Garantire i diritti nell'era dell'IA

Meccanismi di ricorso e tutela dei diritti alla luce del regolamento europeo sull'intelligenza artificiale

HERMES HACKING FOR HUMAN RIGHTS

THE good LOBBY

A cura di **Ernestina Sacchetto** e **Laura Carrer**

Questo policy paper è realizzato da Hermes Center e The Good Lobby Italia nell'ambito del progetto "Your Face, Your Rights" finanziato da European AI & Society Fund.

È stato redatto dall'avvocata Ernestina Sacchetto e da Laura Carrer, con la supervisione di entrambe le organizzazioni.

Il presente policy paper è stato redatto sulla base dei dati e delle fonti normative aggiornate alla data del 30 luglio 2025. Eventuali modifiche legislative o sviluppi giurisprudenziali successivi a tale data non sono stati considerati nell'analisi. Si raccomanda pertanto al lettore di verificare l'eventuale intervenuta evoluzione del quadro normativo o applicativo per un utilizzo conforme e aggiornato delle informazioni contenute nel documento.

Settembre 2025

Indice

Introduzione

L'approvazione del regolamento europeo sull'intelligenza artificiale (UE) 2024/1689, noto come AI Act, segna un passaggio fondamentale nella costruzione di un quadro giuridico europeo volto a disciplinare lo sviluppo, l'adozione e l'utilizzo dei sistemi di intelligenza artificiale (IA) nel mercato interno europeo.

Il documento era stato concepito come esempio di normativa antropocentrica, volto a garantire che l'uso dell'IA fosse sostenibile, affidabile e rispettoso dei diritti fondamentali dell'individuo. Tuttavia, la versione definitiva del testo ha tradito tali obiettivi originari, in quanto ha privilegiato un'architettura normativa basata sul "rischio" per la sicurezza, la salute e i diritti fondamentali, misurandolo rispetto agli interessi economici e strategici dell'industria di intelligenza artificiale. Questo tipo di approccio porta con sé un grave equivoco[1] dal momento che non si possono mettere a bilancio gli interessi delle persone con quelli delle aziende[2].

All'interno di questa cornice, una particolare rilevanza assume il tema dei meccanismi di ricorso ("*redress mechanisms*"). Con l'espressione si intende generalmente qualsiasi procedura che consenta all'individuo o ad un ente di contestarne l'esito di un sistema di intelligenza artificiale, mettere in discussione la logica decisionale e ottenere una forma di riparazione o correzione degli effetti negativi che ne sono derivati.

1 https://www.accessnow.org/eu-regulation-ai-risk-based-approach/
2 https://edri.org/our-work/eu-should-regulate-ai-on-the-basis-of-rights-not-risks/

Nonostante il riconoscimento formale del diritto a presentare un reclamo ad un'autorità di vigilanza del mercato, il testo definitivo del regolamento non indica però in maniera compiuta le caratteristiche e le procedure da seguire per effettuarlo, rinviando genericamente ai sistemi nazionali in materia.

Tale criticità era già stata sollevata nel parere congiunto dello *European Data Protection Board* (EDPB), il comitato europeo per la protezione dei dati, e del Garante europeo della protezione dei dati (GEPD) del 18 giugno 2021, i quali sollecitavano una maggiore chiarezza del testo del regolamento sul tema dei diritti delle persone e dei mezzi di ricorso disponibili in caso di utilizzo improprio dei sistemi di IA o di violazioni di prescrizioni normative previste dal documento normativo.

Alla luce della scarna articolazione dell'articolo 85 dell'AI Act e del generico richiamo alle disposizioni procedurali previste dal regolamento (UE) 2019/1020 in materia di reclami, appare evidente che l'onere di definire in modo puntuale le modalità procedurali dei meccanismi di ricorso e il coordinamento con i sistemi nazionali di tutela giurisdizionale gravi sui singoli Stati membri.

Alcune prime generali indicazioni sul piano nazionale sono presenti nel disegno di legge sull'intelligenza artificiale[3], presentato dal Governo italiano nel marzo scorso, che mira a introdurre principi e criteri direttivi orientati ad adattare la normativa nazionale alle disposizioni del regolamento europeo. Sotto il profilo sistematico e applicativo, però, le soluzioni prospettate appaiono attualmente ancora embrionali e parzialmente indeterminate.

In particolare, non viene esplicitato l'apparato procedurale attraverso cui i *redress mechanisms* dovrebbero essere attuati a livello interno, né vengono chiariti i criteri operativi per la loro applicazione. Manca, dunque, una cornice giuridico-formale che consenta di tradurre le indicazioni programmatiche in dispositivi concretamente azionabili davanti agli organi giurisdizionali o amministrativi competenti.

L'assenza di disciplina procedurale rischia di compromettere l'effettività delle tutele dichiarate, generando incertezza interpretativa e operativa e lasciando ampi margini di discrezionalità all'intervento del giudice o dell'amministrazione. Ne risulta, di fatto, un regime giuridico ancora incompiuto, che necessita di una più estesa elaborazione normativa, tanto

3 Cfr. Disposizioni e deleghe al Governo in materia di intelligenza artificiale, d.d.l. 1146, reperibile all'indirizzo *https://www.senato.it/leggi-e-documenti/disegni-di-legge/scheda-ddl?did=58262*

sul piano sostanziale quanto sul versante procedurale, per assicurare una reale protezione giuridica contro gli abusi derivanti dall'uso improprio dell'intelligenza artificiale.

Glossario

ACN Agenzia per la Cybersicurezza Nazionale

AGID Agenzia per l'Italia Digitale

AI ACT Regolamento (UE) 2024/1689 sull'intelligenza artificiale

AILD Artificial Intelligence Liability Directive

CAIA Comitato per l'IA (AI Board). È l'organismo europeo di coordinamento tra Stati membri e Commissione per l'attuazione uniforme dell'AI ACT

CDFUE La Carta dei diritti fondamentali dell'Unione europea codifica in un unico testo i diritti civili, politici, economici e sociali che l'UE e i suoi Stati membri devono rispettare

Codice Privacy Il d.lgs. 196/2003, come modificato dal d.lgs. 101/2018, costituisce il quadro nazionale italiano di tutela dei dati personali

Deployer Una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale (art. 3, par. 1, n. 4 AI ACT)

GDPR Il Regolamento (UE) 2016/679 stabilisce norme uniformi per la protezione dei dati personali e la libera circolazione di tali dati all'interno del mercato unico europeo

GEPD Garante Europeo della Protezione dei Dati. È l'autorità indipendente che vigila sul trattamento dei dati personali da parte delle istituzioni e degli organi dell'UE

IA Intelligenza artificiale. Il regolamento (UE) 2024/1689 definisce "sistema di IA" «un sistema automatizzato progettato per funzionare 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» (art. 3, par. 1, n. 1 AI ACT)

EDPB Comitato Europeo per la Protezione dei Dati. Garantisce l'applicazione coerente del GDPR, adottando linee guida e decisioni vincolanti nei casi transfrontalieri

