Memento Pratico

COMPLIANCE

AI Act

Nuovi reati 231

NIS2

Antiriciclaggio
Certificazioni ISO
Corpo

Estratto

Lefebvre Giuffrè

INCLUSA VERSIONE DIGITALE

Memento Pratico

COMPLIANCE

Antiriciclaggio
Certificazioni ISO
Corporate Governance
Cybersecurity

Aggiornato al 28 settembre 2025

Lefebvre Giuffrè

L'opera è stata ideata e realizzata dalla

Redazione Memento
Lefebvre Giuffrè

con
i seguenti **Professionisti**

Annalisa De Vivo
Giuseppe Alfieri
Cristina Bauco
Chiara Ciccia Romito
Piercarlo Felice
Camilla Izzi
Silvia Marini
Antonio Valentini
Camilla Zanichelli

Direttore responsabile
Antonella Sciara

Piano dell'opera

CAPITOLO 10

Sicurezza informatica

SOMMARIO

Ogni impresa, indipendentemente dalle dimensioni o dal settore, deve adottare misure di protezione per i propri sistemi, dati e infrastrutture digitali. Sebbene esistano normative specifiche che stabiliscono requisiti di sicurezza per determinati ambiti o categorie di aziende, tutte le imprese, a prescindere dall'ambito normativo specifico a cui sono soggette, sono tenute ad applicare i principi generali previsti in tema di sicurezza informatica nonché apposite misure di sicurezza che costituiscono best practice. **28500**

PRINCIPI GENERALI DI SICUREZZA CIBERNETICA I principi di **riservatezza, integrità** e **disponibilità**, c.d. **triade CIA** (Confidentiality, Integrity, Availability), costituiscono la **base della sicurezza delle informazioni**. **28510**

Gli stessi definiscono i **requisiti di sicurezza primari** cui ogni architettura informativa deve conformarsi, sia nella fase di progettazione sia nell'esercizio operativo.

L'**osservanza** di tali principi intende **garantire che i dati** risultino:

– accessibili esclusivamente da soggetti autorizzati (riservatezza);
– non alterati rispetto al loro stato originale (integrità);
– fruibili con continuità e nei tempi richiesti (disponibilità).

La triade della sicurezza rappresenta, quindi, un insieme di principi che devono essere applicati attraverso un'architettura tecnologica e organizzativa integrata per garantire la protezione dei dati e delle informazioni aziendali.

> L'adozione di queste misure tecniche, unitamente a politiche aziendali e normative specifiche, costituisce il cuore della **gestione della sicurezza delle informazioni**.

OMISSIS

OMISSIS

SEZIONE 9

Intelligenza Artificiale: aspetti di sicurezza informatica

Il Regolamento sull'Intelligenza Artificiale (Reg. UE 2024/1689, c.d. **AI Act**), rappresenta un passo legislativo dell'Unione Europea volto a promuovere lo sviluppo e l'adozione di sistemi di intelligenza artificiale (IA) sicuri e affidabili all'interno del mercato unico, sia nel settore pubblico che privato. L'efficacia delle disposizioni sulla sicurezza informatica dell'AI Act dipende dalla chiara identificazione di cosa costituisce un «sistema di IA», dalla classificazione degli attori soggetti agli obblighi e dalla comprensione del livello di rischio. **29660**

In conformità con l'AI Act, è stata emanata la L. 132/2025, in vigore dal 10 ottobre 2025, volta a disciplinare sul territorio nazionale l'intero sistema dell'intelligenza artificiale. A tal fine il Governo è delegato ad adottare una serie di decreti attuativi entro il 10 ottobre 2026.

DEFINIZIONE (art. 3 AI Act) L'intelligenza artificiale è un sistema di IA automatizzato progettato per funzionare con livelli di autonomia variabili. **29665**

> La definizione **comprende** un ampio spettro di tecnologie, non circoscritte al solo ambito dell'apprendimento automatico (machine learning), ma articolate anche su basi logiche, conoscitive e statistiche. Rientrano, pertanto, nella nozione anche sistemi basati su reti neurali, sistemi esperti, logiche induttive, metodi bayesiani e altre architetture computazionali affini. Il criterio determinante riguarda la facoltà del sistema di **operare in modo autonomo** e di produrre risultati idonei a modificare l'ambiente esterno, sulla base di inferenze, piuttosto che mediante l'esecuzione rigida di istruzioni predeterminate prive di ogni forma di adattamento. Sistemi di automazione che si basano esclusivamente su regole fisse, privi di capacità evolutiva o inferenziale, risultano estranei alla definizione in oggetto.

