


tu che ne sai?

L'intelligenza artificiale più sicura per tutti

Intelligenza Artificiale e cittadini

Guida pratica per capire benefici,
rischi e tutele nei servizi digitali.

Questa guida aiuta i cittadini a usare i servizi digitali con più consapevolezza, a riconoscere i segnali di rischio e a sapere come reagire quando qualcosa non torna.



Questa guida è realizzata nell'ambito del progetto Tu che ne sai? L'intelligenza artificiale più sicura per tutti, finanziato dal MIMIT. D.D. 12 maggio 2025.

Il progetto è realizzato in collaborazione tra Adoc, Cittadinanzattiva, Federconsumatori, U.Di.Con (capofila) e Unione Nazionale Consumatori.

Perché questa guida

L'Intelligenza Artificiale è già parte della nostra vita quotidiana - nei motori di ricerca, nelle chatbot, nei social, nelle app bancarie - spesso senza che ce ne accorgiamo. Può essere molto utile, ma **non è infallibile**: può sbagliare, dare risposte incomplete o prendere decisioni difficili da capire e non sempre è chiaro come vengono usati i nostri dati.

Per questo vale la pena usare i servizi digitali con un po' più di consapevolezza. Non servono competenze tecniche: bastano alcune regole semplici e sapere cosa fare quando qualcosa non torna.

Questa guida ti aiuta a riconoscere i benefici dell'IA e i rischi più comuni, a proteggere i tuoi dati e a muoverti con più sicurezza nel mondo digitale. E se qualcosa va storto, ricorda che non sei solo: informarsi per tempo e chiedere aiuto può fare una grande differenza.

L'obiettivo non è temere la tecnologia, ma usarla in modo più attento e informato.

1. Intelligenza Artificiale: che cos'è, in parole semplici

Quando si parla di Intelligenza Artificiale si pensa spesso a qualcosa di complicato o lontano. In realtà è già presente in molti servizi che usiamo ogni giorno: capisce testi, riconosce immagini, suggerisce scelte, risponde a domande, prende decisioni in automatico. In parole semplici, l'IA analizza grandi quantità di dati, cerca schemi ricorrenti e produce un risultato: una risposta, un consiglio, un contenuto.

Attenzione però: l'IA non ha il buon senso umano, l'esperienza di vita o la responsabilità morale. Lavora basandosi sulla probabilità, per cui può sembrare estremamente sicura di sé anche quando ti sta dando una risposta completamente sbagliata o inventata.

Per un cittadino non serve conoscere i dettagli tecnici. Bastano **tre idee di base**:

1. l'IA è già nella nostra vita quotidiana;
2. può essere utile, ma non è infallibile;
3. se un sistema automatico sbaglia o ti penalizza, il problema è reale anche se la tecnologia non è visibile.

L'IA è uno strumento potente, ma non sostituisce il giudizio umano, la verifica dei fatti e la tutela dei diritti.

2. Dove i cittadini incontrano l'IA nei servizi digitali

L'IA non è presente solo quando apri una chatbot o provi una nuova app. Entra in gioco in molti momenti della vita digitale, spesso senza che te ne accorga.

Prima di un acquisto, i prodotti che vedi, l'ordine dei risultati e le offerte personalizzate sono spesso il frutto di algoritmi automatici. Anche i prezzi possono variare da utente a utente: quello mostrato a te non è necessariamente uguale a quello mostrato a qualcun altro.

Durante un acquisto o l'accesso a un servizio, l'IA gestisce controlli antifrode, verifiche di identità e segnalazioni di attività sospette. Questi sistemi migliorano la sicurezza, ma possono sbagliare: bloccare una carta, sospendere un account o fermare un'operazione legittima senza una spiegazione comprensibile.

Nell'assistenza clienti, chatbot e risponditori automatici sono ormai ovunque. Possono essere comodi per problemi semplici, ma rischiano di dare informazioni sbagliate o di rendere impossibile parlare con una persona reale. Quando si tratta di rimborsi, recessi o garanzie, è sempre meglio verificare anche i documenti ufficiali.

Nei servizi continuativi - energia, telefonia, internet - l'IA può intervenire nelle offerte, nella gestione dei re-

clami e nei controlli sui pagamenti, producendo comunicazioni standardizzate e difficili da contestare.

