

## DECISIONI AUTOMATIZZATE

# Chi è responsabile se decide un algoritmo? Il diritto cerca risposte

Home > Sicurezza Digitale > Privacy



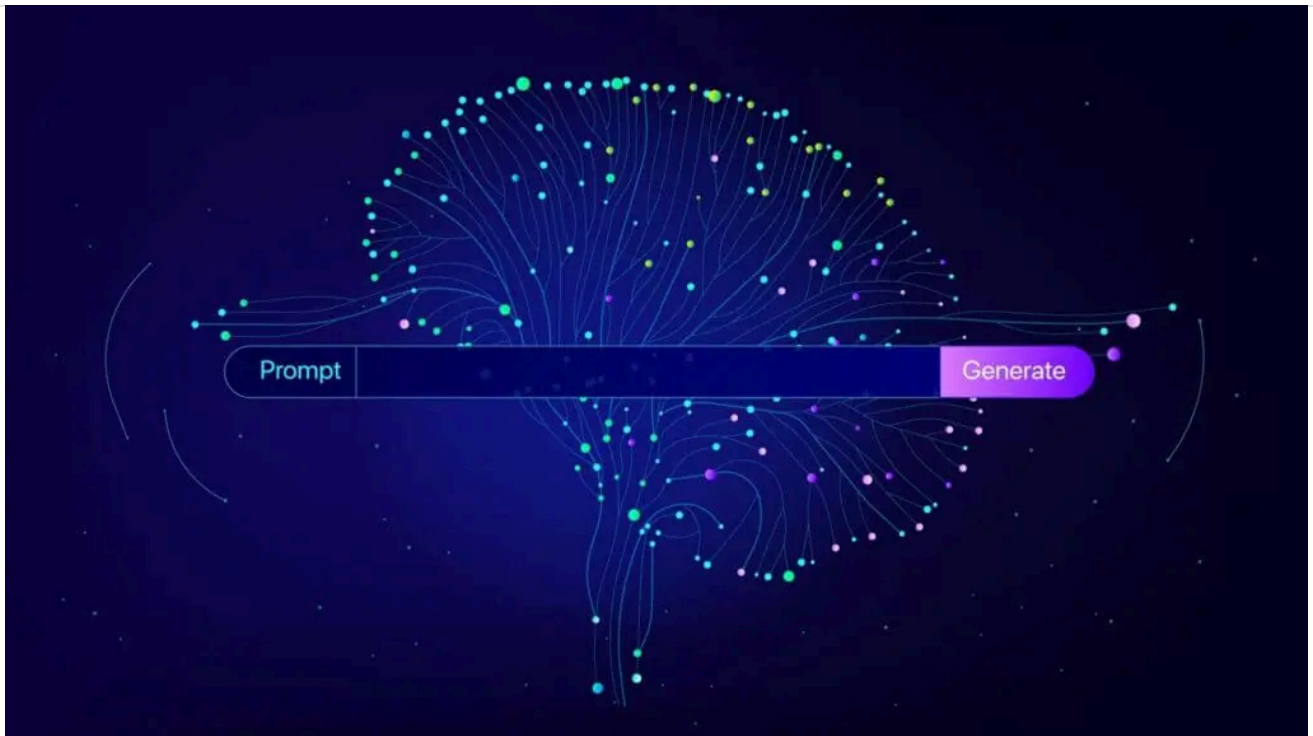
Partecipa al dibattito 

Quando si parla di decisioni dell'AI, il rischio è fermarsi all'etichetta comoda dell'"errore dell'algoritmo". Ma l'automazione non elimina le scelte: le sposta a monte, tra design, dati, metriche e governance, mettendo in tensione colpa, controllo e prevedibilità nel diritto

Pubblicato il 13 feb 2026

**Giacomo Pozzi**

ESSE CI Centro Studi



**M**ai come oggi le **decisioni sono automatizzate**, ma **la responsabilità sembra dissolversi**. Parlare di “errore dell’algoritmo” produce un effetto rassicurante: sposta il peso dalla persona a un’entità tecnica, terza e apparentemente neutra, riducendo la complessità a un “semplice” problema di bug o di calcolo sbagliato.