CATENA DI RESPONSABILITÀ L'AI Act stabilisce una catena di responsabilità che coinvolge **diversi attori**, ciascuno con specifiche funzioni, anche in materia di sicurezza. **29667**

29667 (segue) La distribuzione delle responsabilità lungo la catena di approvvigionamento rappresenta **presupposto essenziale** per la tracciabilità dei doveri imposti agli operatori economici.

Attore	Caratteristica	Funzione
Fornitore (Provider) **(1)**	Qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che sviluppa un sistema o un modello per finalità generali, o che ne commissiona lo sviluppo a terzi	• Sviluppa un sistema di intelligenza artificiale (o ne commissiona lo sviluppo a terzi) e successivamente procede alla sua immissione sul mercato o alla messa in servizio con il proprio nome o marchio, indipendentemente dalla natura onerosa o gratuita dell'operazione • Detiene la responsabilità primaria in ordine alla conformità tecnica del sistema rispetto alla normativa applicabile. In particolare, risponde dell'osservanza dei requisiti essenziali, compresi quelli in materia di cybersicurezza, al fine di garantire l'adozione di misure tecniche e organizzative idonee a garantire l'affidabilità, la robustezza e la resilienza del sistema lungo l'intero ciclo di vita
Utilizzatore (Deployer) **(2)**	Qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne quando l'uso avviene nel corso di un'attività personale non professionale	È responsabile per l'uso sicuro e conforme del sistema nel contesto specifico, compresa la sorveglianza umana e il monitoraggio
Importatore **(2) (3)**	Qualsiasi persona fisica o giuridica ubicata o stabilita nell'UE che immette sul mercato un sistema di intelligenza artificiale contrassegnato dal nome o dal marchio di una persona fisica o giuridica stabilita in un Paese terzo	• Adempie specifici obblighi di verifica e di gestione sicura del sistema, con particolare riferimento alla conformità documentale, alla conservazione delle dichiarazioni di conformità e alla tracciabilità dei requisiti previsti • Controlla l'identità del fabbricante e la presenza della documentazione tecnica completa • Vigila sul rispetto delle condizioni di sicurezza e delle prescrizioni applicabili prima dell'immissione sul mercato
Distributore **(2) (4)**	Qualsiasi persona fisica o giuridica che opera nella catena di approvvigionamento senza rivestire la qualifica di fornitore o di importatore e che procede alla messa a disposizione di un sistema di intelligenza artificiale sul mercato dell'UE	• Verifica la conformità, la conservazione della documentazione prescritta e si occupa della gestione sicura del sistema • Accerta la presenza della marcatura CE • Verifica che il sistema risulti accompagnato da istruzioni chiare e complete • Controlla che il fabbricante abbia redatto la dichiarazione di conformità e che il sistema rispetti integralmente i requisiti stabiliti dalla normativa applicabile

Attore	Caratteristica	Funzione
Rappresentante autorizzato	Persona fisica o giuridica stabilita nell'UE, designata mediante atto scritto da un fornitore avente sede in un Paese terzo, con incarico di agire in nome e per conto di quest'ultimo in relazione a specifici obblighi	Esercita un mandato limitato, circoscritto alle attività espressamente conferite, e risponde dell'adempimento degli obblighi delegati, tra cui rientrano la conservazione della documentazione tecnica, la cooperazione con le autorità competenti e la trasmissione di informazioni o dichiarazioni ufficiali