In banca e nelle assicurazioni, sistemi di scoring automatico possono influenzare la concessione di un credito o la valutazione del rischio. Il problema non è solo ricevere un rifiuto, ma riceverlo senza capire perché e senza sapere se il caso è stato davvero esaminato da una persona.

Sui social e nelle piattaforme online, l'IA decide cosa mostrarti, cosa spingere e cosa nascondere - e può contribuire alla sospensione di un account o alla limitazione di alcune funzioni.

Nei contenuti che circolano online, infine, l'IA può creare o modificare testi, immagini, audio e video in modo molto credibile. Un messaggio ben scritto o una voce familiare non bastano più, da soli, a garantire che ciò che vedi sia autentico.

Sapere dove può comparire l'IA aiuta a non farsi trovare impreparati: a fare le domande giuste, chiedere chiarimenti e conservare le prove quando serve.

3. I benefici dell'IA per i cittadini

L'IA può rendere la vita digitale più semplice e comoda in diversi modi.

Il vantaggio più immediato è la **velocità**: cercare informazioni, ricevere una risposta, completare una procedura - molte operazioni che prima richiedevano tempo ora si risolvono in pochi secondi.

C'è poi la **facilità d'uso**: alcuni sistemi aiutano a orientarsi tra siti, moduli e contenuti, suggerendo informazioni utili e rendendo più semplice trovare quello che si cerca, soprattutto quando le informazioni sono tante e dispersive.

L'IA può anche **personalizzare l'esperienza**: ricordare preferenze, proporre contenuti più vicini agli interessi dell'utente o suggerire percorsi su misura. Se usata bene, rende il servizio più comodo e meno dispersivo.

Un altro beneficio utile è il **supporto nella comprensione**: alcuni strumenti riassumono testi lunghi, spiegano termini difficili o aiutano a confrontare più opzioni. Può essere prezioso quando si leggono condizioni di servizio, comunicazioni tecniche o documenti poco immediati.

Sul piano dell'**accessibilità**, strumenti che combinano testo, voce e immagini possono abbattere barriere pratiche e rendere i servizi digitali più fruibili per persone con esigenze diverse.

Infine, molti servizi automatizzati sono **disponibili h24**, offrendo un primo livello di assistenza anche fuori dagli orari tradizionali - utile per richieste semplici o per orientarsi in un primo momento.

La tecnologia è davvero un beneficio solo quando è chiara, corretta e pensata per le persone. Non è una soluzione perfetta a tutto, ma può essere una risorsa preziosa quando semplifica davvero la vita del cittadino. L'importante è che resti uno strumento al servizio delle persone, non il contrario.

4. I rischi da conoscere

L'IA può sbagliare, fraintendere o prendere decisioni poco chiare. Conoscere i rischi principali aiuta a usare i servizi digitali con più attenzione.

Risposte sbagliate ma convincenti. Una chatbot può scrivere bene e sembrare sicura anche quando dà informazioni errate o incomplete. Quando si tratta di rimborsi, contratti, scadenze o dati personali, vale sempre la pena verificare anche le fonti ufficiali.

Decisioni automatiche difficili da capire. Blocchi di pagamento, sospensioni di account, rifiuti di richieste: spesso arrivano senza una spiegazione chiara. Senza capire il perché, diventa difficile contestare o chiedere una revisione.

Uso poco trasparente dei dati. Molti sistemi analizzano abitudini, preferenze e cronologia senza che l'utente lo percepisca chiaramente. È importante leggere le informative e fare attenzione ai dati che si sceglie di condividere.

Trattamenti ingiusti. I sistemi automatici possono applicare prezzi, offerte o controlli diversi a persone in situazioni simili. Quando si riceve un trattamento sfavorevole senza capirne il motivo, è giusto fermarsi e chiedere spiegazioni.

Pressioni commerciali. Urgenze artificiali, pulsanti in evidenza solo in una direzione, procedure complicate per rinunciare a un acquisto: la tecnologia può spingere a decidere in fretta e senza piena consapevolezza.

Truffe più credibili. Messaggi, immagini, audio e video generati dall'IA possono sembrare autentici anche quando non lo sono. Davanti a richieste urgenti di denaro, codici o dati bancari, è sempre meglio fermarsi e verificare.

