

Etica e privacy familiare nell'era dell'intelligenza artificiale

Ethics and Family Privacy in the Age of Artificial Intelligence

MARTÍN CARBAJO-NÚÑEZ, OFM 

Pontificia Università Antonianum, Roma, Italia
Alfonsianum (Pontificia Università Lateranense), Roma, Italia
FST – University of San Diego, California, USA

ORCID <https://orcid.org/0000-0002-2814-5688> • mcarbajon@gmail.com

Ricevuto: 2025-08-11; recensito: 2025-11-08; accettato: 2026-01-11; pubblicato: 2026-06-30

Riassunto: La progressiva espansione dell'intelligenza artificiale sta trasformando la casa in un oggetto di interesse economico e di intrusione tecnologica. Dispositivi progettati per facilitare la vita familiare, come elettrodomestici, veicoli, sensori e assistenti digitali, stanno trasformando gli spazi più intimi della casa in preziose fonti di dati al servizio delle logiche di mercato. La protezione della privacy familiare, e in particolare la salvaguardia del superiore interesse del minore, deve prevalere su qualsiasi presunto beneficio informativo o interesse commerciale. Infatti, quando la privacy viene violata, l'essere umano viene ridotto a un mero oggetto.

Nella prima parte presenteremo alcune conclusioni sulla privacy familiare tratte dal nostro studio di sessanta e cinque codici deontologici giornalistici provenienti da quarantadue paesi europei. Analizzeremo inoltre le sfide che l'intelligenza artificiale pone alla privacy nell'ambito familiare (cap. 2) e nella vita dei minori (cap. 3), per proporre infine strategie che consentano di affrontare tali sfide (cap. 4).

Parole chiave: Privacy, famiglia, minori, intelligenza artificiale, codici deontologici

Abstract: The progressive expansion of artificial intelligence is transforming the home into an object of economic interest and technological intrusion. Devices designed to facilitate family life, such as household appliances, vehicles, sensors, and digital assistants are turning the most intimate spaces of the home into valuable data sources for market logics. Protecting family privacy, and especially safeguarding the best interests of the child, must take precedence over any supposed informational benefit or commercial interest. In fact, when privacy is violated, the human being is reduced to a mere object.

In the first part, we will outline some conclusions on family privacy from our studies of sixty five national codes of journalistic ethics, drafted and adopted by journalists in forty-two European countries. We will then examine the challenges that AI poses to privacy within the family (ch. 2) and in the lives of minors (ch. 3), and finally propose strategies to address these challenges (ch. 4).

Keywords: Privacy, family, minors, artificial intelligence, codes of ethics

La nostra società digitale ha compiuto notevoli progressi nella valorizzazione e nella protezione della privacy personale, ma ha anche favorito l'esibizionismo e la mercificazione della sfera intima. Oggi, «nella comunicazione digitale si vuole mostrare tutto ed ogni individuo diventa oggetto di sguardi che frugano, denudano e divulgano, spesso in maniera anonima»¹. In questo modo, «cessa di esistere il diritto all'intimità», si sgretola il rispetto verso l'altro e «tutto diventa una specie di spettacolo» (FT 42).

Quando l'intimità personale viene violata, l'essere umano è ridotto a un semplice oggetto (cfr. Carbajo-Núñez, 2011, 2012, 2023). L'intelligenza artificiale (IA) generativa sta condizionando ulteriormente il modo in cui ciascuno esprime la propria interiorità e il modo in cui si viene informati sull'intimità altrui. In questo nuovo contesto, è urgente recuperare la capacità di stupirsi di fronte al «mistero sacro» di ogni essere umano (FT 277), riconoscendogli «il diritto di essere sé stesso e di essere diverso» (FT 218), amandolo «come se al mondo non ci fosse altri che lui» (FT 193).

La commercializzazione dei dati personali è oggi una delle industrie più redditizie (Feldman, Haber, 2020). Le tracce digitali che l'individuo lascia involontariamente in qualsiasi attività quotidiana, sia essa commerciale o ludica, vengono raccolte automaticamente e conservate a tempo indeterminato. A partire da queste informazioni digitali, è possibile costruire un profilo dettagliato della persona, che può essere utilizzato per influenzarne i comportamenti e spingerla al consumismo.

Nella prima parte di questo articolo, presenteremo alcune conclusioni tratte dagli studi che abbiamo condotto su sessantacinque codici deontologici di ambito nazionale², elaborati e adottati dai giornalisti di quarantadue paesi europei. L'obiettivo è comprendere come questi professionisti concepiscono il valore dell'intimità umana e come cercano di tutelarla (cfr. Singh, 2018; Banning, 2020; Miller, 2024). Successivamente, analizzeremo le sfide che l'intelligenza artificiale pone alla privacy nell'ambito familiare (cap. 2) e nella vita dei minori (cap. 3), per proporre infine alcune strategie atte ad affrontare tali sfide (cap. 4)³.