PLD Product Liability Directive

TFUE Trattato sul Funzionamento dell'Unione europea. Definisce le competenze, il funzionamento e le politiche interne dell'Unione, completando il quadro costituzionale primario

TUE Trattato sull'Unione europea. Enuncia i principi fondativi, gli obiettivi e l'architettura istituzionale dell'UE, nonché le disposizioni sul processo di integrazione

Obiettivi

Il policy paper si propone di analizzare in maniera approfondita il tema dei meccanismi di ricorso previsti dall'AI Act, valutandone i limiti e ipotizzando soluzioni normative capaci di garantire un accesso reale ed efficace alla giustizia per i cittadini. Sulla scorta di esperienze già consolidate, come quella del Regolamento generale sulla protezione dei dati (GDPR), suggeriamo la costruzione di un iter standardizzato chiaro e funzionale a garantire un esercizio pieno, effettivo e consapevole del diritto alla protezione da decisioni automatizzate. Ciò con lo scopo di rafforzare il controllo democratico sull'impiego di tecnologie ad alto impatto sociale come l'intelligenza artificiale.
Per questo motivo, in diverse parti del lavoro, si metterà a confronto il regolamento sull'intelligenza artificiale con le regole già previste dal GDPR, per individuare buone pratiche e suggerimenti utili a migliorare la tutela delle persone.

In concreto, il policy paper intende:

- esaminare le azioni che un cittadino può intraprendere in caso di violazione dei propri diritti;
- chiarire le responsabilità e i doveri delle istituzioni competenti designate a livello nazionale per garantire la corretta applicazione del regolamento;
- offrire raccomandazioni operative ai decisori pubblici per facilitare la piena attuazione delle disposizioni europee.

Executive Summary

Il policy paper, frutto della collaborazione tra Hermes Center e The Good Lobby Italia, analizza i **meccanismi di ricorso e tutela dei diritti** previsti dal **Regolamento (UE) 2024/1689, noto come AI Act**, con lo scopo di fornire una valutazione sullo stato di trasposizione in Italia e delle raccomandazioni operative.

L'obiettivo principale del documento è di identificare le lacune e le criticità dell'attuale regolamentazione e proporre soluzioni pratiche che possano facilitare a livello nazionale un **accesso più agevole ed efficace alla giustizia** per qualsiasi persona fisica o giuridica che ritenga vi sia stata una violazione della normativa .

Il ragionamento su cui si basa questo lavoro parte da un fraintendimento di fondo: inizialmente, l'AI Act era stato pensato per mettere al centro la persona, con l'obiettivo di proteggere i diritti fondamentali nell'uso dei sistemi di intelligenza artificiale. Tuttavia, nel corso del tempo, l'approccio scelto si è rivelato diverso.
La versione finale del documento normativo si basa principalmente su una valutazione del rischio, cioè su un sistema che classifica i diversi tipi di IA in base al pericolo che possono rappresentare. Questo approccio ha finito per favorire gli interessi economici e strategici delle imprese che sviluppano e usano l'IA, piuttosto che concentrarsi davvero sulla tutela dei diritti delle persone che ne subiscono gli effetti.

Questo equivoco ha provocato quella che evidenziamo come la maggiore criticità: i diritti delle persone non possono essere messi a bilancio con gli interessi delle aziende.

Basandosi sull'esperienza consolidata derivante dall'applicazione del **Regolamento Generale sulla Protezione dei Dati (GDPR)**, il paper suggerisce l'introduzione di una **procedura nazionale trasparente e standardizzata per i reclami**.

L'AI Act non contiene regole precise su come ottenere un risarcimento in caso di danni causati da un sistema di IA. In questi casi si applica un'altra normativa europea: la Direttiva (UE) 2024/2853 sulla responsabilità per i prodotti difettosi (chiamata anche PLD). Questa direttiva è stata aggiornata di recente per includere anche i prodotti digitali che usano componenti di intelligenza artificiale, come ad esempio un software che prende decisioni in modo autonomo.

Il paper sottolinea che, anche se la direttiva europea offre un primo livello di protezione, è fondamentale che ogni Stato membro – come l'Italia – adotti una normativa nazionale uniforme e chiara, che dica con precisione: chi deve rispondere dei danni (produttore, distributore, fornitore); quali prove deve portare la persona danneggiata; quali procedure seguire per ottenere il risarcimento; quali termini e tempi sono previsti per far valere i propri diritti. Una disciplina di questo tipo, applicabile a livello nazionale e coordinata con la normativa europea, rende più facile per i cittadini essere tutelati e aumenta la fiducia nell'uso dell'intelligenza artificiale.

Nella nostra analisi, ci concentriamo su alcuni elementi dell'AI Act:

- il rapporto tra la vigilanza del mercato (Art. 85) e le "autorità per i diritti fondamentali" designate (Art. 77),
- il diritto a presentare un reclamo all'autorità di vigilanza del mercato (Art. 85),
- il diritto alla spiegazione comprensibile e sostanziale dei processi decisionali automatizzati (Art. 86),
- il richiamo alla Direttiva (UE) 2019/1937 sulla protezione delle persone segnalanti, o "whistleblowers" (Art. 87)

Un elemento centrale dell'analisi è il **rapporto funzionale tra la vigilanza del mercato (ex Art. 85)** e le **"autorità per i diritti fondamentali" designate ai sensi dell'Articolo 77**. Questa interazione costituisce la **pietra angolare del sistema di responsabilità multilivello** dell'AI Act. Mentre le autorità ex Art. 85 esercitano poteri investigativi e correttivi ex post (anche su reclamo), le autorità ex Art. 77 fungono da garanti dei diritti sostanziali, avendo un diritto incondizionato di accesso alla documentazione tecnica in formati e lingue accessibili. Questo crea un "triangolo istituzionale" di controllo. È importante notare che l'Italia non ha ancora comunicato ufficialmente alla Commissione europea l'elenco delle proprie autorità ex Art. 77 entro il termine previsto del 2 novembre 2024, risultando inadempiente.

Per quanto riguarda gli **obblighi delle autorità pubbliche**, l'AI Act prevede una rete articolata di autorità nazionali dotate di poteri investigativi, correttivi e consultivi. Le autorità di vigilanza del mercato possono intervenire anche per sistemi non classificati come "ad alto rischio" se presentano un rischio per i diritti, potendo richiedere informazioni, adottare misure correttive o ordinare il ritiro del sistema dal mercato. Le violazioni possono comportare l'applicazione di **sanzioni pecuniarie significative**, che possono raggiungere fino a 35 milioni di euro o il 7% del fatturato annuo globale per le infrazioni più gravi, come l'uso di sistemi di IA vietati. Spetterà agli Stati membri stabilire in concreto l'entità delle sanzioni, che dovranno essere efficaci, proporzionate e dissuasive, ed è garantito il diritto al ricorso giurisdizionale contro tali provvedimenti.

L'AI Act (Art. 85), pur riconoscendo formalmente il diritto a presentare un reclamo all'autorità di vigilanza del mercato, omette di specificare le caratteristiche e le procedure dettagliate, rimandando genericamente ai sistemi nazionali. Questa lacuna grava sui singoli Stati membri e, a causa della potenziale diversificazione normativa tra i diversi Paesi, rischia di compromettere l'effettività delle tutele.

