FIVERS

Aggiornamento
Data protection, AI, IT and IP

n. 4 / 2025

DATA PROTECTION.

7 Febbraio 2024 – AI e GDPR: la CNIL pubblica nuove raccomandazioni su come rendere le Informative privacy e su come gestire le istanze di esercizio dei dir*itti data protection* rispetto alle specificità di sistemi e modelli di Intelligenza Artificiale.

INTELLIGENZA ARTIFICIALE.

18 Febbraio 2025 – Agenzia per l'Italia Digitale (AgID): pubblicate le Linee Guida per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione.

---

12 Febbraio 2025 – Autorità europea per le Assicurazioni: in consultazione pubblica il Parare sull'applicazione del Regolamento sull'Intelligenza Artificiale al settore assicurativo.

---

7 febbraio 2025 – Commessione UE: pubblicate le Linee Guida sulla interpretazione del concetto giuridico di "sistema di intelligenza artificiale" ai sensi dell'articolo 3(1) del Regolamento 2024/1689 (AI Act).

CYBERSECURITY

18 Febbraio 2025 – Banca d'Italia: istruzioni operative e format per l'autovalutazione ICT DORA.

---

18 Febbraio 2025 – Autorità di Vigilanza europee DORA: aggiornate le FAQ sulla compilazione e tenuta dei registri di informazioni.

---

14 Febbraio 2025 – IVASS: lettera al mercato sulle modalità operative per la notifica dei gravi incidenti TIC ai sensi del Regolamento DORA.

---

13 Febbraio 2025 – Commissione UE: pubblicate le norme tecniche di regolamentazione (RTS) esecutive degli obblighi DORA circa l'attuazione dei Test-led-penetration-test – TLPT.

---

12 Febbraio 2025 - In Gazzetta Ufficiale il DPCM 9 dicembre 2024, n. 221 recante i criteri per l'applicazione della clausola di salvaguardia di cui al Decreto legislativo di recepimento della Direttiva NIS 2.

---

7 Febbraio 2025 – L'Agenzia Nazionale per la Cybersicurezza (ACN) ricorda a tutti i soggetti NIS la scadenza del prossimo 28 Febbraio per registrarsi.

---

5 Febbraio 2025 – ENISA: l'Agenzia per la cybersicurezza UE pubblica il programma di lavoro 2025-2027.

---

4 Febbraio 2025 – Unione Europea: entrato in vigore il Regolamento 2025/35 (*Cyber Solidarity Act*).

MERCATI DIGITALI

13 Febbraio 2025 – Parlamento europeo: via libera al pacchetto normativo sull'IVA digitale.

DATA PROTECTION

7 Febbraio 2024 – AI e GDPR: la CNIL pubblica nuove raccomandazioni su come rendere le Informative privacy e su come gestire le istanze di esercizio dei dir*itti data protection* rispetto alle specificità di sistemi e modelli di Intelligenza Artificiale.

Il GDPR consente lo sviluppo di un'IA innovativa e responsabile in Europa. Le nuove raccomandazioni della CNIL lo illustrano fornendo soluzioni concrete per informare le persone i cui dati vengono utilizzati e per facilitare l'esercizio dei loro diritti.

Adattare i principi del GDPR alle specificità dell'IA.

Alcuni modelli di intelligenza artificiale sono anonimi e quindi non sono soggetti al GDPR. Tuttavia, altri modelli, come un modello linguistico di grandi dimensioni (LLM), possono contenere dati personali. Il Comitato europeo per la protezione dei dati (EDPB) ha recentemente fornito criteri pertinenti sull'applicazione del GDPR ai modelli di IA.

Quando si applica il GDPR, i dati delle persone devono essere protetti, sia all'interno di set di dati di addestramento, sia all'interno di modelli che potrebbero aver memorizzato dati o attraverso l'utilizzo del modello tramite prompt. Sebbene i principi fondamentali della protezione dei dati rimangano applicabili, essi devono essere adattati al contesto specifico dell'IA.