Tabella 1. Documenti deontologici europei oggetto di questo studio

Id.	Paese	Denominazione e istituzione emittente
1	c01 FIP (IFJ)	Federazione Internazionale dei Giornalisti (Tirana)
	c02 Albania	Codice etico del giornalista
	c03 Germania	Codice etico e regolamento del Consiglio della stampa
	c04 Armenia	Codice etico del Club della stampa di Yerevan
5	c05 Austria	Codice etico del Consiglio della stampa

1 Il riferimento è all'enciclica di papa Francesco *Fratelli tutti* (d'ora in poi: *FT*), citata secondo la numerazione dei paragrafi. Nel presente testo useremo il termine «intimità» per indicare due dimensioni: una più profonda e una più esterna. La prima si riferisce al nucleo dell'individuo, al suo mistero personale, al suo essere più profondo. La seconda — che chiameremo anche «privacy» — è più spaziale che psicologica. Indica lo spazio che l'individuo riserva a sé stesso e che condivide solo con le persone più vicine.

2 A fini statistici, i codici di un Paese contano come un'unica unità.

3 Questo articolo si basa sulla conferenza tenuta dal Prof. Martín Carbajo-Núñez durante il nono Simposio internazionale sulla famiglia, organizzato dall'Università di Warmia e Mazury a Olsztyn (Polonia), il 12 giugno 2025.

	c06 Azerbaigian	Codice etico professionale per giornalisti
	c07a Belgio	Codice dei principi giornalistici
	c07b Belgio	Raccomandazioni dell'Associazione dei giornalisti (AGJPB) sul trattamento informativo degli stranieri
	c08 Bielorussia	Codice etico professionale del Sindacato dei giornalisti
10	c09a Bosnia-Erzegovina	Codice della stampa
	c09b Bosnia-Erzegovina	Codice di condotta della radiodiffusione
	c10 Bulgaria	Codice etico dei media bulgari
	c11 Croazia	Codice etico dell'Associazione dei giornalisti
	c12 Repubblica Ceca	Codice di condotta del Sindacato degli editori
15	c12b Repubblica Ceca	Codice etico del Sindacato dei giornalisti
	c13 Danimarca	Codice di condotta approvato dal parlamento e adottato dal Sindacato dei giornalisti
	c14 Slovacchia	Codice etico del Sindacato dei giornalisti
	c15 Slovenia	Codice dell'Associazione e del Sindacato dei giornalisti
	c16a Spagna	Codice della Federazione della Stampa di Spagna (FAPE)
20	c16b Spagna	Codice deontologico del Collegio dei giornalisti della Catalogna
	c17 Estonia	Codice deontologico della stampa
	c18 Finlandia	Linee guida di condotta del Sindacato dei giornalisti
	c19a Francia	Codice del Sindacato dei giornalisti
	c19b Francia	Statuto del diritto all'informazione
25	c19c Francia	Norme e pratiche della stampa quotidiana provinciale
	c20 Grecia	Codice etico della stampa e del settore audiovisivo
	c20b Grecia	Codice etico della Federazione panellenica dei giornalisti
	c21 Ungheria	Codice etico dell'Associazione nazionale dei giornalisti
	c22 Irlanda	Codice di condotta del Sindacato nazionale dei giornalisti
30	c23 Islanda	Norme etiche giornalistiche del Consiglio della stampa
	c24a Italia	Codice etico dell'Ordine e della Federazione della stampa
	c24b Italia	Carta di Treviso su informazione e minori
	c24c Italia	Codice sulla televisione e i minori
	c24d Italia	Codice sul trattamento dei dati personali
35	c25 Lettonia	Codice deontologico del Sindacato dei giornalisti
	c26 Lituania	Codice deontologico della stampa scritta e della radiodiffusione
	c27 Lussemburgo	Codice deontologico del Consiglio della stampa
	c28a Macedonia	Codice deontologico dei giornalisti
	c28b Macedonia	Dichiarazione degli editori e dirigenti di SEEMO
40	c29a Malta	Codice del Club della stampa e dell'Istituto di radiodiffusione

	c29b Malta	Codice deontologico del Club della stampa (TMPC)
	c30 Moldavia	Codice deontologico del Sindacato dei giornalisti
	c31 Montenegro	Codice deontologico delle Associazioni dei giornalisti
	c32 Norvegia	Codice etico della stampa norvegese
45	c33 Paesi Bassi	Norme del Collegio dei giornalisti
	c34a Polonia	Codice dell'Associazione dei giornalisti (AJRP)
	c34b Polonia	Statuto etico di giornalisti, editori e radiodiffusori
	c35a Portogallo	Codice deontologico del Sindacato dei giornalisti
	c36 Romania	Codice deontologico del Club della stampa
50	c37a Russia	Norme sul trattamento informativo del terrorismo
	c37b Russia	Codice etico dei giornalisti
	c38 Serbia	Codice dell'Associazione dei giornalisti indipendenti
	c39 Svezia	Codice del Consiglio della stampa, radio e televisione
	c40 Svizzera	Dichiarazione e norme su diritti e doveri del giornalista
55	c41a Turchia	Principi professionali adottati dal Consiglio della stampa
	c41b Turchia	Codice deontologico dell'Associazione dei giornalisti
	c42a Regno Unito	Codice di condotta del Sindacato nazionale dei giornalisti (NUJ)
	c42b Regno Unito	Codice della Commissione per i reclami della stampa (PCC)
	c42c Regno Unito	Norme dell'Associazione dei fotografi sul lavoro con i minori
60	c42d UK.ofcom	Codice di radiodiffusione di Ofcom (Codice dell'editore)
	c43 Ucraina	Codice etico del giornalista
	c44 Cipro	Codice di condotta del giornalista
	c45a Georgia	Codice etico del giornalista
	c45b Georgia	Norme professionali dei media
65	c46 Kosovo	Codice della stampa

