

Sicurezza online dei minori: dal COPPA 2.0 all'UK Children's Code, verso un nuovo paradigma di protezione digitale



L'evoluzione normativa internazionale sulla tutela dei minori nel cyberspazio segna il passaggio da un modello basato sul consenso genitoriale a un approccio sistemico di "privacy by design". Un'analisi tecnico-giuridica delle implicazioni per piattaforme, sviluppatori e famiglie.

Introduzione: la crisi del modello tradizionale di protezione

Il panorama della sicurezza digitale per i minori sta attraversando una trasformazione paradigmatica. Le statistiche dell'UNICEF indicano che un utente Internet su tre è un minore, mentre i dati del Pew Research Center documentano che il 95% degli adolescenti statunitensi possiede uno smartphone e il 46% dichiara di essere online "quasi costantemente".

Questa pervasività dell'esperienza digitale infantile ha reso obsoleto l'impianto normativo originario del *Children's Online Privacy Protection Act* (COPPA), approvato dal Congresso degli Stati Uniti nel 1998 ed entrato in vigore il 21 aprile 2000 attraverso la *COPPA Rule* emanata dalla Federal Trade Commission. Il framework legislativo pensato per un'era di connessioni dial-up e siti web statici si confronta oggi con ecosistemi algoritmici sofisticati, intelligenza artificiale generativa e modelli di business fondati sull'estrazione

massiva di dati comportamentali.

L'emergere di proposte legislative come il COPPA 2.0 negli Stati Uniti e l'implementazione dell'*Age Appropriate Design Code* nel Regno Unito rappresentano risposte sistemiche a questa inadeguatezza strutturale. Tuttavia, la loro analisi tecnica rivela tensioni irrisolte tra protezione dell'infanzia, innovazione tecnologica e diritti fondamentali.

Il COPPA originario: anatomia di un framework normativo

Architettura giuridica e presupposti tecnologici

Il COPPA del 1998 si fonda su tre pilastri concettuali: la soglia anagrafica dei 13 anni come discriminare per la capacità di prestare consenso digitale, l'obbligo di consenso genitoriale verificabile per la raccolta di dati personali di minori, e requisiti di trasparenza mediante privacy policy dedicate.

La *COPPA Rule* della FTC, codificata nel Title 16 del *Code of Federal Regulations* (Part 312), definisce con precisione le categorie di *personal information* tutelate: nome, indirizzo fisico, identificativi online, dati di geolocalizzazione, contenuti audiovisivi che permettano l'identificazione, e *persistent identifiers* utilizzabili per riconoscere utenti nel tempo e attraverso piattaforme diverse.

Limiti strutturali nell'ecosistema contemporaneo

L'analisi tecnica del framework originario evidenzia criticità sistemiche. In primo luogo, il meccanismo di *actual knowledge* consente alle piattaforme di evitare responsabilità

semplicemente non implementando sistemi di *age verification*, creando un incentivo perverso all'ignoranza deliberata. Il caso *United States v. Google/YouTube* del 2019, conclusosi con una sanzione di 170 milioni di dollari, ha dimostrato come piattaforme con evidenze documentali di utilizzo massivo da parte di minori potessero formalmente sostenere l'assenza di "conoscenza effettiva".

In secondo luogo, la soglia dei 13 anni, mutuata dalla psicologia evolutiva degli anni '90, non riflette le attuali evidenze neuroscientifiche sulla maturazione delle capacità di giudizio digitale. Ricerche pubblicate su *JAMA Pediatrics* documentano come le aree cerebrali preposte alla valutazione del rischio e al controllo degli impulsi continuino a svilupparsi fino ai 25 anni.

COPPA 2.0: l'evoluzione legislativa statunitense

Il Children and Teens' Online Privacy Protection Act

La proposta legislativa nota come "COPPA 2.0", formalmente denominata *Children and Teens' Online Privacy Protection Act*, introduce modifiche sostanziali all'impianto originario. Il disegno di legge, presentato al Senato e oggetto di scrutinio bipartisan, estende le protezioni alla fascia 13-16 anni, introduce il diritto alla cancellazione dei dati (*eraser button*), e vieta esplicitamente il *targeting* pubblicitario basato su dati personali di minori.