(1) La figura del fornitore richiama, per struttura e funzione, la nozione di fabbricante già conosciuta nelle normative di prodotto che compongono il c.d. New Legislative Framework. In entrambi i casi, infatti, il ruolo viene definito dall'intreccio di 2 attività principali:
– lo sviluppo diretto di un modello di IA (oppure il suo sviluppo per il tramite di soggetti terzi);
– l'immissione sul mercato o la messa in servizio del sistema con il proprio nome o marchio, indipendentemente dal fatto che ciò avvenga a titolo oneroso o gratuito.
Un aspetto rilevante riguarda l'ambito territoriale, infatti, ai fini del Regolamento IA, non assume importanza il luogo in cui il fornitore sia stabilito, ma conta il fatto che il sistema di IA venga immesso sul mercato o messo in servizio all'interno dell'UE (art. 2, par. 1 lett. a) AI Act).Il Regolamento estende la propria efficacia anche ai soggetti stabiliti fuori dall'UE, nel caso in cui l'output dei sistemi di IA venga utilizzato nel territorio europeo (art. 2, par. 1 lett. c) AI Act). Questa disposizione realizza il c.d. «effetto Bruxelles», ossia l'espansione indiretta della disciplina comunitaria anche oltre i confini dell'UE, imponendo regole europee a operatori extraeuropei che vogliano mantenere rapporti con il mercato interno.
(2) L'importatore, il distributore o l'utilizzatore assumono la qualifica di **fornitore** nel momento in cui immettono sul mercato un sistema di AI con il proprio nome o marchio, oppure realizzano una modifica sostanziale su un sistema già immesso, ovvero alterano la destinazione d'uso in modo da collocare il sistema all'interno della categoria ad alto rischio (art. 25 AI Act). L'attribuzione di tale qualifica determina l'applicazione integrale degli obblighi previsti dall'AI Act, compresi quelli in materia di progettazione, sviluppo, messa a disposizione, monitoraggio post-commercializzazione e cybersicurezza (art. 16 AI Act). La nozione di «**modifica sostanziale**» non presenta definizione automatica e impone un accertamento attraverso la valutazione tecnico-funzionale delle variazioni introdotte, poiché da tale accertamento deriva l'estensione dell'intero impianto regolatorio (artt. 9-15 AI Act).
(3) La figura dell'importatore si attiva solo quando il fornitore, o più in generale il soggetto che appone il marchio sul sistema di IA, è stabilito al di fuori dell'UE. In tale scenario, l'importatore assume un ruolo decisivo, poiché è il soggetto che, per primo, rende disponibile nel mercato europeo un sistema di IA proveniente da un Paese terzo. In altre parole, l'importatore immette in commercio il prodotto acquistato dal fornitore extra UE, divenendo il tramite attraverso cui il sistema entra nel ciclo di utilizzo e consumo all'interno dell'UE. Il suo compito non si limita alla mera transazione commerciale, ma deve garantire che i sistemi importati rispettino gli standard di conformità e che siano accompagnati dalla documentazione prevista dall'AI Act, soprattutto nei casi in cui si tratti di sistemi ad alto rischio.
(4) Nella pratica il distributore è colui che acquista un sistema di IA già immesso sul mercato e lo rivende a terzi, realizzando la c.d. messa a disposizione. Non partecipa dunque alla fase di sviluppo o di importazione, ma si colloca all'interno della catena commerciale europea, con il compito di garantire che il prodotto ceduto sia conforme agli obblighi previsti dall'AI ACT. La sua responsabilità si fonda soprattutto sull'obbligo di diligenza nella verifica dei requisiti e nella corretta trasmissione delle informazioni.

I. Approccio basato sul rischio

29674 L'AI Act adotta un approccio stratificato basato sul rischio, che determina l'intensità degli obblighi normativi, compresi quelli relativi alla sicurezza informatica.
È **vietato** espressamente (art. 5 AI Act) l'uso di sistemi che utilizzano tecniche subliminali, manipolative o ingannevoli, sfruttano vulnerabilità specifiche, effettuano social scoring da parte di autorità pubbliche, o utilizzano determinati sistemi di

identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di applicazione della legge (salvo eccezioni rigorose).