1. La privacy familiare nei codici deontologici del giornalismo europeo

I documenti di autoregolamentazione etica, comunemente denominati «codici deontologici»⁴, stabiliscono le linee guida che i professionisti dell'informazione devono seguire per svolgere il proprio lavoro in modo responsabile, secondo criteri oggettivi di servizio pubblico.

⁴ Non esiste una terminologia uniforme per designarli. In inglese, le espressioni più comunemente usate sono: '*codes of ethics*', '*codes of conduct*' e '*codes of practice*'. Sebbene a volte siano considerati sinonimi, nella pratica hanno significati diversi. Cfr. (Fisher, Lovell, 2003, p. 210; Laas, Davis, Hildt, 2022).

La rapida crescita del giornalismo digitale (*online*)⁵ e dell'intelligenza artificiale presenta una nuova problematica. Il ruolo tradizionalmente assegnato alla stampa come filtro e garante del diritto all'informazione sembra essersi indebolito. Oggi, chiunque può pubblicare contenuti su Internet senza apparenti restrizioni⁶.

Il rispetto dell'intimità e della vita privata⁷ è presente nel 71,4% dei codici deontologici europei. In essi si difende il diritto di ogni persona, fisica o giuridica, a controllare le proprie informazioni, sia al momento di fornirle che nelle fasi successive di redazione, pubblicazione e archiviazione. Di seguito vengono presentate alcune conclusioni relative all'ambito familiare.

1.1. Criteri etici per la raccolta, la pubblicazione e l'archiviazione

Durante la fase di raccolta, devono essere evitate ingerenze informative nello spazio privato, compreso il domicilio familiare. Inoltre, viene riconosciuto il diritto del soggetto a esercitare un controllo attivo sull'esattezza, l'uso e l'aggiornamento dei suoi dati personali già archiviati.

Il 78,5% dei codici richiede che l'informazione sia ottenuta in modo onesto. Sono ammesse eccezioni a questa norma solo quando i dati raccolti sono di rilevante interesse pubblico e non vi è altro modo per ottenerli senza correre gravi rischi. In ogni caso, deve essere sempre rispettata la proporzionalità tra i mezzi impiegati e l'utilità sociale delle informazioni ricercate.

Una volta pubblicata l'informazione, sia il giornalista che l'impresa informativa hanno l'obbligo di correggere qualsiasi dato errato, incompleto o distorto, facilitando l'esercizio del diritto di replica.

Le informazioni di carattere personale appartengono sempre al soggetto cui si riferiscono. Di conseguenza, è necessario richiederne nuovamente il consenso per utilizzarle a fini diversi da quelli che hanno motivato la raccolta iniziale. Inoltre, coloro che archiviano tali informazioni sono obbligati a tenere informati gli interessati su tutto ciò che è necessario (ubicazione, responsabili, procedure) per consentire loro di esercitare un controllo effettivo sui propri dati.

La pubblicazione di dati personali non è giustificata dal solo fatto che essi siano veri o accessibili; è indispensabile che siano anche rilevanti e che la loro divulgazione generi un «beneficio sociale straordinario». Occorre dunque distinguere tra «soddisfare la curiosità del pubblico» e «servire l'interesse del pubblico». Non è raro che l'audience sia attratta da aspetti irrilevanti o morbosi della vita privata, ma tale fattore non è sufficiente per renderli oggetto di interesse pubblico.

5 Il primo giornale online, cioè pubblicato regolarmente su Internet, è nato nel gennaio 1994. Sei anni dopo c'erano già più di 5400 giornali online (Gunter, 2003, p. 143).

6 Sono diventati popolari i cosiddetti «weblog» o semplicemente «blog», che sono una sorta di giornale online, creato da singoli individui. Cfr. (Miladi, 2022).

7 Alcuni codici distinguono tra «sfera intima» e «privacy» (c12).

1.2. Tutela della privacy dei bambini e dei ragazzi

Il 52,3% dei codici afferma esplicitamente che la protezione della privacy dei minori deve avere la precedenza sul valore informativo della notizia, poiché si tratta di persone ancora vulnerabili e influenzabili. Occorre evitare qualsiasi ingerenza nella loro vita privata che possa causare traumi o compromettere negativamente il loro sviluppo futuro. L'età maggiormente tutelata varia a seconda del codice, potendo arrivare fino ai quattordici, quindici, sedici o diciotto anni.