## Decisioni automatizzate dagli algoritmi: le tutele Gdpr e le eccezioni

12 Febbraio 2019

### Indice degli argomenti ▲

Gli algoritmi non sbagliano: eseguono regole, dati e metriche decise da qualcuno

Quando il problema non è tecnico: le domande giuridiche sulla delega

Decisione distribuita: dove si perde l'autore tra colpa e prevedibilità

Dal bug alla delega: credit scoring, Schufa e tutele GDPR

Decisione e automazione: quando il diritto perde il suo oggetto

Colpa, controllo, prevedibilità: perché le categorie classiche non bastano più

Colpa: dall'errore alla gestione del rischio

Controllo: il mito dell'intervento ex post

Prevedibilità: dal certo al probabilistico

Responsabilità senza colpa: cosa ci dice davvero il GDPR

L'AI Act e la responsabilità spostata a monte: progettare significa già decidere

## Gli algoritmi non sbagliano: eseguono regole, dati e metriche decise da qualcuno

In realtà, gli algoritmi non “sbagliano” nel senso umano che normalmente intendiamo, ma eseguono operazioni logiche coerenti con regole e dati forniti da chi li ha scritti. Se il risultato è distorto, discriminatorio o inadeguato, dipende quindi da scelte progettuali, criteri di addestramento, metriche di performance e contesto d’uso decisi da persone e organizzazioni.

### ★ WHITE PAPER

#### Essere DPO oggi: quali sono le competenze e i requisiti necessari

# Legal # Data protection



## Quando il problema non è tecnico: le domande giuridiche sulla delega

Questa impostazione ha conseguenze giuridiche rilevanti. Se il problema è percepito come meramente “tecnico”, la risposta tende a essere correttiva (fix del codice, audit del modello), trascurando il vero nodo politico e normativo.

Le domande centrali sono altre: chi ha deciso di delegare la decisione a un algoritmo? Con quali garanzie di trasparenza, controllo e tutela dei diritti?

### Decisione distribuita: dove si perde l’autore tra colpa e prevedibilità

Nella sua impostazione tradizionale, il diritto individua, per ogni atto, un suo autore; tuttavia, con l’automazione la decisione è distribuita e mediata da

sistemi complessi, che rendono difficile applicare categorie come colpa e prevedibilità.

## Dal bug alla delega: credit scoring, Schufa e tutele GDPR

---

Ad esempio, immaginiamo un **sistema di scoring creditizio** che assegna automaticamente un punteggio di affidabilità finanziaria basato su dati storici contenuti in banche dati. A fronte del rifiuto alla concessione di un prestito, la banca potrebbe respingere ogni responsabilità dicendo: “Ha deciso l’algoritmo”. Ma, in realtà, dietro quella decisione automatica ci sono scelte e istruzioni ben precise: quali variabili considerare, come ponderarle e quali soglie fissare per l’approvazione.

Se il modello penalizza sistematicamente persone di una certa area geografica o fascia di reddito, non si è davanti a “un errore tecnico”, ma al risultato di bias nei dati e criteri di business incorporati nel design del sistema. Recentemente, la Corte di giustizia, nel caso Schufa, ha chiarito che il credit scoring è **una decisione automatizzata ai sensi dell’art. 22 GDPR** (di cui si parlerà nei successivi paragrafi), con effetti giuridici significativi. Questa impostazione sposta il problema dal “bug” al processo di delega: chi ha deciso di affidare a un algoritmo la valutazione del merito creditizio? Con quali controlli e possibilità di contestazione?

Come si vedrà, **GDPR** e **AI Act** rispondono proprio a questa esigenza: non cercano la “colpa dell’algoritmo”, ma impongono responsabilità organizzativa e obblighi ex ante per garantire che la scelta di automatizzare sia legittima, proporzionata e trasparente.

## Decisione e automazione: quando il diritto perde il suo oggetto

---

Il diritto è costruito attorno a un presupposto: ogni decisione è umana e imputabile a un soggetto dotato di volontà, razionalità e capacità di rispondere

delle proprie scelte. Tutte le categorie giuridiche (responsabilità, colpa, dolo, negligenza) presuppongono questo paradigma. Ma cosa accade quando la decisione è automatizzata?

Nei sistemi algoritmici, la “decisione” non è più un atto unitario, ma diventa:

- **Distribuita:** frammentata tra chi progetta il modello, chi lo addestra, chi lo integra nei processi, chi lo utilizza. Non esiste un unico “decisore”, ma una catena di attori con ruoli e compiti diversi.
- **Mediata da modelli:** il risultato non è frutto di una valutazione diretta, ma di inferenze statistiche basate su dati storici, che incorporano bias e scelte di rappresentazione.
- **Opaca:** la complessità tecnica e la protezione del segreto industriale rendono difficile spiegare il nesso tra input e output, ossia **come** il sistema sia giunto a una data risposta.