29678 **SISTEMI AD ALTO RISCHIO** (artt. 8-15 AI Act) Rientra nella categoria a rischio alto il sistema destinato a operare come componente di sicurezza di un prodotto, oppure identificabile esso stesso come prodotto, disciplinato dalla normativa di armonizzazione dell'UE (All. I AI Act), qualora la legislazione settoriale imponga una procedura di valutazione della conformità da parte di un organismo notificato.
Risulta **compreso** ogni sistema rientrante nelle aree sensibili e nei casi d'uso (All. III AI Act), tra cui figurano:
– l'identificazione biometrica;
– la gestione delle infrastrutture critiche;
– l'istruzione e la formazione professionale;
– l'accesso al lavoro e ai servizi essenziali;
– l'applicazione della legge;
– la gestione dei flussi migratori e l'amministrazione della giustizia.
L'inclusione in tale elenco produce l'**automatica qualificazione** del sistema come ad alto rischio, salvo il ricorrere delle condizioni derogatorie (art. 6, par. 3, AI Act). In presenza di un compito procedurale chiaramente definito, limitato e non autonomo, finalizzato esclusivamente al miglioramento di un'attività umana preesistente e in assenza di operazioni di profilazione, il sistema può essere escluso dall'ambito di applicazione del Titolo III, Capo 2.

29684 **Classificazione** (artt. 8-15 AI Act) La classificazione di un sistema di intelligenza artificiale come «ad alto rischio» costituisce il **presupposto** per l'applicazione dell'intero corpus di obblighi tecnici e organizzativi previsti dall'AI Act.
Tale qualificazione **comporta**, infatti:
– l'adozione di un **sistema di gestione dei rischi**, con misure documentate e continuative volte a identificare, analizzare e contenere i rischi derivanti dall'impiego del sistema;
– l'attuazione di un **governo strutturato dei dati**, finalizzato a garantire la qualità, la completezza e la pertinenza dei dati utilizzati nello sviluppo, nell'addestramento e nella validazione del sistema;
– la predisposizione di una **documentazione tecnica** completa e accessibile, conforme ai contenuti prescritti dal quadro normativo;
– la conservazione delle **registrazioni**, idonea a garantire la tracciabilità delle operazioni rilevanti ai fini della sicurezza e dell'affidabilità del sistema;
– la fornitura di **informazioni trasparenti** agli utilizzatori, con indicazioni chiare e comprensibili sulle funzionalità, sui limiti e sulle condizioni operative;
– l'istituzione di una **sorveglianza umana efficace**, in grado di garantire un controllo consapevole e tempestivo sul funzionamento del sistema;
– l'integrazione dei **requisiti di accuratezza, robustezza e cybersicurezza**, mediante misure tecniche e organizzative tali da garantire l'affidabilità del sistema, la resistenza ai malfunzionamenti e la protezione contro accessi illeciti o manipolazioni.

29688 La classificazione incide anche sulla **procedura di immissione sul mercato**: per la maggior parte dei sistemi, risulta sufficiente una procedura interna di controllo della conformità, condotta sotto la responsabilità del fornitore, mentre, per alcune categorie specifiche, caratterizzate da rischio elevato, risulta necessaria una verifica preventiva da parte di un soggetto terzo qualificato.

Infine, la classificazione influisce sugli **obblighi successivi all'immissione sul mercato**. Pertanto, il fornitore è tenuto a istituire un sistema di monitoraggio post-commercializzazione, volto a verificare il mantenimento dei requisiti e a individuare tempestivamente eventuali criticità; inoltre, quest'ultimo deve attivare un sistema di segnalazione efficace per eventi gravi o disfunzioni significative, al fine di predisporre una risposta immediata e proporzionata. 29691

SISTEMI A BASSO RISCHIO Rientrano nella categoria a rischio limitato i sistemi che **interagiscono con le persone fisiche** (ad esempio, chatbot) o **generano contenuti** (ad esempio, deepfake) e sono soggetti a **obblighi di trasparenza**. 29696
Gli utenti devono essere **informati** che stanno interagendo con un sistema di IA o che il contenuto è generato artificialmente.
Sebbene non vi siano requisiti di sicurezza informatica diretti nell'AI Act per questa categoria, la sicurezza è rilevante per garantire l'integrità della comunicazione e prevenire manipolazioni non divulgate, oltre agli obblighi derivanti da altre normative come il GDPR se vengono trattati dati personali.