Innovazioni tecniche e obblighi di compliance

L'aspetto tecnicamente più significativo riguarda il superamento del modello *notice and consent* verso un approccio

proattivo di minimizzazione dei dati. L'articolato normativo prevede che gli operatori di servizi online diretti a minori o consapevoli della loro presenza debbano limitare la raccolta dati a quanto *strictly necessary* per la funzionalità del servizio, eliminando la legittimazione implicita derivante dal consenso genitoriale per trattamenti non essenziali.

La proposta introduce inoltre il concetto di *dark patterns prohibition*, vietando interfacce progettate per manipolare minori verso la condivisione di dati aggiuntivi. Questa disposizione richiede una ricalibrazione significativa delle pratiche UX delle piattaforme, con implicazioni per meccanismi diffusi come le notifiche push persistenti, i sistemi di gamification e le interfacce che rendono complessa l'*opt-out*.

Il *Kids Online Safety Act* (KOSA)

Parallelamente al COPPA 2.0, il *Kids Online Safety Act* rappresenta un intervento complementare focalizzato non sulla privacy ma sulla sicurezza complessiva. Il KOSA impone alle piattaforme un *duty of care* verso gli utenti minori, richiedendo misure proattive per mitigare rischi quali il cyberbullismo, la promozione di contenuti relativi a disturbi alimentari e l'esposizione a predatori online.

La convergenza tra COPPA 2.0 e KOSA delinea un modello regolatorio che integra protezione dei dati personali e sicurezza del benessere psicofisico, superando la tradizionale dicotomia tra privacy e safety.

UK *Age Appropriate Design Code*: il modello britannico

Genesi e framework istituzionale

L'*Age Appropriate Design Code*, noto anche come *Children's Code*, è stato introdotto il 2 settembre 2020 ed è diventato

pienamente applicabile dal 2 settembre 2021, al termine di un periodo di transizione di 12 mesi, sotto l'egida dell'Information Commissioner's Office (ICO). Il Codice costituisce un'applicazione settoriale del UK GDPR, specificando i requisiti di protezione dei dati per servizi *likely to be accessed by children*, definizione che abbraccia qualsiasi piattaforma che non implementi barriere efficaci all'accesso di minori.

I 15 standard del codice

L'architettura normativa si articola in quindici standard interconnessi che definiscono un framework olistico di protezione. Il principio cardine del *best interests of the child* impone che ogni decisione progettuale consideri prioritariamente l'interesse superiore del minore, in allineamento con l'Articolo 3 della Convenzione ONU sui Diritti dell'Infanzia.

Lo standard *High privacy by default* rappresenta un'inversione paradigmatica rispetto all'approccio *opt-in*: le impostazioni predefinite devono garantire il massimo livello di protezione, e qualsiasi riduzione richiede un'azione consapevole dell'utente. La *Data minimisation* va oltre il principio generale GDPR, richiedendo che la raccolta sia limitata al *minimum necessary to provide the elements of your service in which that child is actively and knowingly engaged*.

Particolare rilevanza tecnica assume lo standard *Profiling*, che vieta l'utilizzo di profilazione se non esistono misure appropriate per proteggere il minore da effetti dannosi. La profilazione a fini di marketing è soggetta a restrizioni stringenti che, di fatto, ne impediscono l'utilizzo nella maggioranza dei casi.

Enforcement e casi applicativi

L'ICO ha dimostrato un approccio *enforcement-oriented*

attraverso interventi significativi. Il report di valutazione del 2023 documenta oltre 50 verifiche di conformità (*compliance checks*) effettuate su organizzazioni, 10 audit di servizi online e 11 indagini aperte relative al *Children's Code*. La multa di 12,7 milioni di sterline comminata a TikTok nell'aprile 2023 per utilizzo illecito di dati di minori rappresenta l'azione di enforcement più rilevante finora intrapresa. Modifiche proattive da parte di piattaforme come TikTok, Instagram e YouTube in risposta alle richieste dell'ICO hanno prodotto cambiamenti globali nelle funzionalità, dimostrando l'effetto extraterritoriale *de facto* della normativa britannica.