I minori non devono essere oggetto di interferenze arbitrarie né di forme di violenza, danno, abuso psicologico o sfruttamento. Il fatto che siano figli di personaggi pubblici non giustifica un minor grado di protezione della loro privacy.

Il giornalista dovrà essere particolarmente prudente quando i minori compaiono come vittime, testimoni o imputati in procedimenti giudiziari, per non danneggiare la loro personalità né compromettere il loro futuro reinserimento sociale. Pertanto, non vanno pubblicati i loro nomi, né le loro fotografie, né alcun dato che ne favorisca l'identificazione, soprattutto nei casi di abuso sessuale⁸. La diffusione dei nomi di minori scomparsi richiederà l'autorizzazione espressa dell'autorità competente. Allo stesso modo, si richiede sensibilità nel trattare dispute familiari o custodie dei figli (c17).

I programmi che possono turbare l'equilibrio psicologico e morale dei minori non devono essere trasmessi in fascia protetta, cioè durante le ore di visione dei bambini. In particolare, si devono evitare contenuti che possono favorire la discriminazione, il disprezzo verso persone o gruppi, la delegittimazione delle figure genitoriali o educative, nonché la trasgressione delle norme sociali fondamentali. Sono sconsigliate anche le rappresentazioni ambigue del bene e del male (c24c).

La partecipazione dei minori ai media è soggetta a restrizioni molto severe, al fine di proteggerli da eventuali esperienze traumatiche (c20, c24b). Sebbene sia sempre richiesto il consenso dei genitori o tutori (c17), ciò non è sufficiente a legittimare qualsiasi forma di partecipazione⁹. Sono particolarmente delicate le interviste su conflitti familiari, divorzi, adozioni, rapimenti, esperienze dolorose o comportamenti delinquenziali (c16a). Solo i temi sportivi sono considerati sufficientemente innocui per la partecipazione infantile (c29b).

2. AI e privacy nell'ambiente familiare

Le sfide per la privacy familiare sono aumentate con lo sviluppo dell'intelligenza artificiale. L'estrazione massiva di dati e l'automatizzazione crescente delle decisioni richiedono una revisione e un aggiornamento dei principi etici sanciti dai professionisti dell'informazione nei rispettivi codici deontologici.

⁸ Ci sono codici che ammettono la possibilità di pubblicare tali informazioni in casi di omicidio o di crimini particolarmente gravi, oppure quando sia dimostrato che vi è un chiaro interesse pubblico (c32).

⁹ (c42d/1). Alcuni codici prevedono la possibilità di intervistare un minore nel caso in cui fosse necessario tutelarne gli interessi (c24a), oppure «se il minore si trova già sotto l'attenzione del pubblico» (c17).

L'intelligenza artificiale favorisce nuove forme di sorveglianza sulla famiglia, limitandone in alcuni casi l'autonomia decisionale. Per affrontare tali sfide, è indispensabile non solo una formazione adeguata delle famiglie, ma anche un quadro normativo etico e giuridico appropriato.

2.1. Il paradosso della casa «intelligente»

I dispositivi dell'Internet delle cose (IoT), come gli assistenti virtuali (Alexa, Google Home, Siri), le telecamere di sicurezza, gli elettrodomestici connessi e i giocattoli intelligenti, stanno trasformando la casa familiare in una «casa intelligente». Sebbene queste tecnologie offrano indubbi vantaggi in termini di comodità ed efficienza, il loro utilizzo comporta rischi significativi per la privacy della vita familiare.

Questi dispositivi raccolgono continuamente dati sulla routine, sulle abitudini, le conversazioni e le preferenze dei membri della famiglia, dati che possono essere utilizzati successivamente per personalizzare contenuti pubblicitari, condizionare l'accesso a servizi assicurativi o come prova in eventuali contenziosi. Nel 2023, l'azienda Amazon ha riconosciuto che certe registrazioni ottenute tramite Alexa erano state utilizzate per addestrare modelli di intelligenza artificiale, anche dopo che alcuni utenti avevano richiesto la cancellazione di tali registrazioni (FTC, 2023).

2.2. Valutazione delle dinamiche familiari a fini predittivi

Il funzionamento dell'intelligenza artificiale e le conclusioni a cui essa giunge non sono necessariamente oggettive né neutrali, poiché dipendono dal tipo di addestramento ricevuto e dai criteri utilizzati per definire ciò che si considera una vita familiare «normale».

Alcuni servizi sociali, giudiziari o sanitari hanno iniziato a utilizzare algoritmi per analizzare dinamiche familiari, modelli di consumo, geolocalizzazioni e attività sui social media, al fine di prevedere potenziali rischi come l'abbandono dei bambini, rotture coniugali o instabilità economica. Sistemi di punteggio algoritmico sono impiegati per classificare il livello di «stabilità» familiare, condizionando così l'accesso a prestazioni sociali, crediti bancari, mutui o assicurazioni personali¹⁰.