Questa trasformazione mette in crisi il diritto perché sfuma l’oggetto della regolazione: **cosa** stiamo regolando? Il singolo output? Il processo di calcolo? La scelta di delegare?

L’art. 22 **GDPR** prova a rispondere, riconoscendo all’interessato il diritto a non essere sottoposto a decisioni con effetti giuridici basate unicamente su trattamenti automatizzati. Ma questa norma fotografa solo la punta dell’iceberg: il problema non è tanto il risultato, quanto la **struttura della decisione** e il reale impatto dell’algoritmo.

Immaginiamo un’azienda che utilizza un algoritmo per filtrare in modo automatico i CV da sottoporre al recruiter. Formalmente, la decisione finale è presa da quest’ultimo, ma, in pratica, ha potuto vedere solo i candidati che il sistema ha ritenuto idonei, non quelli esclusi automaticamente. La decisione è quindi mediata e condizionata da un ranking algoritmico. In questo caso, chi è il “decisore” in senso giuridico? Il recruiter che approva il risultato finale? Il provider che ha progettato il modello? L’organizzazione che ha scelto di

delegare? Il diritto fatica a rispondere perché il suo oggetto di indagine (la decisione imputabile) si è **frammentato** e dissolto in un'intricata rete socio-tecnica.

## Colpa, controllo, prevedibilità: perché le categorie classiche non bastano più

---

Se il diritto perde il suo oggetto, anche le categorie di imputazione vacillano. Queste ultime sono state ideate per un mondo in cui la decisione è umana, ossia un atto unitario imputabile a un soggetto. L'automazione le mette in crisi non perché l'AI sia "nuova", ma perché sposta il luogo della decisione, frammentandone processi e logica. È quindi necessario rivedere le categorie di colpa, controllo e prevedibilità.

### Colpa: dall'errore alla gestione del rischio

---

La nozione stessa di colpa presuppone una deviazione da uno standard di diligenza atteso, ma nei sistemi algoritmici l'"errore" non è un'anomalia: è una certezza prevista, ponderata e accettata. Le decisioni algoritmiche si basano sulla realizzazione statistica di un modello che lavora su probabilità. Se un algoritmo di riconoscimento facciale sbaglia il 2% delle volte, l'errore non dipende da un bug: è il risultato di **metriche di performance note** e accettate dal progettista. Davanti all'errore la domanda, quindi, non è più "chi ha sbagliato?", ma **chi ha deciso che quel margine d'errore era accettabile?** Questo sposta la responsabilità dalla condotta individuale alla **governance del processo**.

Concretamente, nel momento in cui l'AI sposta il luogo della decisione, il diritto deve spostare il luogo della responsabilità. La colpa resta, ma si parametrizza alla cura del processo e alla governance della scelta tecnologica, più che al singolo output "sbagliato". È una responsabilità **organizzativa e preventiva**: se non si possono assicurare condizioni di affidabilità e controllo adeguate al rischio, **non bisogna automatizzare**.

## Controllo: il mito dell'intervento ex post

---

Il controllo umano ex post, per essere effettivo, presuppone che l'operatore abbia la possibilità di intervenire e correggere. Ma nei sistemi complessi questo controllo è spesso parziale: dataset forniti da terzi, modelli addestrati da altri, API proprietarie, log incompleti. Per queste ragioni, anche quando c'è il **cosiddetto human-in-the-loop**, il potere di intervento è spesso meramente formale e non sostanziale. Solitamente, l'uomo alla fine del processo automatico può decidere se approvare o meno il risultato, ma non può intervenire per modificarlo.

Ad esempio, se un algoritmo di scoring respinge una richiesta di prestito, il funzionario può "validare" la decisione, ma non ha strumenti per capire il modello o modificarlo per giungere a un esito differente. Il controllo diventa quindi **rituale** e non effettivo: una formalità che dà una parvenza di supervisione umana. È stato inoltre riscontrato che la supervisione umana può aumentare l'accettazione del sistema da parte degli utenti. Tuttavia, perché sia concreta, la **human oversight** deve essere progettata come potere sostanziale (**interrompere, modificare, disattivare**) e non come un mero bollino rassicurante da apporre sul risultato.