La CNIL ha da tempo stabilito che:

- la determinazione dello scopo va applicata in modo flessibile ai sistemi di IA di uso generale: un operatore che non è in grado di definire tutte le potenziali applicazioni nella fase di addestramento può invece descrivere il tipo di sistema in fase di sviluppo e illustrare le principali funzionalità potenziali.
- il principio di minimizzazione dei dati non impedisce l'uso di grandi set di dati di addestramento. Tuttavia, i dati dovrebbero generalmente essere selezionati e puliti per ottimizzare l'addestramento degli algoritmi, evitando al contempo l'inutile elaborazione di dati personali.
- la conservazione dei dati di addestramento può essere estesa se giustificato e se il set di dati è soggetto a misure di sicurezza adeguate. Ciò è particolarmente importante per le banche dati che richiedono investimenti scientifici e finanziari significativi, che a volte diventano standard riconosciuti all'interno della comunità di ricerca.
- in molti casi è possibile il riutilizzo delle banche dati, comprese quelle disponibili online, a condizione che i dati non siano stati raccolti illecitamente e che il loro riutilizzo sia in linea con lo scopo originario della raccolta.

Le due nuove Raccomandazioni: IA e Informativa agli interessati e IA ed esercizio dei diritti data protection.

La CNIL ha pubblicato due nuove Raccomandazioni per promuovere l'uso responsabile dell'IA, garantendo al contempo il rispetto della protezione dei dati personali. Queste raccomandazioni confermano che i requisiti del GDPR sono sufficientemente equilibrati per affrontare le sfide specifiche dell'IA. Esse forniscono soluzioni concrete e proporzionate per informare le persone e facilitare l'esercizio dei loro diritti.

Quando i dati personali sono utilizzati per addestrare un modello di IA e possono essere potenzialmente memorizzati da esso, le persone interessate devono essere informate.

Il modo in cui queste informazioni vengono fornite può essere adattato in base ai rischi per gli individui e ai vincoli operativi. Ai sensi del GDPR, in alcuni casi, soprattutto quando i modelli di intelligenza artificiale si basano su fonti di dati di terze parti e il fornitore non può contattare direttamente le persone, le organizzazioni possono limitarsi a informazioni generali (ad esempio, pubblicate sul loro sito web). Quando vengono utilizzate più fonti, come è comune con i modelli di intelligenza artificiale generici, è generalmente sufficiente un'ampia divulgazione che indichi le categorie di fonti o elenchi alcune fonti chiave.

Quanto alla Raccomandazione sull'esercizio dei diritti, la normativa europea conferisce alle persone fisiche il diritto di accedere, rettificare, opporsi e cancellare i propri dati personali.

Tuttavia, l'esercizio di questi diritti può essere particolarmente impegnativo nel contesto dei modelli di IA, sia a causa delle difficoltà nell'identificare gli individui all'interno del modello sia a causa della modifica del modello stesso. La CNIL esorta gli sviluppatori di intelligenza artificiale a incorporare la protezione della privacy fin dalla fase di progettazione, a prestare particolare attenzione ai dati personali all'interno dei set di dati di addestramento, a sforzarsi di anonimizzare i modelli ogni volta che ciò non compromette lo scopo previsto ed a sviluppare soluzioni innovative per prevenire la divulgazione di dati personali riservati da parte di modelli di IA.

In alcuni casi, il costo, l'impossibilità tecnica o le difficoltà pratiche possono giustificare il rifiuto di soddisfare una richiesta di esercizio di tali diritti. Tuttavia, laddove il diritto debba essere garantito, la CNIL prenderà in considerazione soluzioni ragionevoli a disposizione del creatore del modello e potrà autorizzare termini di riscontro alle istanze scadenze flessibili. La CNIL sottolinea inoltre che la ricerca scientifica in questo settore si sta evolvendo rapidamente ed esorta le parti interessate dell'IA a rimanere informate sugli ultimi progressi per garantire la migliore protezione possibile dei diritti delle persone.