L'uso di questi sistemi comporta seri rischi etici. Etichettando alcune famiglie come «a rischio», gli algoritmi possono riprodurre pregiudizi strutturali, perpetuare stereotipi sociali e amplificare bias di classe, genere o etnia (Powers, Vogeli, Mullainathan, 2019; Ho, Burke, 2023). Un caso emblematico è stato lo scandalo delle frodi fiscali nei Paesi Bassi, dove un algoritmo segreto ha utilizzato variabili discriminatorie per accusare falsamente migliaia di famiglie come colpevoli di frode (Council of Europe, 2020). Negli Stati Uniti, sistemi come eScore sono stati oggetto di forti critiche per l'impiego di dati potenzialmente discriminatori nella valutazione dell'affidabilità creditizia (CoreLogic, s.d.).

¹⁰ «Redlining is an illegal practice in which lenders avoid providing services to individuals living in communities of color» (U.S. Department of Justice, 2021).

D'altra parte, molte applicazioni di «controllo parentale» si avvalgono di tecnologie IA per monitorare messaggi, geolocalizzazioni e social network degli adolescenti. Sebbene vengano presentate come strumenti di protezione, il loro uso può deteriorare la fiducia tra genitori e figli e offuscare il confine tra protezione e sorveglianza (Feldstein, 2020; FTC, 2024). Applicazioni come Bark o mSpy, che integrano riconoscimento vocale e geolocalizzazione, possono estendere pratiche di controllo occulto all'interno dell'ambiente domestico.

2.3. Deepfakes e diritto all'oblio

L'intelligenza artificiale rende più difficile mantenere l'anonimato e il diritto all'oblio, soprattutto su aspetti sensibili come le cartelle cliniche, i procedimenti giudiziari o i documenti accademici. Anche quando il nome e i dati familiari sono stati cancellati, i sistemi di IA possono identificarli nuovamente attraverso l'incrocio di banche dati e altre analisi.

L'IA generativa può riattivare contenuti legati a situazioni superate, riaprendo stigmi e compromettendo la reputazione e il benessere di persone che hanno cercato di ricostruire la propria vita. La dispersione dei dati personali e familiari su server remoti o cloud digitali impedisce agli utenti di avere un controllo effettivo sulle proprie informazioni, aumentando così il rischio di accessi indebiti o usi impropri.

L'IA consente anche la creazione di contenuti falsi con apparente veridicità (*deepfakes*) a partire da frammenti di dati autentici. Tali contenuti possono includere narrazioni fittizie, ricostruzioni di dispute familiari o scene sessualizzate manipolate. La creazione di pornografia sintetica o la modifica di immagini del passato a fini di ricatto costituiscono nuove forme di violenza digitale con un potenziale traumatico (Jondec Briones et al., 2024), soprattutto quando le vittime sono minori.

La capacità dell'IA di rendere virali i contenuti rappresenta un'ulteriore sfida: notizie che un tempo erano state pubblicate con una certa discrezione possono essere amplificate in contesti diversi dal loro scopo originario. Ad esempio, una nota su una disputa di custodia può riemergere con nuove narrazioni e intenzioni. Ci sono stati anche casi di *deepfake* che hanno ricostruito scene di reati, rendendo riconoscibili dei minori la cui identità era stata inizialmente protetta.

2.4. Controversie familiari e profilazione algoritmica

Il principio secondo cui il giornalista deve agire con delicatezza e rispetto nel trattare i conflitti familiari e le procedure relative all'affidamento dei minori diventa ancora più necessario in un contesto comunicativo influenzato dalle tecnologie di intelligenza artificiale.

Questi strumenti sono in grado di identificare modelli e dinamiche familiari a partire da una molteplicità di fonti, come social network, comunicati stampa, registri giudiziari e altri documenti pubblici legati a conflitti coniugali, divorzi o questioni di tutela. A questo insieme di informazioni si aggiungono fotografie, video e messaggi digitali condivisi, anche da terzi esterni al nucleo familiare.

Nonostante che i contenuti analizzati dall'IA siano già stati divulgati, il loro trattamento automatizzato (Periodismo automatizado, s.d.) può portare a un'amplificazione sproporzionata. Attraverso l'analisi di grandi volumi di dati, i sistemi IA possono ricostruire profili dettagliati che rischiano di stigmatizzare alcune famiglie.

Inoltre, alcuni modelli algoritmici possono generare automaticamente contenuti informativi di carattere sensazionalistico, estraendo dati da archivi giudiziari senza applicare misure adeguate per garantire l'anonimato dei minori coinvolti.

3. Sfide alla privacy dei minori

L'infanzia rappresenta il settore più esposto alle minacce contro la riservatezza della vita familiare. I rischi di re-identificazione, la perpetuazione degli stigmi e la moltiplicazione dei vettori di sorveglianza costituiscono sfide senza precedenti che richiedono una riflessione etica e giuridica approfondita. Di seguito vengono analizzati alcuni casi rappresentativi.

3.1. Reidentificazione a partire da dati anonimizzati

I codici deontologici del giornalismo europeo sottolineano la necessità di proteggere l'identità dei minori in tutte le informazioni che potrebbero condizionare il loro sviluppo personale o il loro futuro. Questa protezione prevede l'uso di tecniche come la pixellatura dei volti o l'omissione dei nomi nei contenuti grafici e testuali.