Impossibilità di parlare con una persona. Chatbot che ripetono le stesse risposte, moduli rigidi, nessun accesso a un operatore: quando il sistema automatico non basta, deve essere possibile chiedere un intervento umano.

Il rischio più grande, in fondo, è fidarsi ciecamente di un sistema solo perché appare moderno e sicuro.

Conoscere questi rischi non serve ad avere paura della tecnologia, serve a usarla meglio.

5. I segnali di attenzione: quando è bene fermarsi e verificare

Non sempre è necessario sapere con certezza se dietro un problema c'è un sistema automatico. Quello che conta è riconoscere i segnali che suggeriscono di fermarsi e verificare prima di agire.

La risposta è troppo generica. Non spiega cosa è successo, perché e cosa puoi fare. Chiedi chiarimenti.

Non c'è un interlocutore umano. Solo chatbot, email automatiche e percorsi che girano in tondo - soprattutto quando si tratta di soldi, contratti, rimborsi o dati personali. **La decisione arriva subito ed è rigida.** Una risposta istantanea, senza spiegazioni e senza tener conto della tua situazione concreta, non va accettata per forza come corretta.

La risposta contraddice i documenti. Se non coincide con il contratto, le condizioni del sito o le comunicazioni precedenti, fermati.

La stessa risposta si ripete identica. Se anche cambiando domanda o aggiungendo dettagli non cambia nulla, il sistema probabilmente non sta valutando davvero il tuo caso.

Ti viene chiesto di agire in fretta. L'urgenza artificiale è uno dei segnali più importanti. Cliccare subito, inquadrare un QR code, comunicare codici o dati bancari: rallenta e verifica sempre.

Il contenuto sembra credibile, forse troppo. Immagini, voci e messaggi possono sembrare autentici anche

quando non lo sono. Non dare per scontato che sia vero solo perché è fatto bene.

Non è chiaro con chi stai parlando. Se non è evidente se dall'altra parte c'è una persona o un sistema automatico, procedi con più cautela.

Ti vengono chiesti troppi dati. Se per una semplice operazione ti vengono richieste informazioni sensibili o documenti non necessari, chiediti se la richiesta sia davvero proporzionata.

Non sai come contestare. La mancanza di un percorso chiaro per segnalare un errore o chiedere una revisione è di per sé un segnale da non ignorare.

Quando noti uno di questi segnali, segui questi passi:

non agire d'impulso; rileggi con calma; confronta con il sito ufficiale o il contratto; salva screenshot, email e numeri pratica; non condividere dati o denaro finché non hai verificato; cerca un canale ufficiale e, se possibile, un contatto umano.

Non serve capire tutta la tecnologia che c'è dietro. Spesso basta accorgersi che qualcosa non torna e fermarsi prima di fare il passo sbagliato.

6. Le 10 regole pratiche per usare meglio i servizi digitali

Non serve essere esperti di tecnologia per usare i servizi digitali in modo sicuro. Spesso bastano poche regole di buon senso, applicate con un po' di attenzione.

1. Verifica prima di fidarti. Se una risposta riguarda soldi, contratti, rimborsi o dati personali, controlla anche il sito ufficiale, il contratto o un'altra fonte affidabile. Non fermarti alla prima risposta ricevuta.

2. Non condividere più dati del necessario. Inserisci solo quello che è strettamente richiesto. Evita di comunicare documenti d'identità, dati bancari, password o informazioni sanitarie se non sei sicuro del perché vengono chiesti.

3. Non decidere cose importanti basandoti solo su una chatbot. Per accettare un'offerta, fare un pagamento o chiudere un contratto, controlla sempre anche i documenti ufficiali. La chatbot può orientarti, ma non sostituisce una verifica diretta.

4. Conserva le prove. Se qualcosa non torna, salva subito screenshot, email, numeri pratica, data e ora.

5. Diffida dall'urgenza. La fretta è il terreno ideale per errori e truffe. Se un messaggio ti spinge a decidere subito o a condividere dati immediatamente, fermati.

6. Controlla da dove arriva il messaggio. Verifica l'indirizzo email, il numero di telefono, il link e il nome

del servizio. Un messaggio credibile non è necessariamente autentico.