Analisi comparativa: due modelli, un obiettivo

Convergenze strutturali

L'analisi comparata evidenzia convergenze significative tra i framework statunitense e britannico. Entrambi i modelli superano la concezione del minore come soggetto passivo la cui protezione è delegata esclusivamente ai genitori, introducendo obblighi diretti per i fornitori di servizi. Il principio di *privacy by default* e la limitazione della profilazione emergono come elementi trasversali.

La centralità del design emerge come caratteristica distintiva condivisa. Sia il COPPA 2.0 con il divieto di *dark patterns*, sia l'UK *Children's Code* con i requisiti di *age appropriate application*, riconoscono che la protezione efficace non può essere affidata esclusivamente a disclaimer legali ma deve essere incorporata nell'architettura stessa dei servizi digitali.

Divergenze metodologiche

Le differenze più significative riguardano l'approccio alla definizione del campo di applicazione. Il modello COPPA mantiene una soglia anagrafica rigida, pur elevandola dai 13 ai 16 anni. L'UK *Children's Code* adotta invece un approccio funzionale, applicandosi a qualsiasi servizio *likely to be accessed by children* indipendentemente dal target dichiarato, e richiedendo una modulazione delle protezioni in base alle fasce d'età (0-5, 6-9, 10-12, 13-15, 16-17).

Sul piano dell'enforcement, il sistema statunitense si affida a sanzioni pecuniarie amministrate dalla FTC, mentre il framework britannico integra il *Children's Code* nel più ampio sistema sanzionatorio del UK GDPR, con potenziali multe fino al 4% del fatturato globale annuo.

Implicazioni Tecniche per lo Sviluppo Software

Age Assurance: sfide e soluzioni

L'implementazione pratica di entrambi i framework richiede meccanismi affidabili di *age assurance*. L'*ICO Age Assurance Opinion* analizza metodologie che spaziano dalla *self-declaration* ai sistemi biometrici, valutandone accuratezza, proporzionalità e impatto sulla privacy.

Le tecnologie di *age estimation* basate su analisi facciale mediante machine learning sollevano questioni complesse. Da un lato offrono verifica *frictionless* che non richiede documenti d'identità; dall'altro introducono rischi di discriminazione algoritmica e implicazioni per il trattamento di dati biometrici di minori. Il Regolamento AI dell'Unione Europea classifica i sistemi di categorizzazione biometrica tra quelli ad alto rischio, richiedendo valutazioni d'impatto e supervisione umana.

Privacy-Preserving Architecture

L'architettura dei servizi digitali *compliant* richiede una riprogettazione che integri *privacy-enhancing technologies* (PETs). Tecniche come la *differential privacy* per l'analytics, la *federated learning* per modelli predittivi, e la minimizzazione mediante anonimizzazione *on-device* rappresentano soluzioni tecniche allineate ai principi normativi.

Il concetto di *data protection by design and by default*, codificato nell'Articolo 25 del GDPR, assume particolare stringenza nel contesto minorile. La documentazione tecnica del progetto LINDDUN, metodologia di *threat modeling* per la privacy, offre un framework sistematico per l'identificazione di vulnerabilità privacy in fase di design.

Il contesto europeo: DSA e GDPR

L'Articolo 28 del *Digital Services Act*

Il *Digital Services Act* dell'Unione Europea introduce all'Articolo 28 obblighi specifici per le piattaforme online accessibili a minori. Le *Very Large Online Platforms* (VLOPs) devono implementare *appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors*.

Il DSA adotta un approccio sistemico richiedendo l'integrazione della protezione dei minori nelle valutazioni del rischio sistemico (Articolo 34) e nelle strategie di mitigazione (Articolo 35). Questa integrazione supera la concezione della protezione dell'infanzia come compliance isolata, posizionandola nel quadro più ampio della governance delle piattaforme.