ESCLUSIONI I sistemi esclusi dall'ambito di applicazione dell'AI Act e, di conseguenza, dai suoi specifici obblighi di sicurezza informatica, sono i seguenti: 29704
– sistemi sviluppati o utilizzati esclusivamente per scopi militari, di difesa o di sicurezza nazionale;
– sistemi di IA e loro output utilizzati esclusivamente a fini di ricerca e sviluppo scientifico puro;
– qualsiasi sistema di IA rilasciato con licenze libere e open-source, a meno che non sia immesso sul mercato o messo in servizio come parte di un sistema ad alto rischio o di un sistema rientrante nelle categorie di rischio inaccettabile o limitato;
– sistemi di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca scientifica e sviluppo;
– componenti di IA forniti nell'ambito di procedure semplificate ai sensi di specifiche direttive.
Le esclusioni sono relativamente circoscritte. La maggior parte dei sistemi di IA sviluppati o utilizzati commercialmente all'interno dell'UE, o i cui output sono utilizzati nell'UE, richiederanno un'attenta valutazione per determinare il loro livello di rischio e gli obblighi di cybersicurezza applicabili ai sensi dell'AI Act.

II. Ruoli e compiti operativi di sicurezza

A. Fornitore di sistemi ad alto rischio

AZIONI OPERATIVE Il fornitore che sviluppa un sistema di intelligenza artificiale ad alto rischio e lo immette sul mercato, assume la **responsabilità** primaria in materia di sicurezza informatica. 29715
Le azioni operative richieste sono riepilogate in tabella:

29715
(segue)

Azione operativa	Caratteristica
Istituire un sistema di gestione dei rischi	Adozione di un sistema di gestione del rischio per l'intera durata del ciclo di vita del sistema **(1)**
Integrare la sicurezza nel ciclo di sviluppo dell'IA (Secure AI Development Lifecycle)	• Protezione dei dati: 1. garantisce l'integrità, la riservatezza e la disponibilità dei dati di addestramento, validazione e test 2. applica controlli sull'origine dei dati, tecniche di anonimizzazione e misure di sicurezza coerenti con il trattamento di dati personali • Sicurezza dell'addestramento: 1. protegge l'infrastruttura da accessi non autorizzati 2. garantisce la correttezza del processo e l'affidabilità del modello generato • Robustezza e difese contro attacchi: 1. esegue test specifici per valutare la resilienza tecnica a errori, input anomali e tentativi di compromissione 2. applica tecniche quali adversarial testing e, se necessario, esercizi di red teaming • Tecniche di hardening: 1. rafforza il modello mediante ottimizzazioni compatibili con i requisiti di sicurezza 2. rafforza l'infrastruttura di distribuzione • Gestione delle dipendenze: analizza e mitiga le vulnerabilità presenti nelle librerie software o nei moduli integrati
Applicare requisiti tecnici di accuratezza, robustezza e cybersicurezza	• Resilienza a input errati o condizioni operative impreviste, senza generare malfunzionamenti critici • Difesa attiva contro accessi non autorizzati, compromissione dei dati e interferenze sul modello **(2)** • Conservazione dei log: garantisce la generazione e l'archiviazione sicura di registri temporizzati, immutabili e rilevanti per la sicurezza e la tracciabilità
Predisporre una documentazione tecnica completa	Elenco di informazioni in tema di: – architettura del sistema – dati utilizzati – processo di sviluppo – misure di sicurezza adottate – risultati dei test – metriche di accuratezza – modalità d'uso previste – piano di monitoraggio successivo all'immissione sul mercato
Effettuare la valutazione della conformità	Esecuzione della procedura prevista per attestare la conformità del sistema ai requisiti applicabili, con specifica attenzione alla sicurezza e all'affidabilità
Istituire un sistema di monitoraggio post-commercializzazione	Raccolta di informazioni sulle prestazioni effettive, sui feedback degli utenti, su vulnerabilità emerse successivamente e su incidenti di sicurezza
Gestire aggiornamenti e patch	Disponibilità e distribuzione tempestiva di aggiornamenti correttivi e patch di sicurezza, sulla base delle evidenze emerse nel monitoraggio
Segnalare incidenti gravi e malfunzionamenti	Notifica tempestiva alle autorità competenti di ogni evento grave che compromette i diritti fondamentali o l'affidabilità del sistema

(1) Il sistema analizza e tratta i rischi specifici per la sicurezza informatica, compresi attacchi avversari, compromissione dei dati (data poisoning), vulnerabilità infrastrutturali e dipendenze da componenti terzi. Ogni fase e ogni decisione vengono documentate.
(2) Il fornitore imposta controlli di accesso, meccanismi di autenticazione, protezione dei dati mediante cifratura, e strumenti di rilevamento e risposta.