Tuttavia, i recenti progressi delle tecnologie di intelligenza artificiale hanno messo in discussione l'efficacia di queste pratiche tradizionali. Esistono infatti strumenti di riconoscimento facciale e di analisi dei dati biometrici che sono in grado di invertire i processi di anonimizzazione, permettendo la reidentificazione dei minori a partire da immagini, localizzazioni e modelli contestuali. Un caso emblematico è stato quello dell'azienda *Clearview AI*, sanzionata per aver raccolto e analizzato i volti di minori senza consenso (Euronews, 2024).

Questi algoritmi non si limitano a identificare i volti in spazi pubblici o scolastici, ma sono anche in grado di arricchire i profili ricostruiti con informazioni aggiuntive, come la geolocalizzazione, l'appartenenza a determinate istituzioni scolastiche o il contesto familiare del minore. La capacità di questi strumenti di incrociare banche dati pubbliche e private aumenta notevolmente l'esposizione dei minori, anche quando siano state adottate misure basilari di anonimizzazione.

3.2. Profilazione automatizzata ed esposizione algoritmica dei minori

Numerose applicazioni educative e ricreative progettate per i minori integrano sistemi di intelligenza artificiale in grado di raccogliere ed elaborare dati sensibili relativi alle loro abitudini, capacità cognitive, emotive e sociali. Questi sistemi consentono di costruire profili automatizzati, spesso senza che vi sia un consenso informato da parte dei genitori o dei tutori legali.

Tale trattamento algoritmico risponde a una logica commerciale che prevale sull'interesse superiore del minore. Si generano così dinamiche di ricompensa e controllo volte a incentivare il consumo, mettendo a rischio lo sviluppo emotivo e sociale dell'infanzia. È significativo che normative come la *Children's Online Privacy Protection Act* (COPPA) negli Stati Uniti proibiscano la raccolta di dati personali dei minori di tredici anni, ma non regolino con la stessa severità l'ottenimento e lo sfruttamento di informazioni inferite tramite IA, come emozioni, tratti di personalità o intenzioni comunicative (Code of Federal Regulations, 2025).

Inoltre, diverse applicazioni per l'infanzia incorporano sistemi di riconoscimento facciale o vocale che consentono di analizzare le reazioni affettive dei minori (gioia, tristezza, frustrazione) con l'obiettivo di adattare dinamicamente i contenuti offerti. Questi dati possono essere utilizzati successivamente per fini commerciali o istituzionali, ad esempio in campagne di marketing mirato. Esiste il rischio che alcuni minori vengano classificati precocemente come soggetti «problematici» o «potenzialmente trasgressivi».

3.3. Minori coinvolti in reati penali

I codici deontologici del giornalismo europeo stabiliscono l'obbligo di proteggere i minori coinvolti in fatti delittuosi, sia in qualità di vittime, che in qualità di testimoni o di presunti responsabili. In questo senso, il Codice della Federazione delle Associazioni dei Giornalisti della Spagna (FAPE) stabilisce che «il giornalista deve astenersi dall'intervistare, fotografare o registrare minori su temi legati ad attività delittuose o riconducibili all'ambito della privacy» (FAPE, s.d.).

La crescente influenza dell'intelligenza artificiale nel settore dell'informazione genera nuovi rischi che richiedono un rafforzamento della protezione dei minori. Ad esempio, i sistemi algoritmici sono in grado di estrarre informazioni da documenti giudiziari, anche dati o contenuti parzialmente anonimizzati, riuscendo in alcuni casi a identificare minori coinvolti in procedimenti penali.

La capacità dell'IA di incrociare dati sparsi, anche quando i riferimenti espliciti sono stati rimossi, aumenta significativamente il rischio di re-identificazione. Inoltre, i profili generati da questi sistemi possono includere valutazioni predittive sul comportamento futuro del minore, contribuendo così alla sua stigmatizzazione e marginalizzazione.

4. Proposte per la protezione della riservatezza familiare

Di seguito si propongono alcune linee d'azione volte a proteggere la privacy dai rischi associati all'uso dell'intelligenza artificiale nei contesti familiari e infantili.

4.1. Migliorare gli algoritmi per garantire la privacy dei minori

Il rispetto della riservatezza familiare deve orientare lo sviluppo dei sistemi, prodotti e dei servizi gestiti mediante l'IA. In questo senso, si raccomanda l'implementazione dell'approccio *Privacy by Design and by Default* (PbD), articolato in base ai

sette principi formulati da Ann Cavoukian (2020; cfr. Giannakakis, 2019). Ciò implica limitare la raccolta dei dati sui minori allo stretto necessario, garantirne una rigorosa anonimizzazione e ottenere sempre il consenso informato e verificabile da parte dei tutori legali.

Va assolutamente evitato l'uso dell'IA per classificare, monitorare o prevedere i comportamenti dei minori in aree sensibili come la salute mentale, l'orientamento sessuale o la condizione socioeconomica. Allo stesso modo, va limitata la raccolta di dati biometrici in spazi frequentati da minori, come aule scolastiche, parchi o centri ricreativi.

