caso di mancata conformità.

Le sanzioni previste dalla Direttiva sono diverse a seconda del grado di violazione e della gravità dell'incidente e si distinguono in sanzioni amministrative che prevedono (i) sanzioni pecuniarie pari a 10milioni di Euro o il 2% del totale fatturato mondiale (si applicherà la più alta tra le due) per i soggetti essenziali; (ii) sanzioni pecuniarie fino a 7milioni di Euro o fino a 1,4% del fatturato mondiale annuo (si applicherà la più alta tra le due) per soggetti importanti.

Per quanto riguarda le sanzioni penali, queste possono includere multe fino a 20 milioni di Euro o il 4% del fatturato globale annuo dell'azienda (a seconda di quale cifra sia più alta). Oltre alle sanzioni pecuniarie, possono essere applicate misure correttive o restrittive.

Inoltre, i responsabili potrebbero essere soggetti a sanzioni penali personali. Inoltre, misure correttive o restrittive possono essere applicate, come la sospensione delle certificazioni o il divieto temporaneo per i dirigenti di ricoprire ruoli aziendali. Le sanzioni possono variare a livello nazionale e dipendono dalla giurisdizione specifica. È sempre consigliabile consultare la normativa locale per dettagli precisi.

6. La situazione in Italia

In Italia è stato pubblicato il Decreto Legislativo 4 settembre 2024, n. 138 che recepisce la Direttiva Nis 2 (il "Decreto Legislativo").

Il Decreto Legislativo, in particolare:

- → conferma il ruolo centrale dell' Agenzia per Cybersicurezza Nazionale ("ACN"), qualificandola come autorità nazionale competente per la Direttiva ed istituisce le Autorità di settore Nis che dovranno collaborare con l'ACN e supportarla nelle relative funzioni;

- → nomina il CSIRT Italia (Gruppo nazionale di risposta agli incidenti di sicurezza informatica) come organo preposto alle funzioni di gestione degli incidenti di sicurezza informatica per i soggetti rientranti nel perimetro di applicazione;

- → assegna al Ministero della Difesa un ruolo specifico nella gestione delle crisi informatiche che riguardano la difesa e la sicurezza militare dello Stato;

- → istituisce in via permanente un Tavolo per l'attuazione della Direttiva NIS 2, con il compito di formulare proposte, esprimere pareri e adottare iniziative, linee guida e atti di indirizzo;

- → prevede l'ampliamento dell'ambito soggettivo di applicazione della Direttiva, la distinzione tra "soggetti essenziali" e "soggetti importanti" e l'adozione di un criterio dimensionale per la loro individuazione;

- → detta gli adempimenti per i soggetti cui si applicherà la Direttiva NIS 2, come la registrazione su una apposita piattaforma (il "Portale ACN"), che dovrà avvenire ogni anno e permetterà di confermare o meno l'inclusione nel perimetro di applicazione. Tale piattaforma sarà anche la base per le comunicazioni e interazioni tra ACN ed i soggetti interessati;

- → determina i criteri per identificare i soggetti che rientrano nel perimetro di applicazione ed i relativi obblighi per quanto riguarda la gestione dei rischi per la sicurezza informatica come, ad esempio, l'obbligo di notificare all'ACN gli incidenti che abbiano avuto impatto sui servizi forniti ed il contenuto delle relative

notifiche e, di aggiornare l'ACN con una relazione intermedia e di redigere una relazione finale entro un mese dalla notifica dell'incidente;

→ stabilisce che gli operatori rientranti nel perimetro di applicazione della Direttiva NIS 2 potranno essere soggetti ad attività di di vigilanza ed audit periodici e mirati sulla sicurezza, da parte di organismi indipendenti o dall'ACN.

→ prevede che qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per conto del soggetto o di esercitare un controllo sul soggetto stesso, assicura il rispetto delle disposizioni di cui al presente decreto. Tali persone fisiche possono essere ritenute responsabili dell'inadempimento in caso di violazione del presente decreto da parte del soggetto di cui hanno rappresentanza. Qualora il soggetto non adempia nei termini stabiliti dalla diffida, l'Autorità può disporre nei confronti delle persone fisiche l'applicazione della sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto. Tale sospensione temporanea è applicata finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide.

→ prevede per i soggetti essenziali, escluse le pubbliche amministrazioni, sanzioni che possono giungere sino ad un massimo di euro 10.000.000 o del 2% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto; mentre per i soggetti importanti, sino a un massimo di euro 7.000.000 o dell'1,4% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto.