Sul piano normativo, **l'AI Act disciplina la supervisione umana (art. 14)**, prevedendo che debba prevenire o ridurre al minimo i rischi per salute, sicurezza o diritti fondamentali che possono emergere dall'utilizzo di un sistema di IA ad alto rischio, anche in condizioni di uso improprio ragionevolmente prevedibile. Nonostante tali intenti, la letteratura ha segnalato limiti e ambiguità della supervisione umana: **cosa, quando e da chi** va esercitata l'oversight? E quanto è prudente affidare ai provider la definizione dell'infrastruttura di controllo? Sono nodi che incrociano design, formazione e governance.

**Prevedibilità: dal certo al probabilistico**

---

Tradizionalmente, il diritto e il concetto di colpa si basano sull'idea che le conseguenze di un'azione siano ragionevolmente prevedibili. Nei sistemi algoritmici, invece, questa certezza viene meno. I modelli di machine learning sono non lineari, dipendono dal contesto e dai dati forniti e generano risultati che possiamo solo stimare in termini probabilistici. In breve, non c'è alcuna garanzia di certezza per il singolo caso.

La prevedibilità diventa quindi **situata e statistica**: conosciamo il rischio medio, non l'esito puntuale. Questo scarto mina la logica giuridica classica, che cerca nessi causali chiari e imputabili, e impone di ripensare la responsabilità come **gestione del rischio**, più che come imputazione di un errore.

## Responsabilità senza colpa: cosa ci dice davvero il GDPR

---

Il GDPR non ridefinisce il concetto di colpa, né cerca il "responsabile dell'errore". Introduce invece una logica diversa: quella della **responsabilità organizzativa e preventiva** in capo al titolare del trattamento. Quest'ultimo non deve solo rispettare le regole, ma deve anche poter dimostrare di averle rispettate. Questo impone di progettare processi, adottare misure tecniche e organizzative proporzionate al rischio e **documentare scelte e controlli**. La responsabilità diventa quindi ex ante, continua e procedurale: non si limita a reagire al danno, ma si concentra sulla cura del processo che porta alla decisione automatizzata.

L'art. 22 GDPR aggiunge tutele individuali (diritto all'intervento umano e possibilità di contestare la decisione), ma queste operano a valle del processo automatizzato. Il vero cambio di paradigma è invece a monte: la scelta di automatizzare deve essere **giustificata, valutata e governata**. In questo senso, il GDPR, anticipando la logica dell'AI Act, ha spostato la responsabilità dalla "colpa per errore" alla responsabilità per **scelta tecnologica**.

Concretamente, a una banca che decida di utilizzare un algoritmo per valutare l'affidabilità creditizia dei clienti non basta dire "l'algoritmo è conforme". Il GDPR impone che **dimostri di aver valutato i rischi per i diritti e le libertà degli**

**interessati (DPIA)**, di aver implementato misure di mitigazione del rischio (es. soglie di confidenza e **controlli umani significativi**) e di aver predisposto procedure per consentire al cliente di contestare la decisione. Se queste misure non esistono, la responsabilità non nasce dall'errore del modello, ma dalla **mancata governance** della scelta di automatizzare.

## **L'AI Act e la responsabilità spostata a monte: progettare significa già decidere**

---

Se il GDPR era già intervenuto su questi temi, con l'AI Act si registra un ulteriore cambio di passo. Si cristallizza l'idea che la responsabilità non sorge solo a valle, dopo che il danno si è già verificato, ma sin dalla fase di progettazione e messa in servizio del sistema. Il regolamento europeo riconosce che la scelta di ricorrere a sistemi automatizzati è già una scelta giuridicamente rilevante, da cui discendono conseguenze importanti.

Per i sistemi ad alto rischio, gli obblighi sono chiari e dettagliati:

- **Gestione del rischio** lungo tutto il ciclo di vita (art. 9)
- **Qualità e governance dei dati** (art. 10)
- **Documentazione tecnica** e registri per garantire tracciabilità (artt. 11–12)
- **Trasparenza** verso gli utilizzatori (art. 13)
- **Supervisione umana effettiva** (art. 14)
- Requisiti di **accuratezza, robustezza e sicurezza** (art. 15)

A questi si aggiungono obblighi per provider e deployer (artt. 16–26), valutazioni di conformità e marcatura CE (artt. 43–49). La logica è chiara: non basta correggere l'errore, bisogna **prevenire il rischio**. Progettare un sistema significa già decidere come e dove delegare potere decisionale, con impatti sui diritti fondamentali. In altre parole, l'AI Act conferma lo spostamento del luogo della responsabilità.