Il disegno di legge italiano sull'IA presenta indicazioni ancora embrionali e indeterminate in tal senso. Il GDPR pur essendo una normativa diversa e diretta a tutelare il trattamento dei dati personali, al contrario, in caso di violazione offre un sistema dettagliato per la presentazione di reclami (Art. 77 GDPR), per l'esercizio diretto dei diritti (Art. 15-22 GDPR) e per la proposizione di ricorsi giurisdizionali, incluso il diritto al risarcimento danni (Art. 82 GDPR).

Il paper si sofferma poi sul **diritto alla spiegazione comprensibile e sostanziale dei processi decisionali automatizzati (Art. 86 AI Act)**. Questo diritto si attiva quando una decisione adottata da un "deployer" basata sull'output di un sistema di IA ad alto rischio ha effetti giuridici o incide significativamente sulla salute, sicurezza o diritti fondamentali della persona. L'obiettivo è superare l'opacità dei sistemi di IA ("black box") e garantire trasparenza sulla logica algoritmica, permettendo al soggetto interessato di comprendere e contestare la decisione. Esempi concreti includono casi di danni derivanti da tecnologie biometriche o decisioni di tipo discriminatorio dovute a bias algoritmici nella selezione automatizzata di candidati.

Inoltre, l'AI Act richiama la **Direttiva (UE) 2019/1937 sulla protezione delle persone segnalanti ("whistleblowers") (Art. 87)**, aspetto cruciale per agevolare le segnalazioni di violazioni e proteggere chi denuncia comportamenti illeciti, favorendo il controllo "dal basso" soprattutto per l'IA ad alto rischio.

Infine, il policy paper propone alcune **raccomandazioni operative ai decisori pubblici** volte a colmare le lacune procedurali dell'AI Act. In particolare, suggerisce un **iter standardizzato per i reclami ispirato al GDPR**, che preveda la presentazione di reclami motivati all'autorità competente (es. ACN per l'Italia) con requisiti chiari sui dati del reclamante, la descrizione del fatto, la norma violata e la documentazione di supporto. Si raccomanda una fase istruttoria da parte dell'autorità, con possibilità di richieste di chiarimenti e perizie tecniche, e il diritto a proporre ricorso giurisdizionale contro le decisioni. L'obiettivo finale è quello di rafforzare il controllo democratico sull'impiego di tecnologie AI ad alto impatto sociale, assicurando che il loro sviluppo e utilizzo rispettino la dignità umana e mantengano al centro la persona.

Si raccomanda inoltre al Governo italiano di includere nell'elenco, tra le altre autorità, anche il Garante per la protezione dei dati personali, l'AGCOM e l'AGCM, data la loro competenza su aspetti rilevanti.

Altre raccomandazioni seguiranno in futuro, a seguito di un confronto previsto nell'autunno 2025 con diverse altre organizzazioni della società civile che si occupano di tutela dei diritti umani e dei diritti civili.

Il modello di *governance* proposto dal regolamento

Prima di entrare nel dettaglio dei meccanismi di tutela previsti in caso di violazione di una delle disposizioni dell'AI Act, occorre chiarire chi sono le autorità competenti previste nel quadro normativo. Il regolamento sull'intelligenza artificiale stabilisce un quadro di *governance* strutturato su due livelli.

Sul piano europeo, viene istituito un **Ufficio per l'Intelligenza Artificiale** presso la Commissione europea. Questo Ufficio ha principalmente un ruolo di supporto tecnico e consulenza, ma in alcuni casi ha anche poteri di controllo diretto, ad esempio quando si tratta di modelli di IA per "usi generali" (come i grandi modelli linguistici, utilizzabili in vari contesti). È previsto anche un **Consiglio europeo per l'intelligenza artificiale**, composto da un rappresentante per ciascuno Stato membro, che fornisce orientamenti e raccomandazioni e favorisce il coordinamento tra i Paesi. Al suo interno, partecipano come osservatori anche l'Ufficio IA e il Garante europeo della protezione dei dati (EDPS).

Ogni Paese poi dovrà designare almeno due tipi di autorità: un'**autorità di notifica**, incaricata dei controlli iniziali sugli strumenti di IA, e un'autorità **di vigilanza**, incaricata delle verifiche successive all'immissione del sistema sul mercato.

In Italia, il disegno di legge nazionale sull'intelligenza artificiale ha previsto che questi compiti vengano svolti da due enti pubblici già esistenti: AgID e ACN.

L'**AgID** si occupa di promuovere lo sviluppo dell'IA e di supervisionare la fase iniziale, cioè quella in cui il produttore del sistema IA deve notificare il prodotto e dimostrare che rispetti i requisiti tecnici e giuridici stabiliti dal regolamento europeo. L'AgID si occupa quindi di valutare, approvare e accreditare gli enti che certificheranno i sistemi di IA, assicurandosi che rispettino tutti gli standard richiesti.

L'**ACN**, invece, ha il compito di controllare che l'uso dei sistemi di IA in Italia non comporti rischi per la sicurezza informatica o per i diritti delle persone. Può condurre ispezioni, intervenire in caso di reclami per violazione delle disposizioni del regolamento e infliggere sanzioni. In più, promuove la ricerca e lo sviluppo nel campo della cybersicurezza applicata all'intelligenza artificiale, per evitare che questi strumenti vengano manipolati o utilizzati in modo improprio.

Presso la Presidenza del Consiglio dei ministri è istituito poi un Comitato di coordinamento, composto dai direttori generali dell'AgID e dell'ACN e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri. Il Comitato ha il compito di assicurare il coordinamento e la collaborazione tra le Autorità nazionali per l'intelligenza artificiale e le altre pubbliche amministrazioni e autorità indipendenti. Infine, restano ferme le competenze, i compiti e i poteri del Garante per la protezione dei dati personali.
Nel corso del documento verrà spiegato in modo più chiaro come funzionano i rapporti tra le diverse autorità previste a livello nazionale, e quali saranno i compiti che ciascuna di esse svolgerà nella pratica.

Obblighi e tutele per i cittadini

Cosa può fare l'interessato in caso di violazione di disposizioni dell'AI Act

Chiunque, persona fisica o giuridica, ritenga che vi sia stata una violazione delle disposizioni del regolamento, ha il diritto di presentare un **RECLAMO MOTIVATO** all'autorità nazionale di vigilanza del mercato competente. È inoltre garantito l'accesso a un **RICORSO GIURISDIZIONALE** contro decisioni (o inerzie) dell'autorità di controllo[4].