Grafico 7.14
I passaggi operativi suggeriti per proteggere la sicurezza informatica della propria organizzazione.

7. Ambito di Applicazione

- Soggetti essenziali (es.: energia, sanità, trasporti, infrastrutture digitali).
- Soggetti importanti (es.: fornitori di servizi digitali, cloud, data center).

Le aziende devono verificare se rientrano nel perimetro attraverso un self-assessment.

8. Obblighi Principali per le Aziende

Le imprese rientranti nel perimetro sono soggette a obblighi stringenti:

→ REGISTRAZIONE ANNUALE SUL PORTALE ACN
La registrazione o l'aggiornamento dei dati è obbligatoria dal 1 gennaio al 28 febbraio di ogni anno (o entro il 17 gennaio per alcuni settori specifici come cloud e data center).

→ NOTIFICA DEGLI INCIDENTI DI SICUREZZA
- Obbligo di segnalare gli incidenti con tre livelli di reporting:
- Entro 24 ore: notifica iniziale.
- Entro 72 ore: relazione intermedia.
- Entro 30 giorni: relazione finale.
- Fornitura di informazioni:

Le aziende incluse nel perimetro dovranno trasmettere all'ACN le informazioni richieste entro un periodo stabilito (es.: dal 15 aprile al 31 maggio).

→ VIGILANZA E AUDIT
Le aziende saranno soggette a:
- Audit periodici e mirati sulla sicurezza informatica da parte dell'ACN o organismi indipendenti.
- Controlli per verificare l'implementazione delle misure richieste dalla Direttiva.

→ TEMPISTICHE E SCADENZE CHIAVE
31 dicembre 2024:
Completamento del self-assessment per verificare l'applicabilità della Direttiva.

1 gennaio - 28 febbraio 2025:
Registrazione annuale sul Portale ACN.

31 marzo 2025:
Comunicazione dell'inclusione nel perimetro da parte dell'ACN.

5 aprile - 31 maggio 2025:
Fornitura delle informazioni richieste per i soggetti inclusi nel perimetro.

1 gennaio 2026:
Obbligo di notifica degli incidenti di sicurezza.

13. Suggerimenti operativi

L'ACN ha pubblicato delle linee guida che stabiliscono i termini, le modalità ed i procedimenti di utilizzo e accesso al Portale ACN e, in particolare, ai Servizi NIS nonché le ulteriori informazioni che i soggetti rientranti nel perimetro di applicazione devono fornire all'ACN ai fini dello svolgimento delle funzioni attribuite dal Decreto Legislativo.

Grafico 7.14

Passaggio	Descrizione
1 - Designare un responsabile della sicurezza informatica:	Identifica una figura all'interno dell'organizzazione responsabile della gestione della sicurezza informatica.
2 - Sviluppare una politica di sicurezza informatica:	Crea una politica che definisca le misure di sicurezza da adottare e le procedure per gestire gli incidenti.
3 - Implementare misure di sicurezza tecniche e organizzative appropriate:	Valuta e adotta le misure necessarie per proteggere i sistemi e i dati.
4 - Monitorare e tenere aggiornato:	Mantieni un approccio continuo alla sicurezza, monitorando costantemente le minacce e aggiornando le misure di protezione.

I soggetti tenuti a conformarsi alla Direttiva dovranno procedere:

I) ad una valutazione completa dei rischi cyber per identificare le minacce e le vulnerabilità nei propri sistemi informatici e reti, mappando le risorse critiche, l'analisi delle minacce e la valutazione dell'impatto di eventuali incidenti;

II) alla pianificazione e implementazione delle misure di sicurezza sulla base dei risultati della valutazione dei rischi e sviluppare un piano di sicurezza che includa misure specifiche per mitigare le vulnerabilità identificate;

III) formare il personale su buone pratiche di sicurezza informatica e sensibilizzarlo sui rischi cyber (ad esempio con sessioni di formazione periodiche, simulazioni di phishing e promozione di una cultura della sicurezza;

IV) collaborare con le autorità competenti del proprio Stato Membro per segnalare eventuali incidenti di sicurezza e partecipare a esercitazioni di gestione delle crisi;

V) monitorare costantemente i propri sistemi per rilevare eventuali anomalie o attività sospette e rivedere periodicamente il proprio piano di sicurezza in base all'evoluzione delle minacce e delle tecnologie;

VI) verificare ed aggiornare i contratti.

10. Schema esplicativo

Ambito di applicazione:

Si applica a:

→ organizzazioni pubbliche e private che gestiscono servizi essenziali per la società;

→ fornitori di servizi essenziali, società energetiche, servizi sanitari, trasporti, infrastrutture di comunicazione elettronica e servizi bancari e finanziari.