- 7. Chiedi spiegazioni chiare.** Se una risposta è vaga o una decisione ti penalizza senza motivi comprensibili, hai tutto il diritto di chiedere cosa è successo e come puoi contestarlo.
- 8. Cerca un contatto umano quando serve.** Se la chatbot non basta, non arrenderti: cerca un'assistenza clienti, un recapito email, una PEC o uno sportello dedicato.
- 9. Confronta più fonti.** La risposta del sistema automatico coincide con le condizioni contrattuali? Con la FAQ ufficiale? Con le comunicazioni scritte dell'azienda? Se no, approfondisci.
- 10. Quando qualcosa non torna, fermati.** Non proseguire per inerzia. Un dubbio è sempre un segnale da prendere sul serio.

Usa gli strumenti digitali con fiducia, ma non senza controllo.

7. Truffe e inganni potenziati dall'IA

L'IA non viene usata solo per migliorare i servizi digitali. Può essere usata anche per ingannare. E oggi le truffe sono diventate molto più difficili da riconoscere.

In passato un messaggio falso si smascherava facilmente: errori di scrittura, immagini poco realistiche, toni generici. Oggi non è più così. L'IA può scrivere messaggi formali e convincenti, clonare una voce, generare immagini realistiche e simulare conversazioni credibili. Un contenuto ben fatto non è garanzia di autenticità.

I casi più comuni. Il falso messaggio di assistenza - che sembra arrivare da una banca, un corriere o un gestore di pagamenti - invita a cliccare un link, aggiornare dati o risolvere un problema urgente. Il falso allarme di sicurezza ("accesso sospetto", "account in sospeso", "verifica la tua identità") punta a ottenere password, codici o dati bancari. Ci sono poi falsi investimenti, rimborsi e premi, spesso personalizzati e dall'aspetto professionale - il che li rende ancora più pericolosi.

Audio e video manipolati. Oggi è possibile imitare la voce o il volto di una persona in modo molto realistico. Anche davanti a una voce o un'immagine che sembrano familiari, vale sempre la pena verificare su un secondo canale prima di agire.

La personalizzazione è il vero pericolo. Un messaggio può contenere il tuo nome, fare riferimento a un acquisto recente o imitare il tono di una comunicazione ufficiale. Più sembra vicino alla tua realtà, più è facile abbassare la guardia.

Segnali da non ignorare: urgenza (“agisci subito”), richiesta di dati riservati, pressione emotiva (paura, minacce, promesse), link che portano fuori dai canali ufficiali.

Cosa non fare: non cliccare subito, non richiamare il numero del messaggio, non inviare documenti o codici, non autorizzare pagamenti, non scaricare file senza verificare la fonte.

Cosa fare subito: entra nel sito ufficiale digitando l'indirizzo tu stesso; contatta il servizio con recapiti che già conosci; salva screenshot, numeri e orari. Se hai già condiviso dati, agisci subito: cambia le password, contatta la banca e blocca gli strumenti di pagamento.

La regola da ricordare è semplice: più un messaggio sembra urgente e perfettamente costruito, più vale la pena fermarsi. Non si tratta di diffidare di tutto, ma di non reagire d'impulso. In caso di dubbio, qualche minuto di verifica vale sempre più di un errore a cui può essere poi difficile rimediare.

8. I tuoi diritti e le tutele principali

Usare un servizio digitale automatizzato non significa rinunciare ai propri diritti. Anche quando dietro c'è un sistema di IA, **esistono regole precise a tutela del cittadino.**

Sapere con chi stai parlando. La normativa europea prevede obblighi di trasparenza: in determinati casi devi poter capire se stai interagendo con un sistema automatico e non essere indotto a credere che sia una persona reale.

Ricevere informazioni corrette. Un'impresa non può usare strumenti digitali per confonderti, omettere informazioni importanti o spingerti verso una scelta che non avresti fatto se fossi stato informato correttamente. Se una chatbot dà informazioni sbagliate o una piattaforma usa modalità poco trasparenti, non è solo un problema tecnico: può essere una violazione delle regole sulla correttezza commerciale.

Protezione dei dati personali. Quando un sistema di IA usa i tuoi dati, continuano a valere le regole sulla privacy. Hai diritto a sapere quali dati vengono trattati, perché e con quali garanzie. Puoi chiedere di accedervi, correggerli o, in certi casi, chiederne la cancellazione. Se ritieni che vengano usati in modo illecito, puoi rivolgerti al Garante per la protezione dei dati personali.