INTELLIGENZA ARTIFICIALE.

18 Febbraio 2025 – Agenzia per l'Italia Digitale (AgID): pubblicate le Linee Guida per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione.

Dal 18 febbraio al 20 marzo 2025 sono in consultazione pubblica le Linee Guida per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione, adottate con la Determinazione n.17/2025.

Previste dal Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026, le Linee Guida di AgID per l'adozione, l'acquisto e lo sviluppo di sistemi di IA nella Pubblica Amministrazione sono emanate seguendo l'iter previsto all'articolo 71 del Codice dell'Amministrazione Digitale (CAD). Quelle in consultazione riguardano, nello specifico, le modalità di adozione dei sistemi di Intelligenza Artificiale, con particolare riferimento agli aspetti di conformità normativa e di impatto organizzativo.

È possibile partecipare alla consultazione, fornendo commenti e suggerimenti, attraverso la piattaforma Forum Italia

---

12 Febbraio 2025 – Autorità europea per le Assicurazioni (EIOPA): in consultazione pubblica il Parare sull'applicazione del Regolamento sull'Intelligenza Artificiale al settore assicurativo.

L'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA) posto in consultazione pubblica la sua *Opinion sulla governance e la gestione dei rischi dell'intelligenza artificiale*, che fornisce alle autorità di vigilanza e alle imprese di assicurazione orientamenti su come interpretare e attuare le disposizioni del settore assicurativo alla luce dell'uso dei sistemi di IA nel settore assicurativo.

Il parere dell'EIOPA fornisce ulteriore chiarezza sui principi e sui requisiti fondamentali previsti dalla legislazione del settore assicurativo che dovrebbero essere presi in considerazione in relazione all'uso dei sistemi di IA.

Si applica a quei sistemi di IA che non sono considerati pratiche di IA vietate o ad alto rischio ai sensi della legge sull'IA.

Sebbene la legislazione in materia di assicurazioni si applichi a tutti i sistemi di IA utilizzati nel settore assicurativo, per evitare complessità e sovrapposizioni normative, l'ambito di applicazione del parere non copre le pratiche di IA vietate o i sistemi di IA ad alto rischio ai sensi della legge sull'IA. Si basa sul principio di proporzionalità e segue un approccio basato su principi, garantendo che sia sufficientemente flessibile per adattarsi agli sviluppi tecnologici e del mercato nel tempo.

Il parere è in linea con i principi e i requisiti di base dell'AI Act e di altre iniziative internazionali in questo settore, come quelle dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), del G20 o dell'Associazione internazionale delle autorità di vigilanza delle assicurazioni (IAIS), sostenendo in tal modo un approccio armonizzato.

Il parere definisce aspettative di vigilanza di alto livello in merito ai principi di governance e di gestione del rischio che le imprese di assicurazione dovrebbero applicare per garantire un uso responsabile dei sistemi di IA adattati a casi d'uso specifici. Questi principi, tra gli altri, includono:

- applicare un approccio proporzionato e basato sul rischio durante l'intero ciclo di vita dei sistemi di IA,
- agire sulla base di correttezza e principi etici, nel migliore interesse dei consumatori,
- definire chiaramente i ruoli e le responsabilità del personale interessato,
- essere in grado di spiegare in modo significativo i risultati dei sistemi di IA,
- l'attuazione di solide politiche di governance dei dati e
- mantenere una documentazione e registri adeguati e ordinati.

---

7 febbraio 2025 – Commessione UE: pubblicate le Linee Guida sulla interpretazione del concetto giuridico di "sistema di intelligenza artificiale" ai sensi dell'articolo 3(1) del Regolamento 2024/1689 (AI Act).