4.2. Meccanismi di riparazione e responsabilità

Una volta raccolti i dati, è indispensabile disporre di protocolli rigorosi per la conservazione, l'accesso e l'utilizzo degli stessi, supervisionati mediante audit periodici, obbligatori e indipendenti. Tali audit dovranno verificare il rispetto degli standard internazionali (ISO, s.d.), come la norma ISO/IEC 27090, garantire il diritto all'oblio dei minori e promuovere un'educazione digitale che permetta loro di gestire consapevolmente la propria impronta digitale.

La Legge sull'Intelligenza Artificiale dell'Unione Europea (AI Act, 2024) riconosce espressamente la necessità di valutare le applicazioni rivolte ai minori quando queste comportano un rischio elevato. La responsabilità legale degli sviluppatori aumenta in modo significativo nei casi in cui si dovessero verificarsi danni ai minori, obbligandoli a garantire una robusta anonimizzazione e a utilizzare filtri preventivi per impedire la generazione di contenuti che li menzionino o stigmatizzino. I dati giudiziari relativi a minori non devono mai essere utilizzati per l'addestramento dei modelli di IA, nemmeno a fini statistici.

La gravità delle potenziali violazioni della privacy dei minori giustifica l'imposizione di sanzioni esemplari. Inoltre, i mezzi di comunicazione e le agenzie di stampa dovranno implementare protocolli rigorosi di verifica e sistemi di allerta nei loro strumenti di IA, per garantire che i contenuti generati non includano pregiudizi (*bias*) né riferimenti inappropriati a scuole, attività extrascolastiche o indirizzi familiari.

Conclusioni

La curiosità morbosa e la commercializzazione della vita privata costituiscono una minaccia diretta alla dignità umana e allo sviluppo armonico della persona. Ognuno di noi ha bisogno di integrare in modo equilibrato le nuove possibilità offerte dalla società dell'informazione, senza che la propria comunicazione cessi di essere «incarnata», rispettosa, autenticamente umana.

La progressiva espansione dell'intelligenza artificiale sta trasformando la casa in un oggetto di interesse economico e di intrusione tecnologica. Dispositivi progettati per facilitare la vita familiare — elettrodomestici, veicoli, sensori, assistenti digitali — fanno

parte dell'Internet delle Cose (IoT), una rete che costantemente raccoglie e scambia informazioni, trasformando gli spazi più intimi della casa in fonti preziose di dati per le logiche di mercato.

In questa linea, il documento *Antiqua et nova*, elaborato dai Dicasteri per la Dottrina della Fede e per la Cultura e l'Educazione (2025), propone una riflessione etica e relazionale che invita a riumanizzare i processi tecnologici e comunicativi. La tutela della privacy familiare e, in particolare, la salvaguardia del superiore interesse dei minori deve avere la precedenza su ogni presunto vantaggio informativo o interesse commerciale. Si tratta di garantire che i bambini possano crescere senza essere esposti mediaticamente né stigmatizzati digitalmente.

È urgente ritrovare un equilibrio tra il rispetto dell'intimità personale e la necessaria vicinanza all'altro. Così come ci «togliamo i sandali» davanti al «mistero sacro dell'altro» (Francesco, 2016; cfr. *FT* 277), dobbiamo anche evitare di lasciarlo nella solitudine, nell'indifferenza e nell'anonimato. Come avverte papa Francesco in *Fratelli tutti*, «il rispetto per l'altro si sgretola» quando lo si emargina, lo si ignora e, al tempo stesso, si invade senza pudore la sua vita (*FT* 42).

L'intrusione tecnologica nella sfera domestica, anche negli spazi più intimi, richiede l'imposizione di limiti chiari e la promozione di spazi di disconnessione digitale, dove le relazioni familiari possano fiorire senza essere condizionate dalla sorveglianza o dalla quantificazione.

Dichiarazioni

Finanziamento della ricerca: La presente pubblicazione non ha ricevuto alcun finanziamento esterno.

Dichiarazione del comitato etico competente: Non applicabile.

Dichiarazione sulla disponibilità dei dati: Non applicabile.

Ringraziamenti: Non applicabile.

Conflitto di interessi: L'autore dichiara di non avere alcun conflitto di interessi relativo alla pubblicazione della presente ricerca.

Bibliografia

- AI Act. (2024). *Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)*. Recuperato da: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.
- Banning, S. A. (2020). *Standards of Work Today: Using History to Create a New Code of Journalism Ethics* [eBook]. Newcastle-upon-Tyne: Cambridge Scholars Pub.
- Carbajo-Núñez, M. (2007). Intimidad y comunicación. Bases filosófico-teológicas para un encuentro en autenticidad. *Antonianum*, 82, 637–675.