OBBLIGHI DI SEGNALAZIONE (art. 73 AI Act) Il fornitore di sistemi di IA ad alto rischio deve comunicare tempestivamente alle **autorità di vigilanza** dei **mercati** degli Stati membri in cui si è verificato l'incidente **gli incidenti gravi** che coinvolgono sistemi di IA immessi nel mercato dell'UE. **29720**

La segnalazione deve avvenire **immediatamente** dopo che il fornitore ha stabilito un **nesso causale** tra il sistema di IA e l'incidente. Se non si stabilisce un nesso causale definitivo, la segnalazione deve comunque essere **effettuata entro** 15 giorni dalla conoscenza dell'incidente, tenendo conto della gravità dell'incidente stesso.

Nel caso di un incidente grave che comporta **un'infrazione diffusa** o che abbia implicazioni gravi per la sicurezza e il benessere pubblico, la segnalazione deve essere trasmessa immediatamente e **non oltre** 2 giorni dalla conoscenza dell'incidente. Se necessario, il fornitore può presentare una relazione iniziale incompleta riguardo all'incidente grave, con l'intento di fornire una comunicazione tempestiva. La relazione iniziale sarà seguita da una versione **completa**, che fornirà dettagli ulteriori sull'incidente e sulle azioni intraprese per risolverlo. L'approccio consente di avviare rapidamente il processo di segnalazione, pur mantenendo la necessaria accuratezza nelle informazioni fornite.

Il fornitore del sistema di IA ad alto rischio è tenuto a **condurre indagini** senza indugi sull'incidente grave, valutare i rischi e implementare le misure correttive. Durante tale fase, il fornitore deve **cooperare** con le autorità competenti e, se necessario, con gli organismi notificati. In ogni caso, è indispensabile che il fornitore non compia alcuna modifica al sistema di IA che possa interferire con una futura valutazione delle cause dell'incidente, prima di aver informato le autorità competenti riguardo a tali azioni.

> Un caso particolarmente urgente si verifica quando un incidente provoca il **decesso di una persona**: in questo caso, la segnalazione deve avvenire subito dopo aver stabilito o sospettato il nesso causale tra il sistema di IA e l'incidente grave, ma non oltre 10 giorni dalla conoscenza dell'incidente.

OBBLIGHI SUCCESSIVI Dopo aver ricevuto una segnalazione di incidente grave, l'autorità di vigilanza del mercato deve **informare immediatamente** le autorità nazionali competenti le quali, **entro** 7 giorni, devono adottare le misure appropriate per gestire l'incidente, in conformità con le procedure di notifica. **29726**

Per i sistemi di IA ad alto rischio che sono **componenti di sicurezza di dispositivi** o dispositivi stessi (Reg. UE 2017/745; Reg. UE 2017/746), la segnalazione riguarda solo **incidenti gravi** che rientrano nella **categoria di sicurezza** (art. 3 punto 49 lett. c) Reg. UE 2024/1689).

La **notifica** di tali incidenti deve essere trasmessa all'autorità nazionale competente designata dagli Stati membri in cui si è verificato l'incidente, le quali, a loro volta, sono obbligate a notificare immediatamente alla Commissione Europea qualsiasi incidente grave, indipendentemente dal fatto che abbiano adottato o meno misure nei confronti dell'incidente (art. 20 Reg. UE 2019/1020).