Contestare le decisioni automatiche. Quando una decisione che ti riguarda è presa unicamente da un sistema automatico - e ha effetti concreti sulla tua vita - il GDPR prevede tutele specifiche: puoi chiedere l'intervento di una persona, esprimere il tuo punto di vista e contestare l'esito.

Revisione umana reale. L'intervento umano non deve essere solo formale: deve essere effettivo, con una persona competente che riesamini davvero il caso e possa, se necessario, correggere la decisione automatica.

A chi rivolgersi. Per problemi sui dati personali: Garante Privacy. Per pratiche commerciali scorrette o ingannevoli: AGCM. Per questioni bancarie, finanziarie o assicurative: le autorità di settore competenti.

Non tutti i diritti si applicano allo stesso modo in ogni situazione, ma il principio è semplice: se un sistema automatico ti condiziona o ti danneggia, non sei obbligato ad accettarlo passivamente. Puoi chiedere chiarimenti, contestare e pretendere una verifica reale del tuo caso.

9. Cosa fare se pensi di aver subito un problema

Quando un servizio digitale ti crea un problema, la cosa più importante è non restare bloccato tra rabbia e confusione. Anche senza sapere se dietro ci sia un sistema automatico, puoi muoverti con ordine fin da subito.

1. Ricostruisci cosa è successo. Fermati un momento e metti in fila i fatti: cosa è successo, quando, su quale piattaforma, quale operazione stavi facendo e quale risposta hai ricevuto.

2. Salva subito le prove. Screenshot, email, messaggi in chat, numeri pratica, data e ora, importi coinvolti. Non aspettare: chat e schermate possono sparire rapidamente.

3. Non cancellare tutto d'impulso. Quando si è irritati viene spontaneo chiudere tutto. Prima di farlo, salva almeno gli elementi essenziali: una semplice schermata può fare la differenza tra un problema difficile da ricostruire e un reclamo fondato.

4. Verifica se il problema è reale. A volte si tratta di un errore temporaneo. Controlla se il messaggio si ripete, se il contratto dice qualcosa di diverso e se canali ufficiali riportano le stesse informazioni.

5. Chiedi spiegazioni chiare. Non fermarti alla prima risposta generica. Chiedi perché l'operazione è stata bloccata, quale regola è stata applicata, se il caso è stato esaminato da una persona e come puoi contestare.

- 6. Usa canali ufficiali e tracciabili.** Email ufficiale, modulo reclami, PEC, numero clienti sul sito ufficiale. Evita canali informali che non lasciano traccia.
- 7. Chiedi una revisione del caso.** Hai diritto a chiedere un controllo più approfondito, un esame umano del caso e una risposta scritta più dettagliata.
- 8. Proteggi dati e account, se necessario.** Se hai cliccato su qualcosa di sospetto o condiviso dati per errore, agisci subito: cambia le password, controlla movimenti e accessi, contatta la banca e blocca eventuali strumenti di pagamento.
- 9. Metti tutto per iscritto.** Una buona segnalazione include: chi sei, quale servizio, cosa è successo, quando, quale danno hai subito, quali prove hai e cosa stai chiedendo.
- 10. Non aspettare se il danno è concreto.** Se il problema riguarda denaro, dati personali o accesso a un servizio importante, muoviti presto.

La regola pratica è semplice: prima documenta, poi contesta. Non serve sapere quale tecnologia c'è dietro. Quello che conta è non restare passivi e muoversi con ordine - è il modo migliore per limitare il danno e far valere le proprie ragioni.

10. Le associazioni dei consumatori: un aiuto concreto

Quando un servizio digitale non funziona, una chatbot non risolve nulla o una decisione automatica ti penalizza, è facile sentirsi soli e disorientati. È proprio in questi casi che un'associazione dei consumatori può fare la differenza.

Non si tratta solo di chiedere un'opinione. Un'associazione può aiutarti a capire se il comportamento del servizio è corretto, quali diritti puoi far valere, quali prove conservare, come scrivere una contestazione efficace e a chi rivolgerti. Un supporto pratico, non solo informativo.