- Carbajo-Núñez, M. (2011). Informazione e Diritto all'Intimità. Una prospettiva cristiana. *Frontiere*, 8, 129–147.
- Carbajo-Núñez, M. (2012). El espectáculo de la intimidad. Raíces históricas de la comunicación centrada en el yo. *El Ágora USB*, 12(2), 449–534.
- Carbajo-Núñez, M. (2014). L'attenzione alla soggettività e l'appello alla coscienza nei codici deontologici del giornalismo europeo. in A. V. Amarante (ed.), *Fedeli alla chenosi del Redentore. Scritti in onore di Sabatino Majorano* (pp. 129–143). Bologna: EDB.
- Carbajo-Núñez, M. (2023). *La fraternità universale. Radici francescane di Fratelli tutti*. Napoli: EDI.
- Cavoukian, A. (2020). Understanding How to Implement Privacy by Design, One Step at a Time. *IEEE Consumer Electronics Magazine*, 9, 78–82.
- Code of Federal Regulations. (2025). *Part 312 – Children's Online Privacy Protection Rule* (22.04.2025). Recuperato da: <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312>.
- CoreLogic. (s.d.). *CoreLogic Score* [glossario]. Recuperato da: https://twia.msbscommercial.com/Help/Content/Resources/Glossary/CoreLogic_Score.htm.
- Council of Europe. (2020). *Netherlands – Report of the Childcare Allowance Parliamentary Inquiry Committee entitled “Unprecedented injustice” (Ongekend onrecht)* (17.12.2020). Recuperato da: [https://www.coe.int/en/web/venice-commission/-/CDL-REF\(2021\)073-e](https://www.coe.int/en/web/venice-commission/-/CDL-REF(2021)073-e).
- Dicastero per la Dottrina della Fede, Dicastero per la Cultura e l'Educazione. (2025). *Antiqua et Nova. Nota sul rapporto tra intelligenza artificiale e intelligenza umana*. Recuperato da: https://www.vatican.va/roman_curia/congregations/cfaith/documents/rc_dff_doc_20250128_antiqua-et-nova_it.html.
- Euronews. (2024). *Países Bajos multa a Clearview AI por construir una base de datos ilegal* (3.09.2024). Recuperato da: <https://es.euronews.com/next/2024/09/03/paises-bajos-multa-a-clearview-ai-por-construir-una-base-de-datos-ilegal>.
- Federación de Asociaciones de Periodistas de España (FAPE). (s.d.). *Código deontológico*. Recuperato da: <https://fape.es/home/codigo-deontologico-1/>.
- Federal Trade Commission (FTC). (2023). *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests*. Recuperato da: <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>.
- Federal Trade Commission (FTC). (2024). *Staff Report. A look behind the Screens: Examining the data practices of social media and video streaming services* (Sept. 2024). Recuperato da: https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.
- Feldman, D., Haber, E. (2020). Measuring and protecting privacy in the Always-on era. *Berkeley Technology Law Journal*, 5, 197–249.
- Feldstein, S. (2020). State surveillance and implications for children. *UNICEF Issue Brief, 1* (Aug. 2020). Recuperato da: <https://www.unicef.org/innocenti/media/1136/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf>.
- Fisher, C., Lovell, A. (2003). *Business ethics and values*. Essex: Prentice Hall.
- Francesco. (2016). Messaggio per la 50ª Giornata Mondiale delle Comunicazioni Sociali (24.01.2016). *L'Osservatore Romano*, 17 (23.01.2016), 7.
- Francesco. (2020). *Fratelli tutti. Lettera enciclica* (3.10.2020). Città del Vaticano: LEV. [AAS 112 (2020) 969–1074].
- Giannakakis, I. (2019). *Privacy by Design and By Default. A Practical Guide for the Digital Era*. Saarbrücken: LAP.
- Gunter, B. (2003). *News and the Net*. London: Routledge.
- Ho, S., Burke, G. (2023). *Child welfare algorithm faces Justice Department scrutiny* (1.02.2023). Recuperato da: <https://apnews.com/article/justice-scrutinizes-pittsburgh-child-welfare-ai-tool-4f61f45bfc3245fd2556e886c2da988b>.
- International Organization for Standardization (ISO). (s.d.). *ISO/IEC 27090*. Recuperato da: <https://www.iso.org/standard/56581.html>.

- Jondec Briones, H. P. et al. (2024). El uso ilícito de las técnicas de inteligencia artificial y la necesidad de su regulación: el deepfake. *Vniversitas Jurídica*, 73. <https://doi.org/10.11144/Javeriana.vj73.uiti>.
- Laas, K., Davis, M., Hildt, E. (edd.). (2022). *Codes of ethics and ethical guidelines: emerging technologies, changing fields* [eBook]. Cham: Springer.
- Miladi, N. (2022). *Global media ethics and the digital revolution*. London: Routledge.
- Miller, B. (2024). *Reporting by the code: journalistic ethics and responsibilities*. London: SAGE.
- Periodismo automatizado. (s.d.). in *Wikipedia*. Recuperato da: https://es.wikipedia.org/wiki/Periodismo_automatizado.
- Powers, B., Vogeli, C., Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464), 447–453.
- Singh, P. P. (2018). *European codes of journalism ethics*. New Delhi: Global Open University.
- U.S. Department of Justice. (2021). *Press release: Justice department announces new initiative to combat redlining* (22.10.2021). Recuperato da: <https://www.justice.gov/archives/opa/pr/justice-department-announces-new-initiative-combat-redlining>.