Ipotizziamo ad esempio il caso di una società operante nel settore della logistica, che acquisisce e utilizza un sistema di ottimizzazione dei flussi di magazzino alimentato da un algoritmo di intelligenza artificiale. Il sistema è classificabile come "sistema di IA ad alto rischio" ai sensi dell'Allegato III del regolamento europeo: ciò perché incide direttamente sulla sicurezza e sulla salute dei lavoratori, regolando i tempi e i ritmi di carico-scarico attraverso sensori biometrici e strumenti di tracciamento ambientale.
Nel corso dell'utilizzo, l'azienda rileva malfunzionamenti significativi del sistema, che produce ordini di movimentazione contraddittori e, in alcuni casi, incompatibili con le norme di sicurezza sul lavoro. L'impresa, dopo aver richiesto chiarimenti al fornitore senza ricevere adeguata documentazione circa la conformità del sistema al regolamento e senza evidenza di alcuna valutazione del rischio aggiornata[5], decide di presentare un reclamo all'autorità nazionale di vigilanza del mercato.

4 Vedi *considerando 170*

5 Ai sensi degli articoli 6 e seguenti del regolamento AI Act, infatti, occorre che siano rispettati una serie di requisiti per la fornitura di sistemi di IA ad alto rischio

L’articolo 85 dell’AI Act stabilisce infatti che:

> *Fatti salvi altri ricorsi amministrativi o giurisdizionali, qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni del presente regolamento può presentare un reclamo alla pertinente autorità di vigilanza del mercato. Conformemente al regolamento (UE) 2019/1020, tali reclami sono presi in considerazione ai fini dello svolgimento delle attività di vigilanza del mercato e sono trattati in linea con le procedure specifiche stabilite a tal fine dalle autorità di vigilanza del mercato.*

In altre parole, il regolamento dice che, se una persona fisica o un ente pensa che siano stati violati i propri diritti o che il sistema di intelligenza artificiale non sia conforme alla legge, può presentare un reclamo all’autorità nazionale di vigilanza del mercato. Questa autorità ha il compito di controllare che i sistemi di IA immessi sul mercato rispettino le regole europee. Più nel dettaglio, ricevuto il reclamo, l’autorità dovrà esaminare il caso e decidere se avviare un’indagine o intervenire in altro modo, secondo le sue procedure interne.
Peraltro, ciò non esclude la possibilità di ricorrere anche ad altri strumenti giuridici, come un’azione davanti a un giudice ordinario. Questo significa che l’interessato ha una doppia possibilità di tutela, e potrà scegliere quale strada percorrere in base al tipo di problema e agli effetti subiti.

Ad esempio, se una persona è stata direttamente danneggiata da un errore del sistema di IA (come un danno economico o reputazionale), e vuole ottenere un risarcimento, sarà più opportuno rivolgersi al giudice civile, perché solo quest’ultimo può condannare al pagamento di un indennizzo. Se invece la preoccupazione riguarda il malfunzionamento di un prodotto sul mercato o l’uso improprio di una tecnologia da parte di un’azienda, e si vuole sollecitare un controllo pubblico o il ritiro del prodotto, sarà più utile presentare un reclamo all’autorità di vigilanza del mercato, affinché intervenga sul produttore o sul fornitore.

La norma, quindi, lascia aperte più strade e consente di modulare la reazione legale in base alla gravità del danno, alla natura del soggetto coinvolto, e alle finalità perseguite (correttive, sanzionatorie o risarcitorie).

Tuttavia, le regole pratiche – come a chi rivolgersi, quali documenti presentare, entro quali tempi – non sono ancora stabilite in modo chiaro, e ogni Paese dell'Unione europea potrà decidere in modo diverso. Come detto, al momento in Italia, non esiste ancora una procedura precisa che dica cosa deve fare concretamente una persona (fisica o giuridica) per fare un reclamo contro l'uso scorretto di un sistema di intelligenza artificiale.
Per aiutare a capire meglio questa situazione, può essere utile fare un confronto pratico con un altro regolamento europeo già noto e applicato da anni: quello sulla protezione dei dati personali (il GDPR). In quest'ultimo caso, le regole per fare un reclamo sono chiare: esistono moduli specifici, autorità ben identificate (come l'Autorità Garante per la protezione dei dati personali) e tempi stabiliti per ricevere una risposta.

In particolare, gli strumenti per difendere i propri diritti in caso di violazioni del trattamento dei dati personali sono previsti sia dal Codice Privacy italiano (cioè il decreto legislativo 196 del 2003, aggiornato nel 2018), sia dal GDPR. Se una persona pensa che i propri dati siano stati usati in modo non conforme alla normativa, ha il diritto di presentare un reclamo al Garante per la protezione dei dati personali. Il Garante può avviare un'indagine per verificare se c'è stata una violazione delle regole e prendere eventualmente dei provvedimenti.
Questa possibilità è prevista sia dall'articolo 77 del GDPR, sia da alcuni articoli specifici del Codice Privacy italiano (in particolare gli articoli da 140-bis a 143), che servono proprio ad adattare la legge italiana al regolamento europeo.

	AI Act (Reg. UE 2024/1689)	GDPR (Reg. UE 2016/679 + Codice Privacy)
CHI PUÒ PRESENTARE IL RECLAMO	Qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione	Qualsiasi persona fisica interessata
A CHI SI PRESENTA IL RECLAMO	Autorità di vigilanza del mercato nazionale	Garante per la protezione dei dati personali
NORME DI RIFERIMENTO	Art. 85 AI Act + Reg. (UE) 2019/1020	Art. 77 GDPR + Artt. 140-bis – 143 Codice Privacy
FINALITÀ DEL RECLAMO	Attivare le attività di vigilanza del mercato e segnalare possibili violazioni	Segnalare una violazione della normativa sulla protezione dei dati e ottenere una verifica dell'Autorità

1 COME SI PRESENTA IL RECLAMO AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI?

In questo caso la normativa di riferimento è:

- l'articolo 77 GDPR
- l'articolo 141 e seguenti del Codice Privacy

Chi può farlo?

Qualsiasi persona che ritenga che il trattamento dei dati personali che la riguardano violi il GDPR. Il reclamo può essere sottoscritto direttamente dall'interessato oppure, per suo conto, da un avvocato, un procuratore, un organismo, un'organizzazione o un'associazione. In tali casi, è necessario conferire una procura da depositarsi presso il Garante assieme a tutta la documentazione utile ai fini della valutazione del reclamo presentato.

A chi ci si rivolge?

Al Garante per la protezione dei dati personali, autorità nazionale indipendente.

Il reclamante potrà far pervenire l'atto utilizzando la modalità ritenuta più opportuna:

a) messaggio di posta elettronica certificata indirizzata a: protocollo@pec.gpdp.it
b) raccomandata A/R indirizzata al: Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 Roma
c) consegna a mano presso gli uffici del Garante per la protezione dei dati personali, Piazza Venezia, 11 - Roma

Il reclamo e l'eventuale procura dovranno essere sottoscritti con firma autenticata, ovvero con firma digitale, ovvero con firma autografa (in tale ultimo caso, al reclamo dovrà essere allegata copia di un documento di riconoscimento dell'interessato/a in corso di validità).

2 ESERCIZIO DIRETTO DEI DIRITTI NEI CONFRONTI DEL TITOLARE DEL TRATTAMENTO

Normativa di riferimento:
Articoli 15-22 GDPR

Quali diritti si possono esercitare?