Sinergie con il GDPR

Il Considerando 38 del GDPR stabilisce che i minori *merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned*. L'Articolo 8 fissa a 16 anni la soglia per il consenso autonomo ai servizi della società dell'informazione, con facoltà per gli Stati membri di abbassarla fino a 13 anni.

Le Linee Guida dell'EDPB sul trattamento dei dati dei minori nel contesto dei servizi online forniscono interpretazione autorevole, enfatizzando la necessità di linguaggio *age-appropriate* nelle informative, la limitazione del legittimo interesse come base giuridica per trattamenti invasivi, e l'applicazione rigorosa del principio di minimizzazione.

Criticità e prospettive future

Tensioni con i diritti fondamentali

L'implementazione di meccanismi robusti di *age verification* solleva tensioni con principi fondamentali quali l'anonimato online e la libertà di espressione. L'Electronic Frontier Foundation ha espresso preoccupazioni circa il potenziale utilizzo di infrastrutture di *age assurance* per finalità di sorveglianza generalizzata. Il report dell'Alto Commissariato ONU per i Diritti Umani sul diritto alla privacy nell'era digitale evidenzia come misure di protezione mal calibrate possano paradossalmente esporre i minori a rischi derivanti dalla concentrazione di dati sensibili.

L'Intelligenza artificiale generativa

L'emergere di sistemi di IA generativa introduce complessità non previste dai framework normativi in analisi. Chatbot conversazionali, generatori di immagini e assistenti virtuali

creano interfacce che possono risultare particolarmente attraenti per i minori, con rischi che spaziano dalla raccolta conversazionale di dati sensibili alla generazione di contenuti inappropriati.

Il *Voluntary Commitment on AI Safety* sottoscritto dalle principali aziende tecnologiche presso la Casa Bianca include impegni specifici sulla sicurezza per i minori, ma la natura volontaria e l'assenza di meccanismi di verifica ne limitano l'efficacia.

Verso una governance globale

La frammentazione normativa tra giurisdizioni crea inefficienze e potenziali arbitraggi regolatori. Iniziative multilaterali come il *Global Online Safety Regulators Network*, che riunisce regolatori da Australia, Regno Unito, Irlanda e altri paesi, rappresentano tentativi di coordinamento che potrebbero evolvere verso standard internazionali condivisi.

Conclusioni: un cambio di paradigma necessario

L'analisi tecnico-giuridica del COPPA 2.0 e dell'UK *Children's Code* evidenzia una transizione fondamentale nella concezione della protezione digitale dell'infanzia. Il passaggio da un modello centrato sul consenso parentale a un framework che impone obblighi strutturali ai fornitori di servizi riflette la consapevolezza che, in ecosistemi digitali progettati per massimizzare l'*engagement*, la responsabilità non può ricadere esclusivamente sulle famiglie.

Le sfide implementative rimangono sostanziali: l'*age verification* solleva questioni di privacy che richiedono soluzioni tecniche innovative, la definizione di *best interests* necessita di traduzione in specifiche tecniche azionabili, e l'evoluzione rapida delle tecnologie digitali

rischia di rendere obsolete normative concepite per l'ecosistema attuale.

Tuttavia, l'emergere di un consenso trasversale tra giurisdizioni diverse sulla necessità di protezioni strutturali suggerisce che il paradigma sta effettivamente mutando. Per i professionisti della sicurezza informatica e per gli sviluppatori, questo implica la necessità di integrare la protezione dei minori non come *afterthought* di compliance ma come requisito architetturale fondamentale, al pari della sicurezza dei dati e della resilienza dei sistemi.

Il futuro della sicurezza online dei minori dipenderà dalla capacità di tradurre principi normativi elevati in implementazioni tecniche efficaci, mantenendo il delicato equilibrio tra protezione e rispetto dell'autonomia progressiva dei giovani utenti digitali.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/coppa-2-0/>