Governance e ruolo degli Stati Membri:

→ Gli Stati Membri devono garantire che i soggetti essenziali e importanti abbiano un organo di gestione che approvi formalmente le misure di gestione dei rischi cyber.

Responsabilità dell'organo di gestione aziendale:

→ L'articolo 20 richiede agli organi di gestione aziendale di assumersi la responsabilità delle misure di cybersecurity.

Valutazione dei rischi:

→ Le organizzazioni conducono una valutazione completa dei rischi cyber per identificare minacce e vulnerabilità nei sistemi informatici e reti.

Pianificazione e implementazione delle misure di sicurezza:

→ Sviluppo di un piano di sicurezza con misure specifiche per mitigare le vulnerabilità.

Formazione e sensibilizzazione:

→ Formazione del personale su buone pratiche di rischi cyber.

Collaborazione con le autorità competenti:

→ Segnalazione di incidenti di sicurezza e partecipazione a esercitazioni di gestione delle crisi.

Monitoraggio e revisione:

→ Monitoraggio costante dei sistemi per rilevare anomalie o attività sospette;

revisione periodica del piano di sicurezza.

Colophon

Capitoli da 1 a 6

7.1 Normative sulla responsabilità da danno cagionato dai sistemi di Intelligenza Artificiale
7.2 Product Liability Directive (2024/2853)

→ **Contributors**
Jacopo Liguori, Valentina Pinna

withersworldwide

7.3 Regolamento (UE) 2022/868 relativo alla governance europea dei dati
7.4 Regolamento (UE) 2023/2854 del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo
7.5 European Health Data Space

→ **Contributors**
Licia Garotti, Marco Galli, Gregorio Lamberti, Vittoria Omarchi, Giorgia Valsecchi, Matilde Maiorano

PedersoliGattai

7.6 Digital Services Act:
7.7 Digital Markets

→ **Contributors 7.6**
Marco Berliri, Valerio Natale, Giacomo Bertelli

→ **Contributors 7.7**
Marco Berliri, Giovanni Trabucco, Erika De Santis

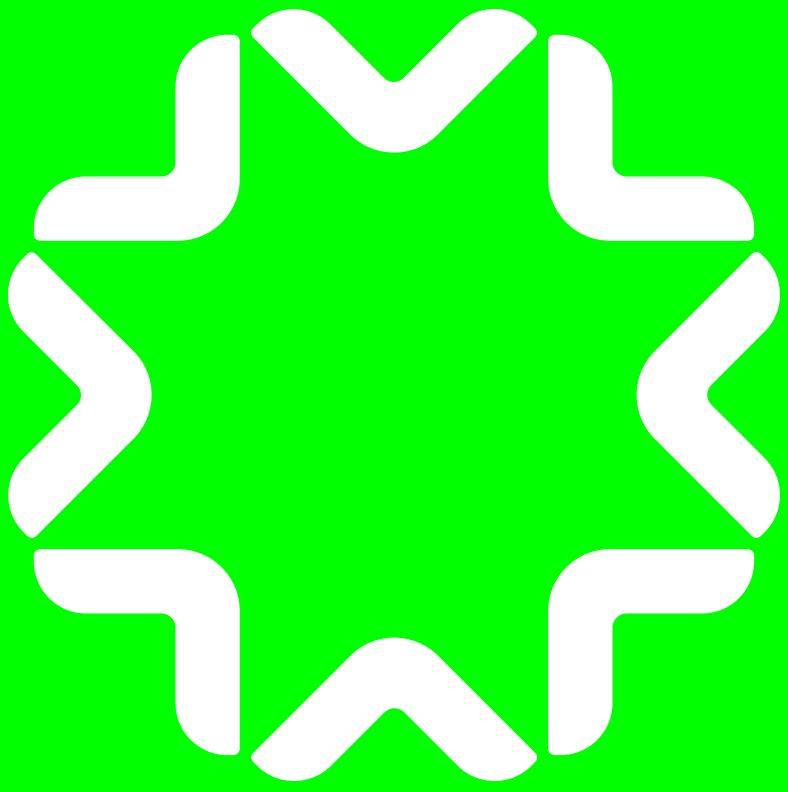
Hogan Lovells

Other Relevant Contributors:

→ **Contributors**
Veronica Muratori, Gianmarco Marani

K&L GATES

ITALIAN
TECH
ALLIANCE



italiantechalliance.com