- Diritto di accesso
- Diritto alla rettifica
- Diritto alla cancellazione ("diritto all'oblio")
- Diritto alla limitazione del trattamento
- Diritto alla portabilità dei dati
- Diritto di opposizione
- Diritto di non essere sottoposto a decisioni automatizzate

Come si esercitano?

Inviando una richiesta scritta al titolare del trattamento (email, PEC, raccomandata A/R).

Il titolare deve rispondere entro un mese, eventualmente prorogabile di due mesi in casi complessi.

3 PROPORRE RICORSO GIURISDIZIONALE

Normativa di riferimento:
- Art. 78 e 79 GDPR
- Art. 152 Codice Privacy

In quali casi?
- Se non si è soddisfatti dell'esito del reclamo presso il Garante
- Se si vuole agire direttamente per ottenere un risarcimento o per ottenere un provvedimento del giudice

A chi ci si rivolge?
- Tribunale ordinario competente per territorio
- Anche senza aver prima presentato reclamo al Garante

4 RICHIEDERE IL RISARCIMENTO DEL DANNO

Normativa di riferimento:
Art. 82 GDPR

Il soggetto danneggiato ha diritto a ottenere un risarcimento dal titolare o dal responsabile del trattamento, qualora subisca danni materiali o immateriali a causa di una violazione del GDPR.

… e in caso di danno derivante dall'uso di un sistema di IA?

A differenza del GDPR, che prevede un articolato sistema di tutela anche risarcitoria in caso di violazione del diritto alla protezione dei dati personali, il regolamento sull'intelligenza artificiale non contempla una disciplina *ad hoc* volta a regolare il risarcimento dei danni causati da sistemi di IA.

In origine, si pensava di colmare questa mancanza con una direttiva specifica – la cosiddetta Direttiva sulla responsabilità da intelligenza artificiale (*Artificial Intelligence Liability Directive*, AILD) – pensata per uniformare le regole sulla responsabilità civile applicabili ai sistemi di IA nei vari Stati membri. Tuttavia, la Commissione europea ha recentemente deciso di ritirare la proposta, a causa della mancanza di un accordo politico tra i Paesi e per la forte pressione in tal senso dell'amministrazione statunitense[6].

In mancanza di una normativa specifica e uniforme, oggi si fa riferimento alle regole contenute nella recente direttiva (UE) 2024/2853 sulla responsabilità per i prodotti difettosi (la nuova *Product Liability Directive* o PLD). Gli Stati membri, inclusa l'Italia, hanno tempo fino al 2026 per recepirla nel proprio ordinamento.

Questa direttiva amplia in modo esplicito il proprio campo di applicazione anche ai prodotti digitali, inclusi quelli che integrano componenti di

6 *https://www.ansa.it/europa/notizie/rubriche/altrenews/2025/02/12/la-commissione-ue-ritira-la-direttiva-sulla-responsabilita-da-intelligenza-artificiale_d929ebe1-e344-415f-ae82-c49dda2fd230.html*

intelligenza artificiale, e introduce un'importante novità: rende infatti più semplice per chi subisce un danno dimostrare la responsabilità, alleggerendo il cosiddetto onere della prova[7]. Parallelamente, restano in vigore le norme generali sulla responsabilità extracontrattuale previste dai singoli ordinamenti nazionali.

Il risultato attuale è un quadro normativo frammentato e ancora in fase di definizione, che mette in evidenza la necessità di un intervento a livello europeo capace di armonizzare le regole, e che servirebbe a garantire maggiore certezza giuridica, una tutela effettiva per chi subisce danni e una chiara responsabilità per chi sviluppa e immette sul mercato tecnologie basate sull'intelligenza artificiale.

7 L'onere della prova è il principio secondo cui spetta alla parte che afferma un fatto fornire le prove necessarie a dimostrarlo. In ambito di responsabilità civile, ciò significa che chi subisce un danno deve dimostrare l'esistenza del danno, il nesso causale che lega il comportamento tenuto al danno subito e la responsabilità del soggetto accusato.

Cosa può fare l'interessato a fronte di un processo decisionale automatizzato?

Nel quadro delle garanzie previste dal regolamento sull'intelligenza artificiale, la tutela degli individui non può esaurirsi nel solo esercizio del diritto di proporre reclamo. Essa trova un rafforzamento significativo nell'articolo 86, il quale introduce un ulteriore presidio di garanzia: il **DIRITTO A OTTENERE UNA SPIEGAZIONE COMPRENSIBILE E SOSTANZIALE DEI PROCESSI DECISIONALI** adottati dai cosiddetti *deployers* qualora questi ultimi abbiano basato la propria decisione sugli *output* generati da sistemi di IA ad alto rischio. Tale diritto si attiva allorché la decisione incida, in modo giuridicamente rilevante o con effetti equivalenti, sulla persona interessata, pregiudicandone la salute, la sicurezza o i diritti fondamentali.

DEPLOYER
Una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale (art. 3, par. 1, n. 4 AI ACT)

In una prospettiva orientata alla tutela della persona, la previsione di una "spiegazione chiara e significativa" si configura come uno strumento di trasparenza, volto a svelare il contenuto e la logica sottesa alle operazioni algoritmiche che condizionano l'esito del processo decisionale automatizzato. Tale misura consente non solo una valutazione critica dell'affidabilità e della correttezza del risultato ottenuto dal sistema, ma garantisce altresì che la persona possa effettivamente comprendere le ragioni della decisione subita

e, conseguentemente, esercitare in modo informato e consapevole i propri diritti procedimentali e sostanziali.

La norma nasce dall'esigenza di colmare il divario tra la complessità tecnica dei sistemi di intelligenza artificiale – spesso caratterizzati da una struttura opaca e difficile da comprendere secondo logiche lineari (le cosiddette *black box*) – e il diritto alla trasparenza degli algoritmi. L'articolo 86 prevede però delle eccezioni: se il diritto nazionale o quello europeo stabilisce che, in certi contesti (per esempio per motivi di sicurezza nazionale), non è obbligatorio fornire tutte queste informazioni, allora questo diritto alla spiegazione può essere limitato.

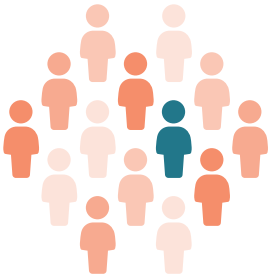
Caso 1

Si pensi al caso di un grande centro commerciale dove è installato un sistema di riconoscimento facciale all'ingresso per "motivi di sicurezza". Questo sistema confronta i volti dei visitatori con un database interno che include persone ritenute "pericolose", ad esempio soggetti che in passato avrebbero avuto comportamenti scorretti (anche solo sospetti) nei negozi del gruppo. Un giorno, un cliente abituale viene fermato alla porta e gli viene impedito di entrare. Il personale afferma che il sistema di intelligenza artificiale ha identificato il suo volto come appartenente a una persona presente nel database. Al cliente non viene però spiegato il motivo del blocco, né viene data la possibilità immediata di contestare la decisione.

