

particolare, rimane limitato a quanto strettamente necessario per quanto riguarda il periodo di tempo e l'ambito geografico e personale. Nel decidere in merito alla richiesta, tale autorità tiene conto degli elementi di cui al paragrafo 2. Nessuna decisione che produca effetti giuridici negativi su una persona può essere presa unicamente sulla base dell'output del sistema di identificazione biometrica remota «in tempo reale».

4. Fatto salvo il paragrafo 3, ogni uso di un sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto è notificato alla pertinente autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati conformemente alle regole nazionali di cui al paragrafo 5. La notifica contiene almeno le informazioni di cui al paragrafo 6 e non include dati operativi sensibili.

5. Uno Stato membro può decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni di cui al paragrafo 1, primo comma, lettera h), e ai paragrafi 2 e 3. Gli Stati membri interessati stabiliscono nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo e comunicazione ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati al paragrafo 1, primo comma, lettera h), compresi i reati di cui alla lettera h), punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto. Gli Stati membri notificano tali regole alla Commissione al più tardi 30 giorni dopo la loro adozione. Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota.

6. Le autorità nazionali di vigilanza del mercato e le autorità nazionali per la protezione dei dati degli Stati membri cui è stato notificato l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto a norma del paragrafo 4, presentano alla Commissione relazioni annuali su tale uso. A tal fine, la Commissione fornisce agli Stati membri e alle autorità nazionali di vigilanza del mercato e di protezione dei dati un modello comprendente informazioni sul numero di decisioni che le autorità giudiziarie competenti, o un'autorità amministrativa indipendente la cui decisione è vincolante, hanno adottato in risposta alle richieste di autorizzazione a norma del paragrafo 3 e il loro esito.

7. La Commissione pubblica relazioni annuali sull'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto, fondate sui dati aggregati negli Stati membri sulla base delle relazioni annuali di cui al paragrafo 6. Tali relazioni annuali non includono dati operativi sensibili delle relative attività di contrasto.

8. Il presente articolo lascia impregiudicati i divieti che si applicano qualora una pratica di IA violi altre disposizioni di diritto dell'Unione.

CAPO III

SISTEMI DI IA AD ALTO RISCHIO

SEZIONE 1

Classificazione dei sistemi di IA come «ad alto rischio»

Articolo 6

Regole di classificazione per i sistemi di IA ad alto rischio

1. A prescindere dal fatto che sia immesso sul mercato o messo in servizio indipendentemente dai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

- a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;
- b) il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I.

2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.

3. In deroga al paragrafo 2, un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale.

Il primo comma si applica quando è soddisfatta almeno una qualsiasi delle condizioni seguenti:

- a) il sistema di IA è destinato a eseguire un compito procedurale limitato;
- b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata;
- c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; o
- d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.

Fatto salvo il primo comma, un sistema di IA di cui all'allegato III è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche.

4. Un fornitore che ritiene che un sistema di IA di cui all'allegato III non sia ad alto rischio ne documenta la valutazione prima che tale sistema sia immesso sul mercato oppure messo in servizio. Tale fornitore è soggetto all'obbligo di registrazione di cui all'articolo 49, paragrafo 2. Su richiesta delle autorità nazionali competenti, il fornitore mette a disposizione la documentazione relativa alla valutazione.

5. Dopo aver consultato il consiglio europeo per l'intelligenza artificiale («consiglio per l'IA»), ed entro il 2 febbraio 2026, la Commissione fornisce orientamenti che specificano l'attuazione pratica del presente articolo in linea con l'articolo 96, insieme a un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio.

6. Alla Commissione è conferito il potere di adottare atti delegati in conformità dell'articolo 97 al fine di modificare il paragrafo 3, secondo comma, del presente articolo aggiungendo nuove condizioni a quelle ivi stabilite, oppure modificandole, qualora vi siano prove concrete e affidabili dell'esistenza di sistemi di IA che rientrano nell'ambito di applicazione dell'allegato III ma non presentano un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche.

7. La Commissione adotta atti delegati in conformità dell'articolo 97 al fine di modificare il paragrafo 3, secondo comma, del presente articolo sopprimendo qualsiasi condizione ivi stabilita, qualora vi siano prove concrete e affidabili che è necessario al fine di mantenere il livello di protezione della salute, della sicurezza e dei diritti fondamentali previsto dal presente regolamento.

8. Eventuali modifiche alle condizioni di cui al paragrafo 3, secondo comma, adottate in conformità dei paragrafi 6 e 7 del presente articolo non riducono il livello globale di protezione della salute, della sicurezza e dei diritti fondamentali nell'Unione previsto dal presente regolamento e garantiscono la coerenza con gli atti delegati adottati a norma dell'articolo 7, paragrafo 1, e tengono conto degli sviluppi tecnologici e del mercato.

Articolo 7

Modifiche dell'allegato III

1. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato III aggiungendo o modificando i casi d'uso dei sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

- a) i sistemi di IA sono destinati a essere usati in uno dei settori elencati nell'allegato III;
- b) i sistemi di IA presentano un rischio di danno per la salute e la sicurezza, o di impatto negativo sui diritti fondamentali, e tale rischio è equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio di cui all'allegato III.