B. Utilizzatore

L'utilizzatore ha la responsabilità di garantire che il sistema sia impiegato in modo sicuro e appropriato nel suo specifico contesto operativo. **29735**

29740 OBBLIGHI L'utilizzatore è tenuto a:

– **osservare** in modo sistematico tutte le **istruzioni** rilasciate dal fornitore, comprese quelle relative alla configurazione sicura del sistema, alla corretta delimitazione dell'uso previsto, alle attività di manutenzione ordinaria e straordinaria, nonché alle misure tecniche e organizzative da adottare nell'ambiente operativo;

– garantire l'**implementazione delle prescrizioni** indicate, senza introdurre modifiche, estensioni funzionali o variazioni nelle condizioni d'impiego che possano compromettere la sicurezza, la robustezza o la conformità del sistema;

– implementare la **sorveglianza umana**, incaricando personale competente previamente formato e autorizzato, sul sistema di intelligenza artificiale ad alto rischio, secondo le istruzioni e le specifiche fornite dal fornitore;

– garantire **qualità e sicurezza dei dati di input** forniti al sistema di intelligenza artificiale esercitando un controllo diretto per verificarne pertinenza, qualità e adeguatezza rispetto alla finalità dichiarata del sistema ed escludendo nonché adottando procedure idonee a escludere input anomali o difformi e mantenendo tracciabilità documentata delle fonti e dei criteri di selezione applicati;

– implementare i **controlli ambientali e infrastrutturali** che si sostanziano in attività di controllo sugli accessi al sistema, mediante autenticazione forte e politiche di autorizzazione granulari; protezione della rete locale, mediante segmentazione, firewall, crittografia delle comunicazioni e verifica dell'integrità dei canali; sicurezza fisica delle infrastrutture, con protezione degli spazi, dei dispositivi e dei supporti contenenti il sistema o dati sensibili;

– monitorare il **funzionamento del sistema nel proprio contesto operativo** e conservare i log, per un periodo minimo di 6 mesi, nei registri (log) generati automaticamente dal sistema, qualora tali dati ricadano sotto la sua sfera di controllo;

– comunicare, senza ritardi, **rischi significativi** e **incidenti gravi** al fornitore o al distributore. In tal caso, sospende l'uso del sistema fino a nuova istruzione e trasmette tempestivamente la segnalazione all'autorità competente per la vigilanza del mercato.

> **Precisazioni 1)** Con riferimento all'**implementazione della sorveglianza umana**, il personale designato dispone delle conoscenze necessarie per:

– monitorare il funzionamento del sistema;

– comprendere gli output generati sulla base delle informazioni rese accessibili attraverso i meccanismi di trasparenza predisposti dal fornitore;

– rilevare tempestivamente eventuali anomalie e segnali di comportamento irregolare potenzialmente riconducibili a vulnerabilità di sicurezza;

– intervenire in modo diretto, sospendere l'operatività del sistema o disattivarne le funzionalità, qualora la prosecuzione del suo utilizzo comprometta la sicurezza, la correttezza operativa o la conformità agli scopi dichiarati.

2) L'accurata **selezione dei dati di input** forniti al sistema di intelligenza artificiale è determinante ai fini della sicurezza operativa, in quanto consente di prevenire l'introduzione di dati corrotti, distorti o intenzionalmente malevoli, idonei a compromettere la robustezza e l'affidabilità del sistema.

3) La **conservazione dei log** risulta essenziale per l'analisi forense e per le indagini successive in caso di incidente o malfunzionamento.

4) In presenza di **incidenti gravi** si applicano anche gli obblighi previsti per la **notifica rafforzata**.

C. Importatore e distributore

L'importatore e il distributore, pur ricoprendo ruoli distinti nella catena del valore, condividono un **nucleo essenziale di obblighi** volti a garantire la conformità e la sicurezza dei sistemi di intelligenza artificiale immessi o resi disponibili sul mercato dell'Unione europea. **29750**