Secondo il regolamento, se una persona subisce un trattamento ingiusto – ad esempio il divieto di accesso a un luogo pubblico – sulla base del risultato di un sistema di intelligenza artificiale ad alto rischio, ha diritto a una spiegazione chiara e comprensibile. Il soggetto che ha utilizzato il sistema deve quindi chiarire:

1) che ruolo ha avuto il sistema di IA nel prendere quella decisione;
2) quali criteri sono stati usati;
3) quali dati sono stati analizzati;
4) se c'è stato un errore nel riconoscimento.

IL CLIENTE POTREBBE DUNQUE CHIEDERE SPIEGAZIONI FORMALI SULL'USO DEL SISTEMA E SUL MOTIVO PER CUI È STATO BLOCCATO; PRESENTARE UN RECLAMO ALL'AUTORITÀ NAZIONALE DI VIGILANZA SUL MERCATO CONTESTANDO L'USO IMPROPRIO DEL RICONOSCIMENTO FACCIALE; AVVIARE UN'AZIONE LEGALE, SE RITIENE CHE LA DECISIONE GLI ABBIA CAUSATO UN DANNO.



Caso 2

Si immagini ora il caso di una decisione automatizzata di tipo discriminatorio, generata da un sistema di intelligenza artificiale affetto da *bias* algoritmico. Ciò potrebbe avvenire, ad esempio, durante la selezione automatica di candidati per un impiego pubblico o nell'accesso a servizi essenziali, in cui il sistema potrebbe discriminare per identità di genere o per provenienza etnica. Se, in casi simili, non è stato garantito all'interessato il diritto a ricevere una spiegazione chiara e comprensibile su come il sistema abbia preso quella decisione, sarà possibile presentare un reclamo all'autorità di controllo.

SE LA PROCEDURA NON PORTA AI RISULTATI SPERATI, L'INTERESSATO POTRÀ AGIRE IN SEDE CIVILE PER OTTENERE UN RISARCIMENTO DEL DANNO SUBITO. A OGGI, QUESTA RICHIESTA PUÒ BASARSI SIA SULLE REGOLE GENERALI DI RESPONSABILITÀ CIVILE PREVISTE DAL DIRITTO NAZIONALE, SIA – UNA VOLTA RECEPITA INTERNAMENTE – SULLE NUOVE NORME PREVISTE DALLA DIRETTIVA EUROPEA SULLA RESPONSABILITÀ PER DANNI DA PRODOTTI DIFETTOSI (LA COSIDDETTA *PRODUCT LIABILITY DIRECTIVE O PLD*).

Le segnalazioni di violazioni e la normativa di riferimento a tutela del *whistleblower*

Nella parte del regolamento dedicata ai mezzi di ricorso, l'articolo 87 richiama espressamente la direttiva (UE) 2019/1937, che stabilisce le regole per la segnalazione di eventuali violazioni e tutela le persone che decidono di segnalarle (*whistleblowers*). Questa normativa mira a garantire protezione a chi, agendo in buona fede, porta alla luce delle violazioni di disposizioni normative nazionali o dell'Unione europea (illeciti civili, amministrativi, condotte illecite ai sensi del d.lgs. 231/2001, illeciti penali e contabili) che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui è venuta a conoscenza in un contesto lavorativo pubblico o privato.

Il richiamo alla direttiva sul *whistleblowing* risponde all'esigenza di garantire a chiunque venga a conoscenza di violazioni del Regolamento AI – compresi funzionari pubblici, dipendenti di imprese o soggetti incaricati di attività tecniche – di segnalarle in anonimato e senza timore di ritorsioni. Ciò può rivelarsi fondamentale in particolare nel contesto dell'IA ad alto rischio, dove errori o abusi possono produrre gravi conseguenze su diritti e libertà fondamentali.

Il regolamento richiama la direttiva per:

- Agevolare le segnalazioni di violazioni del regolamento da parte di soggetti interni a organizzazioni che sviluppano, distribuiscono o utilizzano sistemi di IA.
- Proteggere il segnalante quando denuncia comportamenti illeciti, come l'impiego non autorizzato di IA ad alto rischio o l'omessa valutazione di conformità.
- Favorire il controllo dal basso del rispetto dei diritti fondamentali, anche in assenza di vigilanza formale da parte delle autorità preposte.

Obblighi dell'autorità di vigilanza in caso di violazione di disposizioni del regolamento

Uno dei principali obiettivi dichiarati dell'AI Act è quello di assicurare l'effettività dei diritti riconosciuti agli interessati e garantire un'efficace tutela rispetto agli effetti potenzialmente lesivi derivanti dall'impiego di sistemi di intelligenza artificiale.

Come anticipato, a livello nazionale, il ruolo centrale è affidato alle **autorità di vigilanza** designate dagli Stati membri, che devono essere dotate di poteri investigativi, correttivi e consultivi. Tali autorità saranno competenti a ricevere i reclami da parte dei soggetti interessati e ad adottare provvedimenti nei confronti di operatori economici o autorità pubbliche che impieghino sistemi di IA in violazione del Regolamento.

L'articolo 74 dell'AI Act, facendo esplicito rinvio al sistema previsto dal regolamento (UE) 2019/1020 sulla vigilanza del mercato e la conformità dei prodotti, disciplina i poteri specifici dell'autorità di vigilanza, la cui competenza in Italia sarà rivestita da ACN.

In particolare, l'autorità riveste diverse funzioni:

1. **FUNZIONE DI SUPPORTO E CONSULENZA**:
le autorità offrono orientamenti sull'attuazione del regolamento, in particolare alle piccole medie imprese (e startup), tenendo conto

– se del caso – degli orientamenti e della consulenza del Comitato scientifico e della Commissione.

2. **FUNZIONE DI VIGILANZA**:
le autorità di vigilanza del mercato potranno intervenire ogni volta ritengano che un sistema presenti un rischio per i diritti. In questi casi, possono chiedere ai fornitori informazioni e accedere alla documentazione tecnica, sollecitare l'adozione di misure correttive e ordinare il ritiro del sistema dal mercato, se non conforme.

In base all'articolo 73 dell'AI Act, le autorità possono agire di propria iniziativa oppure a seguito di segnalazioni, in particolare in caso di "gravi incidenti" notificati dai fornitori di IA.

Immaginiamo che in una città italiana sia stato adottato un sistema di intelligenza artificiale per analizzare automaticamente le chiamate al numero unico di emergenza. Il sistema serve per classificare le chiamate ricevute (urgenti e meno urgenti) e capire quali interventi inviare per primi: ambulanza, polizia o vigili del fuoco. Durante una giornata particolarmente caotica, il sistema classifica per errore una chiamata urgente come non prioritaria. Il paziente subisce danni gravi a causa di questo ritardo.
In questo caso:

1) il fornitore del sistema, appena viene a conoscenza dell'incidente e del possibile collegamento con l'errore del sistema IA, deve segnalarlo entro massimo 15 giorni (o meno, vista la gravità).

2) L'autorità nazionale (es. ACN in Italia) riceve la segnalazione e può intervenire: ritirare il software, aprire un'indagine e avvisare la Commissione europea.