Continua l'azione interpretativa dell'AI Act portata avanti dalla Commissione UE. Dopo la recente approvazione delle Linee Guida sulle pratiche di IA vietate, ecco l'adozione degli orientamenti interpretavi sulla definizione giuridica di "sistema di intelligenza artificiale" (art. 3.1 Reg. 1689/2024).

Anche queste Linee Guida, come quelle sulle pratiche vietate, sono allo stato approvate ma non ancora formalmente adottate. Si tratta di atti rilevanti (ancorché non vincolanti) poiché – come ricordato in precedenti post – la diretta applicabilità a far data dal 2 febbraio 2025 dei primi 5 articoli (compreso l'articolo 3, che reca 68 definizioni giuridiche) consente ora non solo di rivedere in tale prospettiva i contratti con i fornitori di servizi e prodotti AI-based, ma anche (e a ciò mirano le ultime linee guida) ad assistere i fornitori e le altre persone interessate nel determinare se un sistema software costituisca un "sistema di IA" e sia dunque soggetto alle norme del Regolamento.

Per rientrare nell'AI Act, dobbiamo guardare (a) all'architettura del sistema (b) alle funzionalità specifiche e (c) alla presenza dei sette elementi menzionati nella definizione riportata all'articolo 3(1) dell'AI Act, e cioè:

1. Sistema basato su macchine;
2. Autonomia;
3. Adattabilità;
4. Perseguimento di obiettivi impliciti o espliciti;
5. Inferenza e generazione di output utilizzando tecniche di AI;
6. Output quali previsioni, contenuti, raccomandazioni o decisioni;
7. Output che possono influenzare gli ambienti fisici o virtuali.

CYBERSECURITY

18 Febbraio 2025 – Banca d'Italia: istruzioni operative e format per l'autovalutazione ICT DORA.

Con la Comunicazione al mercato dello scorso 23 dicembre 2024 in materia di sicurezza ICT, le entità finanziarie sono state invitate dalla Banca d'Italia a valutare il proprio posizionamento rispetto ai requisiti introdotti dal Regolamento UE 2022/2554 sulla Resilienza Operativa Digitale (DORA) e ad effettuare un'autovalutazione del proprio sistema di gestione dei rischi ICT.

Per agevolare le entità finanziarie nella conduzione delle analisi richieste e, al contempo, favorire la comparabilità delle risposte, la Banca d'Italia ha messo a disposizione degli intermediari

- Istruzioni operative relative alle valutazioni previste dalla Comunicazione al mercato in materia di sicurezza ICT
- Modello per l'autovalutazione rischi ICT

---

18 Febbraio 2025 – Autorità di Vigilanza europee DORA: aggiornate le FAQ sulla compilazione e tenuta dei registri di informazioni.

Le autorità europee di vigilanza (AEV) hanno aggiornato le FAQ sulla segnalazione dei registri di informazioni ai sensi dell'articolo 28, paragrafo 3, del Regolamento DORA. L'aggiornamento include dettagli su quali informazioni devono essere comunicate a partire dal 2025, su come mantenere e comunicare i registri a vari livelli e sulle scadenze per la comunicazione per il 2025 e il 2026. Altri aspetti chiariti nelle FAQ riguardano profili tecnici quali il formato richiesto per i registri, l'uso di modelli e le convenzioni di denominazione dei file per la segnalazione alle AEV.

---

14 Febbraio 2025 – IVASS: lettera al mercato sulle modalità operative per la notifica dei gravi incidenti TIC ai sensi del Regolamento DORA.