# Decisioni algoritmiche come banco di prova dello Stato di diritto digitale

Le decisioni algoritmiche rappresentano un banco di prova per lo Stato di diritto nell'era digitale.

L'innovazione non riduce il bisogno di regole: lo rende più stringente. Occorre garantire che **trasparenza, tracciabilità, controllo umano e tutela dei diritti** siano elementi strutturali del progetto, non aggiunte marginali. GDPR e **AI Act** convergono su questa logica, spostando la responsabilità dalla ricerca del "colpevole" alla **governance preventiva** delle scelte tecnologiche.

La domanda chiave non è più "chi ha commesso l'errore?", bensì: **chi ha deciso di automatizzare** in questo modo, con questi dati e queste condizioni? È su questa decisione che deve fondarsi la responsabilità giuridica nel nuovo Stato di diritto digitale, imponendo una governance che non si limiti alla compliance, ma integri etica, trasparenza e **accountability by design**.

## ★ WHITEPAPER

### Norma ISO 31700 e privacy by design: cosa devono sapere aziende e consulenti

# Contract Management

# Privacy/Compliance



@RIPRODUZIONE RISERVATA

Valuta la qualità di questo articolo





Giacomo Pozzi

ESSE CI Centro Studi

Seguimi su 

## Leggi anche:

- [GDPR, quando “bypassare” il Garante: la tutela giurisdizionale diretta](#)
- [Dal porno alla CIE: così avanza il tecnocontrollo digitale](#)
- [GDPR, tutto ciò che c'è da sapere per essere in regola](#)



*Lasciaci il tuo parere!*

**B** *I* U         

 Nome

 Email\*

 Sito web

Commenta

0 COMMENTI

### WHITE PAPER

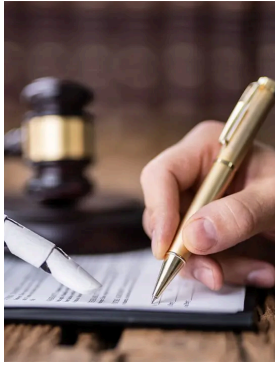
Dalla normativa all'azione: come rendere concreta la legge sull'IA

### WHITEPAPER

NIS2: come conformarsi alla direttiva e potenziare la sicurezza

dell'UE

07 Nov 2025



Scaricalo gratis!

DOWNLOAD

informatica

25 Set 2024

Scaricalo gratis!

DOWNLOAD

## Argomenti

**F** formazione

**M** Machine Learning


**T** tracciabilità

## Canali

**P** Privacy

**S** Sicurezza digitale

## Con o Senza – Galaxy AI per il business

Galaxy AI 

 Filtra per topic



# CON SENZA l'AI in ufficio?

**PA mobile, i vantaggi di continuità operativa, sicurezza integrata e lavoro connesso**

## TECNOLOGIE

PA mobile, i vantaggi di continuità operativa, sicurezza integrata e lavoro connesso

## InnovAttori

**Tracciabilità supply chain, come Erp e cloud spingono la competitività**

14 Nov 2025

**Manifattura elettronica, come salvare il settore con la gestione smart degli impianti**

31 Ott 2025

**Cybersecurity nel manifatturiero, perché puntare sulle persone: il ruolo di policy e formazione**

01 Ott 2025

**AI per il lavoro in condizioni estreme, quali tecnologie scegliere**

27 Ago 2025

**Verso una PA cognitiva: ecco le strategie di innovazione per gli enti**

14 Ago 2025

[Vedi tutti gli approfondimenti >](#)


## Articoli correlati

### DIRITTI

GDPR, quando "bypassare" il Garante: la tutela giurisdizionale diretta

09 Set 2025

di Roberta D'Ercole e Lorenzo Scapellato

Condividi 

## Dal porno alla CIE: così avanza il tecnocontrollo digitale

11 Lug 2025

di Marco Calamari

Condividi 

### GDPR

GDPR, tutto ciò che c'è da sapere per essere in regola

04 Giu 2025

di Anna Cataleta e Alessandro Longo

Condividi 

### WHITEPAPER

NIS2: come conformarsi alla direttiva e potenziare la sicurezza informatica

25 Set 2024

Scaricalo gratis!

DOWNLOAD