3) Se il sistema è stato usato anche in altri Paesi, potrebbero partire indagini coordinate a livello europeo.

Sanzioni e misure esecutive

Qualora le misure correttive citate non siano sufficienti, l'articolo 99 dell'AI Act prevede che le autorità di vigilanza possano infliggere sanzioni pecuniarie e adottare misure di esecuzione, inclusi avvertimenti e misure di natura non pecuniaria (non meglio definite dal regolamento, la cui disciplina è lasciata alla normativa nazionale).

Il regolamento è invece più stringente rispetto alle sanzioni pecuniarie.

VIOLAZIONE	Sanzioni Pecuniarie (Euro)	Percentuale del Fatturato
USO DI SISTEMI DI IA VIETATI	Fino a 35 milioni di euro	Fino al 7% del fatturato annuo globale
VIOLAZIONE DEGLI OBBLIGHI GENERALI DEL REGOLAMENTO	Fino a 15 milioni di euro	Fino al 3% del fatturato
TRASMISSIONE DI INFORMAZIONI ERRATE	Fino a 7,5 milioni di euro	Fino all'1 % del fatturato

Spetterà agli Stati membri stabilire in concreto l'entità delle sanzioni, che dovranno essere efficaci, proporzionate e dissuasive (comprese le sanzioni amministrative), e comunicarle alla Commissione. In aggiunta, spetterà sempre agli Stati membri definire se e come tali sanzioni potranno essere inflitte anche alle autorità pubbliche e a organismi pubblici nazionali in caso di violazione dell'AI Act.

Garanzie procedurali e autonomia nazionale

L'esercizio dei poteri sanzionatori da parte dell'autorità di vigilanza dovrà essere soggetto alle garanzie procedurali previste dal diritto dell'Unione e da quello nazionale, incluso il diritto al ricorso giurisdizionale. Ne deriva dunque che i provvedimenti adottati dalle autorità di vigilanza potranno essere sottoposti alla valutazione delle Corti nazionali (e, nel caso, della Corte di giustizia tramite un rinvio pregiudiziale[8]).

8 Il rinvio pregiudiziale è uno strumento previsto dal diritto dell'Unione Europea che permette ai giudici nazionali di chiedere chiarimenti alla Corte di giustizia dell'Unione Europea (CGUE) su come interpretare o applicare una norma europea. Quando un giudice in uno Stato membro dell'UE si trova davanti a una legge europea che non è chiara, o ha dei dubbi su come usarla in un caso concreto, può "sospendere" il procedimento e fare una domanda alla Corte UE. La Corte risponde con una sentenza interpretativa che chiarisce il significato della norma europea. Dopo la risposta, il giudice nazionale riprende il processo e decide il caso tenendo conto della spiegazione fonita dalla Corte di giustizia.

Inoltre, è importante precisare che la funzione sanzionatoria non è demandata in via esclusiva alle autorità di vigilanza che dovranno controllare sulla corretta applicazione del regolamento. Infatti, il paragrafo 9 dell'art. 99 lascia liberi gli Stati di prevedere che le sanzioni pecuniarie siano inflitte dai tribunali nazionali competenti o da altri organismi, secondo il proprio ordinamento giuridico nazionale. Dunque, in linea con l'autonomia procedurale degli Stati membri, non solo la dimensione organizzativa delle autorità di vigilanza ma anche la distribuzione dei poteri rispetto all'imposizione di eventuali sanzioni in caso di violazioni dell'AI Act si configura sotto un profilo scarsamente armonizzato a livello sovranazionale, se non rispetto a dei criteri minimi, e sostanzialmente affidato alle normative nazionali.

Rapporti tra le autorità e gli organismi pubblici nazionali coinvolti

Nel regolamento europeo sull'intelligenza artificiale, oltre all'**autorità di notifica** (che si occupa della fase iniziale di conformità dei sistemi di IA) e all'**autorità di vigilanza** (che sorveglia i sistemi già in uso), è previsto un ruolo diverso per altri enti pubblici o autorità che hanno il compito specifico di tutelare i diritti fondamentali delle persone. Secondo l'articolo 77, questi enti hanno il diritto di chiedere – in modo chiaro, accessibile e nella lingua necessaria – tutti i documenti e le informazioni relativi al funzionamento dei sistemi di intelligenza artificiale, se lo ritengono necessario per verificare se i diritti delle persone siano stati rispettati.

Ogni Stato membro dell'Unione Europea deve individuare queste autorità e comunicarne l'elenco alla Commissione europea, così che sia noto a livello europeo.

L'autorità prevista dall'articolo 77 assume dunque il ruolo di garante sostanziale dei diritti: se la documentazione fornita è incompleta o poco chiara, può chiedere all'autorità di vigilanza del mercato di svolgere ulteriori verifiche tecniche sul sistema di IA. Si attiva così un meccanismo di controllo che integra la sorveglianza prevista dall'articolo 85 – che riconosce a chiunque il diritto di segnalare una violazione – con il ruolo terzo dell'autorità di notifica, responsabile della designazione e del controllo degli organismi che valutano la conformità dei sistemi.

Il risultato è un triangolo istituzionale: l'autorità di notifica garantisce la solidità preventiva (*ex ante*) del sistema di certificazione; l'autorità di vigilanza assicura la sorveglianza (*ex post*) e tutela le persone attraverso il diritto al reclamo; l'autorità ex articolo 77 vigila sulla compatibilità dei sistemi di IA con la Carta dei diritti fondamentali, potendo accedere, condividere e, se necessario, trasferire evidenze alle altre due articolazioni per l'adozione di misure correttive o sanzionatorie.

L'Italia, a oggi, non ha ancora trasmesso alla Commissione europea la lista ufficiale delle autorità ex articolo 77. Secondo gli aggiornamenti diffusi dalla Commissione e riportati dalla stampa specializzata, risulta inadempiente insieme all'Ungheria. Attualmente, la designazione del Garante per la protezione dei dati personali per i sistemi di IA indicati nell'allegato III, punti I, 6, 7 e 8, così come il possibile coinvolgimento di altre autorità settoriali quali AGCOM e AGCM, è ancora in fase di proposta. Manca ancora la formale notificazione alla Commissione.

Raccomandazioni

LE SEGUENTI RACCOMANDAZIONI SONO STATE IDENTIFICATE A SEGUITO DI UN CONFRONTO CON LE ORGANIZZAZIONI ADERENTI ALLA RETE PER DIRITTI UMANI DIGITALI (RDUD), DURANTE UN WORKSHOP TENUTOSI A MILANO IL 14 OTTOBRE 2025.

1 Definizione di tempistiche procedimentali ex art. 85

Introdurre (i) termini per ACN: dai 5 ai 10 giorni per protocollazione e competenza, 30 giorni per valutazione preliminare (ammissibilità), 60 giorni per decisione sul merito o adozione di misure interinali.

In caso di mancata risposta oltre i termini prevedere un meccanismo di ricorso interno al Responsabile della Trasparenza entro 15 giorni per definire o motivare la proroga.