L'IVASS ha reso note le modalità operative con cui le imprese assicurative e gli intermediari di assicurazione, di riassicurazione e assicurativi a titolo accessorio di maggiore dimensione sono tenuti a inviare tempestivamente all'Istituto le segnalazioni di grave incidente informatico e, su base volontaria, di minacce cyber ai sensi del Regolamento europeo DORA (Reg. UE 2022/2554 - Digital Operational Resilience Act). Il Regolamento DORA, applicabile dal 17 gennaio 2025, si pone l'obiettivo di conseguire l'adeguata resilienza degli operatori e del sistema finanziario europeo, individuando, tra l'altro, misure per la prevenzione, la risposta e la ripresa delle operazioni in caso di attacco o incidente.

---

13 Febbraio 2025 – Commissione UE: pubblicate le norme tecniche di regolamentazione (RTS) esecutive degli obblighi DORA circa l'attuazione dei Test-led-penetration-test – TLPT.

La Commissione Europea ha pubblicato lo Standard Tecnico di Regolamentazione (RTS) per l'implementazione dei *Threat-Led Penetration Testing (TLPT)* ai sensi del Regolamento DORA.

Solo le entità finanziarie che hanno un certo grado di importanza sistemica e sono sufficientemente mature dal punto di vista delle TIC sono tenute a svolgere un TLPT.

Le entità finanziarie tenute a svolgere un TLPT saranno determinate dalle autorità TLPT. Le autorità TLPT sono definite all'articolo 1, paragrafo 7, delle RTS e comprendono l'autorità pubblica per il settore finanziario dello Stato membro dell'UE. Nel determinare le entità finanziarie tenute a condurre un TLPT, l'autorità TLPT può considerare, tra l'altro:

- fattori di carattere sistemico e di impatto, quali:
-
    - le dimensioni di un'entità finanziaria e se fornisce servizi finanziari in più di uno Stato membro dell'UE;
    - la criticità o l'importanza dei servizi forniti;
    - la sostituibilità dei servizi forniti; e
    - la complessità del modello di business; e
    -
- Fattori di rischio relativi alle TIC, tra cui:
-
    - il profilo di rischio;
    - il panorama delle minacce;

- il grado di dipendenza da funzioni essenziali o importanti dell'entità finanziaria; e
- la maturità delle misure operative di rilevamento e mitigazione della sicurezza delle TIC.

---

12 Febbraio 2025 - In Gazzetta Ufficiale il DPCM 9 dicembre 2024, n. 221 recante i criteri per l'applicazione della clausola di salvaguardia di cui al Decreto legislativo di recepimento della Direttiva NIS 2.

È stato pubblicato nella Gazzetta Ufficiale n. 33 del 10 febbraio 2025 il DPCM 9 dicembre 2024, n. 221, che definisce i criteri per l'applicazione della clausola di salvaguardia prevista dall'art. 3, commi 4 e 12, del Decreto Legislativo n. 138/2024.

Il provvedimento si inserisce nell'ambito del recepimento della Direttiva (UE) 2022/2555 (Direttiva NIS 2), volta a rafforzare la sicurezza informatica a livello europeo, e fornisce indicazioni operative per l'esclusione di alcune imprese dall'applicazione delle misure di cybersicurezza previste dal decreto NIS.

Il regolamento, adottato su proposta dell'Agenzia per la Cybersicurezza Nazionale, stabilisce criteri chiari per la deroga alle norme sulla sicurezza delle reti e dei sistemi informativi, introducendo un meccanismo di registrazione e valutazione per i soggetti richiedenti. L'obiettivo è garantire un equilibrio tra tutela della cybersicurezza e proporzionalità delle misure imposte alle imprese, evitando oneri sproporzionati per realtà aziendali che operano con autonomia infrastrutturale e gestionale.

Di seguito, i criteri per l'applicazione della clausola di salvaguardia di cui all'art. 3 del DPCM:

1. La richiesta di applicazione della clausola di salvaguardia può essere accolta qualora il soggetto dichiari congiuntamente:

a) la totale indipendenza dei propri sistemi informativi e di rete NIS da quelli delle imprese collegate, nel senso che i sistemi informativi e di rete delle imprese collegate non contribuiscono in alcun modo al funzionamento dei sistemi informativi e di rete NIS del soggetto medesimo;

b) la totale indipendenza delle proprie attività e servizi NIS da quelli delle imprese collegate, nel senso che le attività e i servizi delle imprese collegate non contribuiscono in alcun modo allo svolgimento delle attività e all'erogazione dei servizi NIS del soggetto medesimo.