Quando è utile contattarla. Quando ricevi risposte automatiche poco chiare o contraddittorie; quando non riesci a parlare con una persona; quando un rimborso o una contestazione vengono respinti senza spiegazioni; quando sospetti un uso scorretto dei tuoi dati; quando hai dubbi su offerte, contratti o consensi digitali; quando pensi di aver subito una truffa.

Perché è meglio muoversi presto. Molti aspettano troppo, perdendo tempo tra chatbot e messaggi senza risposta. Intervenire prima aiuta a conservare le prove nel modo giusto, evitare che il problema peggiori, contestare entro i tempi utili e scegliere subito il canale più efficace.

Un aiuto anche nella complessità. Condizioni lunghe, linguaggi tecnici, procedure automatizzate: orientarsi non è sempre facile. L'associazione può tradurre tutto questo in indicazioni pratiche e aiutarti a capire quali passi conviene davvero fare.

Non solo tutela individuale. Quando più cittadini segnalano problemi simili, le associazioni possono individuare pratiche scorrette ricorrenti e contribuire a rafforzare la tutela dei consumatori in modo più generale. Chiedere aiuto, quindi, non serve solo a risolvere il proprio caso.

In caso di dubbio, non aspettare: un primo orientamento può già fare la differenza.

Scheda pratica finale

La regola di fondo è semplice:

fermati, verifica, documenta, poi agisci.

Le 5 cose da ricordare sempre

-
- 1. Non fidarti della prima risposta.** Se riguarda soldi, contratti, rimborsi o dati personali, verifica sempre anche da una fonte ufficiale.

 - 2. Non agire di fretta.** Se un messaggio ti mette pressione o ti chiede di decidere subito, fermati.

 - 3. Salva tutto ciò che può essere utile.** Screenshot, email, chat, numeri pratica, date e orari possono diventare fondamentali.

 - 4. Proteggi i tuoi dati.** Non comunicare password, codici, dati bancari o documenti senza essere sicuro del perché vengono chiesti.

 - 5. Chiedi spiegazioni chiare.** Se una decisione ti penalizza o una risposta è vaga, hai il diritto di chiedere chiarimenti e, se serve, una revisione del caso.
-

Se succede questo, fai questo

SITUAZIONE

COSA FARE

Una chatbot ti dà una risposta importante

Controlla anche il sito ufficiale o il contratto; fai uno screenshot; cerca un contatto umano.

Un pagamento viene bloccato

Non ripetere subito l'operazione; controlla le comunicazioni ufficiali; contatta la banca; conserva data, ora e importo.

Un account viene sospeso

Salva la schermata; verifica se c'è una motivazione; controlla email e notifiche; chiedi una revisione.

Ricevi un messaggio urgente che chiede dati o denaro

Non cliccare sul link; non condividere codici o documenti; entra dal sito ufficiale in modo autonomo; se hai dubbi, interrompi.

Un'offerta o un contratto non ti sono chiari

Non accettare subito; rileggi condizioni, costi e durata; verifica rinnovi automatici o penali; conserva una copia.

Pensi di aver subito una truffa

Blocca subito ciò che puoi; cambia le password; contatta la banca; salva le prove e ricostruisci i passaggi.

Sospetti un uso scorretto dei tuoi dati

Controlla quali dati hai comunicato; rileggi l'informativa privacy; chiedi chiarimenti su rettifica, opposizione o cancellazione.

Prove da conservare: screenshot, email, chat, numeri pratica, data e ora degli eventi, link e nome del servizio, contratto o condizioni consultate, ricevute e movimenti di pagamento.

Domande utili da farti subito: Cosa è successo? Ho salvato le prove? La risposta è davvero chiara? Sto usando un canale ufficiale? Mi stanno mettendo fretta? Mi chiedono dati o soldi in modo insolito? Posso chiedere una revisione?

Davanti a un servizio digitale poco chiaro o a una decisione automatica che ti penalizza, non devi scegliere tra fidarti ciecamente e diffidare di tutto. La scelta migliore è usare la tecnologia con attenzione, fare verifiche semplici e agire con metodo.

Per ulteriori informazioni e orientamento rivolgiti a

Unione Nazionale Consumatori
www.consumatori.it



UNC
CONSUMATORI.IT

tu che ne sai?

L'intelligenza artificiale più sicura per tutti

Un progetto in collaborazione tra



UNC
CONSUMATORI.IT

Finanziato dal MIMIT.D.D. 12 maggio 2025