In caso di mancata risposta da parte del Responsabile della Trasparenza entro i 15 giorni stabiliti, prevedere la possibilità di ricorso per silenzio-inadempimento al giudice amministrativo e un meccanismo di segnalazione al difensore civico/organismo di vigilanza superiore, ove previsto.

2 Alternativa tra reclamo ad ACN e ricorso al giudice (art. 85 AI Act): chiarezza e coordinamento

Esplicitare in quali casi è possibile procedere con il reclamo ex art. 85 AI Act e in quali casi è possibile esperire ricorso diretto al giudice; Prevedere meccanismi di coordinamento per evitare conflitti/duplicazioni procedimentali.

3 Motivazione obbligatoria e "rafforzata" dei provvedimenti ACN

Rendere la motivazione dei provvedimenti un requisito obbligatorio, includendo: (a) ricostruzione tecnico-organizzativa della catena socio-tecnica (modelli, dataset, controlli interni); (b) inquadramento normativo (AI Act, GDPR, lex specialis settoriale).

Proposta di implementazione: definizione del decisore pubblico di un template standard con sezioni fisse e allegati tecnici.

4 Registro pubblico dei casi: anonimizzato, aperto, interoperabile

Istituire un archivio dei procedimenti definiti centralizzato, in formato aperto, anonimizzato, aggiornato con cadenza almeno trimestrale.

5 Reindirizzamento di competenza tra le Autorità

Se il reclamo ex art. 85 AI Act è presentato ad un'autorità incompetente, l'autorità ricevente ha l'obbligo di trasferimento d'ufficio entro 5 giorni lavorativi all'Autorità competente, con notifica di avvenuto inoltro al l'istante.

6 Procedura per decisioni automatizzate ex art. 86 (in coordinamento con art. 22 GDPR e 11 LED)

Chiarire che, in presenza di decisione unicamente automatizzata o con effetti giuridici/analoghi significativi, l'istante può intraprendere diverse

strade: (i) proporre reclamo ex art. 85 AI Act; (ii) esercitare i diritti ex artt. 22 GDPR e 11 LED (intervento umano).

7 Eccezioni all'art. 86: tassonomia, test e garanzie

Codificare in linee guida vincolanti le deroghe previste dal paragrafo 2 dell'art. 86 AI Act (es. obblighi legali, sicurezza pubblica, esigenze investigative), subordinandole a test di necessità e proporzionalità, valutazioni d'impatto e garanzie compensative (audit ex post, limitazioni temporali).

8 Risarcimento del danno da sistemi di IA: iter coordinato

Definire la procedura da seguire per chiedere il risarcimento del danno derivante da sistema di IA, prevedendo ove possibile meccanismi stragiudiziali.

9 Alternativa tra reclamo ad ACN e ricorso al giudice (art. 85 AI Act): chiarezza e coordinamento

Esplicitare in quali casi è possibile procedere con il reclamo ex art. 85 AI Act e in quali casi è possibile esperire ricorso diretto al giudice; Prevedere meccanismi di coordinamento per evitare conflitti/duplicazioni procedimentali.

10 Unità settoriali specializzate in ACN

Istituire unità verticali per domini ad alto rischio (sanità, assicurazioni/finanza, PA/servizi amministrativi, lavoro/HR, istruzione, infrastrutture critiche), con team interdisciplinari composti da giuristi, data scientist, ingegneri sicurezza, ethicist, ecc.

11 Definire l'elenco delle Autorità ex art. 77 AI ACT

Si propone di individuare le seguenti istituzioni tra le autorità che tutelano i diritti fondamentali previste dall'articolo 77 dell'AI ACT:

- Garante per la protezione dei dati personali (GPDP)
- Garante nazionale dei diritti delle persone private della libertà personale (GNPL)
- Autorità per le garanzie nelle comunicazioni (AGCOM)
- Commissione di garanzia per l'attuazione della legge sullo sciopero nei servizi pubblici essenziali (CGS)
- Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (IVASS – ex ISVAP)
- Autorità garante per l'infanzia e l'adolescenza (AGIA)
- Autorità Garante nazionale dei diritti delle persone con disabilità (AGDPD)
- Ufficio Nazionale Antidiscriminazioni Razziali (UNAR)
- Ispettorato Nazionale del Lavoro (INL)

12 Definizione procedimento reclamo ex art. 85 AI Act

Fase di proposizione

Dati del reclamante
Nome, cognome, residenza/domicilio, eventuale rappresentanza

Descrizione del fatto
Dinamica dell'accaduto: natura del sistema IA, soggetto che lo ha impiegato, contesto e modalità

Norma violata
Riferimento agli articoli del Reg. 2024/1689 che si ritengono violati (es. artt. 5, 9, 13, 26)

Documentazione a supporto
Screenshot, notifiche, informative ricevute, eventuali danni subiti

Richiesta Provvedimenti attesi

Interruzione del trattamento, accertamento della violazione, sanzione, ecc.

La presentazione dovrebbe essere telematica, con modello standardizzato, tramite PEC o piattaforma dedicata.

Fase istruttoria (accertamenti dell'ACN)

Una volta ricevuto il reclamo e protocollato (5-10 giorni), l'ACN dovrebbe entro 30 giorni:

- verificare l'ammissibilità formale (presenza dei requisiti, legittimazione attiva);
- avviare una fase istruttoria, eventualmente richiedendo chiarimenti all'operatore IA coinvolto (fornitore o utilizzatore);
- acquisire eventuali perizie tecniche sui sistemi coinvolti (anche con il supporto del Comitato europeo sull'intelligenza artificiale).

Esito dell'accertamento e adozione di misure

Se la violazione è accertata, ACN:

- Può ordinare la cessazione dell'uso del sistema.
- Può imporre modifiche tecniche o l'interruzione temporanea.
- Può comminare sanzioni pecuniarie.
- Il provvedimento è motivato.

Contro la decisione dell'ACN (sia in caso di accoglimento parziale che di rigetto), chiarire se il cittadino potrà in ogni caso proporre ricorso giurisdizionale dinanzi al giudice competente.

Nei casi gravi o transfrontalieri, l'ACN dovrebbe informare il Board europeo per l'intelligenza artificiale (EAB) e, se necessario, la Commissione.

HERMES
HACKING FOR HUMAN RIGHTS

Hermes Center è un'associazione nata nel 2012 che crede in una società in cui la tecnologia non costituisca una minaccia, ma una risorsa preziosa in grado di garantire la sicurezza degli utenti e rispettarne il diritto alla privacy e alla libertà di espressione. Attraverso le nostre iniziative, promuoviamo la consapevolezza circa i pericoli legati all'utilizzo degli strumenti informatici.

THE good LOBBY

The Good Lobby è un'organizzazione non profit impegnata a rendere più democratico l'accesso al potere. Contribuiamo a rafforzare le capacità della società civile di agire nella sfera politica e di inserirsi nei processi decisionali, portando la voce degli interessi collettivi. Promuoviamo inoltre leggi, regolamenti e pratiche capaci di difendere i valori democratici e lo stato di diritto.