2. La clausola di salvaguardia non può essere richiesta dal soggetto a cui si applica la disciplina del decreto NIS ai sensi dell'articolo 3, comma 10, del medesimo decreto.

---

7 Febbraio 2025 – L'Agenzia Nazionale per la Cybersicurezza (ACN) ricorda a tutti i soggetti NIS la scadenza del prossimo 28 Febbraio per registrarsi.

La nuova direttiva NIS (Network and Information Security), recepita in Italia con il DLGS 138/2024, è ormai entrata in vigore dal 16 ottobre 2024. La direttiva ha l'obiettivo di rafforzare la sicurezza delle reti e dei sistemi informativi, in base a una normativa che introduce previse scadenze e specifici obblighi per le organizzazioni pubbliche e private che operano in settori essenziali.

Per tutti i soggetti NIS, dal primo dicembre al 28 febbraio è possibile registrarsi tramite il portale dei servizi dell'Agenzia per la cybersicurezza nazionale.

Al fine di promuovere uno svolgimento agevole della registrazione, ACN raccomanda di procedere subito al censimento del punto di contatto e alla compilazione della dichiarazione sul portale dei servizi.

Nella sezione dedicata alla nuova disciplina NIS è presente materiale informativo e una ampia collezione di risposte a domande frequenti in costante aggiornamento. ACN segnala, in particolare, la FAQ 3.1 che delinea il processo di autovalutazione che i potenziali soggetti NIS dovranno svolgere per determinare la necessità, o meno, di registrarsi.

Infine, ACN ricorda che l'ultimo termine per la registrazione, per tutti i soggetti NIS, scadrà il prossimo 28 febbraio e che la mancata registrazione entro la predetta data è assistita dalle sanzioni pecuniarie amministrative previste dall'articolo 38, commi 10 e 11, del decreto NIS, fino ad un massimo del 0.1% del fatturato.

---

5 Febbraio 2025 – ENISA: l'Agenzia per la cybersicurezza UE pubblica il programma di lavoro 2025-2027.

Il 5 febbraio 2025, l'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA) ha pubblicato un documento unico di programmazione che delinea la programmazione pluriennale 2025-2027 e il programma di lavoro per il 2025.

Il programma descrive in dettaglio gli obiettivi e le attività dell'ENISA, tra cui l'istituzione di una banca dati delle vulnerabilità dell'UE e di un registro per le entità digitali per migliorare la collaborazione transfrontaliera, nonché la rendicontazione sullo stato della sicurezza informatica dell'UE.

Il programma complessivo riguarda, tra l'altro, gli obiettivi e le attività operative e aziendali dell'ENISA in relazione al recepimento della Direttiva relativa a misure per un elevato livello comune di cibersicurezza nell'Unione (Direttiva NIS 2), nonché l'impatto del Cyber Resilience Act (CRA), del Cyber Solidarity Act (CSA) e del Digital Operational Resilience Act (DORA).

---

4 Febbraio 2025 – Unione Europea: entrato in vigore il Regolamento 2025/35 (Cyber Solidarity Act).

Il 4 febbraio 2025 è entrato in vigore ed è applicabile 25 è stato ufficialmente pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento 2025/35 che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (Cyber Solidarity Act).

Il nuovo regolamento stabilisce le capacità dell'UE per rendere l'Europa più resiliente e reattiva di fronte alle minacce informatiche, rafforzando nel contempo i meccanismi di cooperazione.