OBBLIGHI Gli obblighi a carico di importatore e distributore comprendono: **29755**
– l'**accertamento preliminare** che il sistema rechi la marcatura CE, risulti accompagnato dalla dichiarazione di conformità dell'UE e dalle istruzioni d'uso redatte in forma accessibile, nonché la verifica dell'identità e della tracciabilità del fornitore o del rappresentante autorizzato, e, se applicabile, dell'altro soggetto coinvolto nella catena distributiva;
– il **controllo delle condizioni logistiche di stoccaggio, movimentazione e trasporto,** sotto la propria responsabilità, al fine che tali condizioni non alterino le caratteristiche del sistema né compromettano il rispetto dei requisiti di sicurezza, robustezza e affidabilità dichiarati;
– la **segnalazione di non conformità** o di potenziali rischi per i diritti fondamentali, la salute, la sicurezza o l'ambiente, al fornitore, all'importatore o al distributore, a seconda dei casi, nonché alle autorità di vigilanza del mercato competenti, partecipando, inoltre, a ogni misura correttiva richiesta dalle autorità per il ripristino della conformità o il ritiro del sistema dal mercato.

III. IA generativa negli ambienti di lavoro

L'introduzione di sistemi di IA generativa negli ambienti di lavoro ha determinato un'accelerazione significativa nei processi di automazione documentale, supporto decisionale e gestione operativa. **29765**
Tali sistemi, basati in larga parte su modelli linguistici di grandi dimensioni (c.d. Large Language Models - **LLM**), ampliano la capacità di elaborazione semantica e di generazione autonoma di contenuti, ma introducono rischi informatici specifici con impatti diretti sulla riservatezza, integrità e disponibilità dei dati.

MODALITÀ OPERATIVE A livello operativo, l'uso di strumenti di IA generativa deve risultare **subordinato** a una valutazione di impatto sulla sicurezza informatica (c.d. cybersecurity risk assessment) e autorizzato da un'apposita funzione aziendale, con particolare attenzione ai profili di data governance e di access control. **29768**
A fini di accountability, la policy aziendale dovrebbe contenere almeno i seguenti **requisiti tecnici**:
– ambiti di utilizzo consentiti, con divieto assoluto di input contenenti dati personali, informazioni riservate o materiali soggetti a segreto professionale o industriale;
– configurazione restrittiva degli strumenti (ad esempio, disabilitazione di integrazioni con repository documentali o directory aziendali);
– validazione umana obbligatoria degli output, con esclusione di utilizzi decisionali, contrattuali o comunicativi in assenza di revisione;

– divieto di accesso da dispositivi non gestiti o da ambienti non conformi alla policy di sicurezza (ad esempio, BYOD non autorizzato);
– formazione tecnica periodica con aggiornamento al mutare delle versioni o delle architetture delle piattaforme impiegate;
– sistema di responsabilità e sanzioni interne, in coerenza con il regolamento aziendale, in caso di violazioni delle regole stabilite.

29774 GESTIONE E PREVENZIONE DEI RISCHI In quanto **tecnologie a interfaccia linguistica**, le piattaforme generative operano attraverso input testuali forniti dall'utente e restituiscono output adattivi.
Questo paradigma espone a **rischi di fughe di dati** (c.d. data leakage) dovuti a:
– inserimento improprio di dati personali, informazioni confidenziali o documenti riservati;
– elaborazione dei dati mediante **infrastrutture cloud esterne**, localizzate in giurisdizioni extra-UE non sempre conformi al GDPR;
– potenziali esposizioni dovute a vulnerabilità infrastrutturali, come evidenziato dal disservizio di OpenAI del marzo 2023, culminato in una violazione di data isolation.
Ulteriori **criticità** derivano da:
– **prompt injection attacks**, quali tecniche di manipolazione che inducono il modello a eseguire operazioni non autorizzate o a rivelare informazioni riservate, sfruttando la propensione del sistema ad accettare ogni input come valido;
– **automation bias**, ossia la progressiva riduzione della vigilanza umana in seguito a un utilizzo sistematico degli output generati, con conseguente rischio di cognitive offloading e deresponsabilizzazione operativa.
Alla luce di tali vulnerabilità, la gestione aziendale non può limitarsi a un'analisi ex post, ma deve **adottare un modello** preventivo e proattivo, conforme ai principi di privacy by design e by default (artt. 5, 24 e 25 GDPR), integrato con gli obblighi derivanti dall'AI Act (ossia, alfabetizzazione digitale e competenza tecnica degli operatori) e con le misure di sicurezza organizzative e tecniche previste dal Decreto Nis.

OMISSIS