Esso mira principalmente a:

- sostenere il rilevamento e la conoscenza delle minacce e degli incidenti di cibersicurezza significativi o su vasta scala
- rafforzare la preparazione e proteggere i soggetti critici e i servizi essenziali, come gli ospedali e i servizi pubblici
- rafforzare la solidarietà a livello dell'UE, la gestione concertata delle crisi e le capacità di risposta in tutti gli Stati membri
- contribuire a garantire un panorama digitale sicuro per i cittadini e le imprese

Per rilevare le minacce informatiche gravi in modo rapido ed efficace, il nuovo regolamento istituisce un "*sistema di allarme in materia di cibersicurezza*", ossia un'infrastruttura paneuropea costituita da poli informatici nazionali e transfrontalieri in tutta l'UE. Si tratta di soggetti incaricati di condividere le informazioni nonché di rilevare le minacce informatiche e agire di conseguenza. Rafforzeranno il quadro europeo esistente mentre, a loro volta, le autorità e i soggetti pertinenti saranno in grado di rispondere in modo più efficiente ed efficace agli incidenti gravi.

Il nuovo regolamento prevede inoltre la creazione di un meccanismo per le emergenze di cibersicurezza destinato ad accrescere la preparazione e potenziare le capacità di risposta agli incidenti nell'UE. Tale meccanismo sosterrà:

- azioni di preparazione, compreso lo svolgimento di verifiche presso soggetti che operano in settori altamente critici (sanità, trasporti, energia ecc.) per rilevare potenziali vulnerabilità sulla base di scenari di rischio e metodologie comuni
- una nuova riserva dell'UE per la cibersicurezza, consistente in servizi di risposta agli incidenti erogati dal settore privato che sono pronti a intervenire su richiesta di uno Stato membro o di istituzioni, organi e organismi dell'UE, nonché di paesi terzi associati, in caso di incidenti di cibersicurezza significativi o su vasta scala
- assistenza reciproca in termini finanziari

Infine, il nuovo regolamento istituisce un meccanismo di valutazione e riesame per valutare, tra l'altro, l'efficacia delle azioni nell'ambito del meccanismo per le emergenze di cibersicurezza e l'uso della riserva per la cibersicurezza, nonché il contributo del regolamento al rafforzamento della posizione competitiva del settore industriale e dei servizi.

Modifica mirata del regolamento sulla cibersicurezza del 2019.

La modifica mirata intende rafforzare la ciberresilienza dell'UE consentendo la futura adozione di sistemi europei di certificazione per i "servizi di sicurezza gestiti". I servizi di sicurezza gestiti, offerti ai clienti da imprese specializzate, sono essenziali per la prevenzione e il rilevamento degli incidenti di cibersicurezza, la risposta agli stessi o la ripresa da essi. Possono consistere, ad esempio, nella gestione degli incidenti, in test di penetrazione, in audit di sicurezza e nella consulenza relativa all'assistenza tecnica.

La modifica consentirà l'introduzione di sistemi europei di certificazione per i servizi di sicurezza gestiti. Contribuirà ad aumentarne la qualità e comparabilità, a promuovere l'emergere di fornitori di servizi di cibersicurezza affidabili e a evitare la frammentazione del mercato interno, visto che alcuni Stati membri hanno già iniziato ad adottare sistemi nazionali di certificazione per i servizi di sicurezza gestiti. In attesa del riesame periodico del regolamento sulla cibersicurezza, previsto entro il 28 giugno 2024, l'accordo provvisorio:

- chiarisce la definizione di "servizi di sicurezza gestiti" e garantisce l'allineamento alla direttiva riveduta sulle reti e i sistemi informativi (NIS 2)
- allinea gli obiettivi di sicurezza di tali sistemi di certificazione agli obiettivi di sicurezza di altri sistemi ai sensi del regolamento sulla cibersicurezza in vigore
- contiene modifiche dell'allegato del regolamento sulla cibersicurezza, in cui figura un elenco di requisiti che gli organismi di valutazione della conformità devono soddisfare
- specifica che la consultazione di tutti i soggetti pertinenti da parte dell'ENISA dovrebbe avvenire tempestivamente e prevede la possibilità che l'ENISA o la Commissione presentino ai colegislatori note informative trimestrali sul funzionamento dei sistemi di certificazione.

MERCATI DIGITALI

13 Febbraio 2025 – Parlamento europeo: via libera al pacchetto normativo sull'IVA digitale.

Dopo l'approvazione da parte del Consiglio UE lo scorso 24 novembre 2024, il Parlamento europeo ha dato il via libera all'aggiornamento della normativa IVA con l'obiettivo di adattarla alle dinamiche del mercato digitale. L'approvazione delle modifiche, che recepiscono le indicazioni espresse dagli Stati membri nel novembre scorso, rappresenta un passo significativo nella lotta alle distorsioni della concorrenza e alle frodi fiscali.

Obbligo di IVA per le piattaforme digitali

Uno degli aspetti più rilevanti della riforma riguarda l'introduzione dell'obbligo di versamento dell'IVA per i servizi forniti attraverso piattaforme online. A partire dal 2030, tali piattaforme saranno tenute a riscuotere e versare l'imposta nella maggior parte dei casi in cui i fornitori di servizi individuali non vi provvedano autonomamente. La misura ha l'obiettivo di porre fine a una disparità normativa che ha finora favorito alcuni settori dell'economia digitale, come gli affitti brevi e il trasporto passeggeri su strada, rispetto alle attività economiche tradizionali, già soggette all'IVA.

Gli Stati membri potranno comunque prevedere esenzioni per le piccole e medie imprese, in linea con la posizione espressa dal Parlamento Europeo, al fine di mitigare l'impatto burocratico per le realtà di dimensioni ridotte.

Digitalizzazione della dichiarazione IVA e contrasto alle frodi

Un ulteriore pilastro della riforma è rappresentato dalla digitalizzazione degli obblighi di dichiarazione IVA per le transazioni transfrontaliere. Entro il 2030, le imprese saranno tenute a emettere fatture elettroniche per le operazioni business-to-business (B2B) internazionali, con una comunicazione automatizzata dei dati alle autorità fiscali competenti. Questa innovazione rafforzerà il contrasto alle frodi IVA, consentendo agli organi di vigilanza di monitorare in tempo reale le transazioni e di ridurre il cosiddetto “gap IVA”, ossia la differenza tra le imposte effettivamente riscosse e quelle dovute.

Semplificazione amministrativa: il rafforzamento degli sportelli unici

Per ridurre gli oneri amministrativi delle imprese operanti su scala internazionale, la normativa prevede il potenziamento degli sportelli unici IVA online. Grazie a questa misura, un numero crescente di aziende potrà adempiere agli obblighi fiscali attraverso un unico portale e in una sola lingua, favorendo una maggiore uniformità e semplificazione nel sistema di riscossione dell'IVA a livello comunitario.

Impatto economico e prospettive future

L'aggiornamento delle norme IVA è frutto di un processo di revisione durato oltre due anni e si inserisce nel più ampio pacchetto normativo "IVA nell'era digitale" (ViDA), presentato dalla Commissione Europea l'8 dicembre 2022. Secondo le stime della Commissione, l'adozione di queste misure consentirà agli Stati membri di recuperare fino a 11 miliardi di euro di IVA non riscossa ogni anno per il prossimo decennio. Inoltre, le imprese beneficeranno di un risparmio annuo stimato in 4,1 miliardi di euro in costi di conformità e 8,7 miliardi di euro in spese amministrative e di registrazione.

Con questa riforma, l'Unione Europea compie un passo decisivo verso un sistema fiscale più equo, trasparente e adeguato alle esigenze del mercato digitale, garantendo una maggiore efficienza sia per le imprese sia per le amministrazioni fiscali nazionali.
