La responsabilità delle piattaforme digitali nella protezione dei minori tra normative e sfide etiche

di: EMANUELE D'EMILIO, MICHELE CILETTI, FRANCESCO ANTONIO SANTANGELO, FRANCESCO PIO SAVINO e FRANCESCA CANGELLI

Sommario

Il "Libro Bianco Media e Minori 2.0" (Agcom 2018) evidenzia che oltre un terzo dei minori tra i 9 e i 12 anni possiede un profilo su un social network, mentre molti adolescenti conoscono persone che non rispettano i limiti d'età per l'accesso ai social media. Questa realtà solleva importanti questioni legate alla protezione dei minori nell'era digitale. Il Regolamento (UE) 2016/679 (GDPR) stabilisce che solo i minori di almeno 16 anni possono fornire un consenso informato al trattamento dei dati personali online, richiedendo per i più giovani il consenso da parte dei genitori. Tuttavia, l'efficacia di queste misure è limitata dalla mancanza di strumenti di controllo adeguati. Il presente contributo, attraverso una rassegna della letteratura condotta attraverso database come IEEE, Scopus e Web of Science, mira ad analizzare le sfide poste dall'intelligenza artificiale, e le questioni cruciali in merito alla gestione della privacy dei minori online e in che modo viene effettuato il trattamento dei loro dati.

Keywords

Media Awareness, Privacy, Artificial Intelligence e Social Network

Abstract

The "White Paper on Media and Minors 2.0" (Agcom 2018) highlights that over one-third of minors aged 9 to 12 have a profile on a social network, while many adolescents know individuals who do not respect age limits for accessing social media. This reality raises important questions related to the protection of minors in the digital age. Regulation (EU) 2016/679 (GDPR) establishes that only minors aged at least 16 can provide informed consent for the processing of personal data online, requiring parental consent for younger individuals. However, the effectiveness of these measures is limited by the lack of adequate control tools. This contribution, through a literature review conducted using databases such as IEEE, Scopus, and Web of Science, aims to analyze the challenges posed by artificial intelligence and the crucial issues regarding the management of minors' online privacy and how their data is processed.

1. Introduzione

L'avvento dei social network ha trasformato radicalmente la comunicazione, con impatti rilevanti sui minori. Il "*Libro Bianco Media e Minori 2.0*" dell'Agcom (2018) segnala che oltre un terzo dei minori tra i 9 e i 12 anni ha un profilo social, nonostante il limite di età sia 13 anni. Questo divario solleva questioni etiche e legali, evidenziando la necessità di un'educazione digitale e di regolamentazioni adeguate. Tra i principali rischi figurano il cyberbullismo, la diffusione di contenuti inappropriati e le violazioni della privacy, che colpiscono soprattutto i giovani, particolarmente vulnerabili (Savino et al., 2023). Tuttavia, i social offrono anche opportunità di apprendimento, creatività e sviluppo di competenze digitali essenziali. La teoria dei "nativi digitali" (Prensky, 2001) suggerisce che i giovani abbiano un approccio diverso alla tecnologia rispetto alle generazioni precedenti, influenzando aspetti come identità, attenzione e competenze sociali (Twenge, 2017). Il concetto di "sé digitale" diventa quindi centrale nella formazione dell'identità e dell'autostima (Livingstone, 2008). I social media possono anche favorire l'autoespressione, l'apprendimento e la costruzione di legami sociali, offrendo spazi per la creatività e l'attivismo civico (Kahne et al., 2015). In questo contesto, un'educazione digitale efficace, basata su approcci come il peer-to-peer learning, è fondamentale per preparare i minori a navigare consapevolmente. La collaborazione tra istituzioni, scuole e aziende tecnologiche è cruciale per creare un ambiente digitale sicuro. Con l'avanzare delle tecnologie,

come i Large Language Models (LLMs), emergono nuove sfide che richiedono interventi regolatori mirati, per garantire un utilizzo consapevole e sicuro delle piattaforme. Ancora, secondo il rapporto ISTAT intitolato "Indagini Bambini e Ragazzi" (2023), oltre l'85% dei ragazzi tra gli 11 e i 19 anni possiede un profilo su un social network. Questo divario tra l'età legale di utilizzo e l'età effettiva di accesso solleva crescenti preoccupazioni etiche e legali, evidenziando l'urgenza di un approccio più strutturato alla regolamentazione e all'educazione digitale. I giovani, essendo più esposti rispetto alle generazioni precedenti, si trovano a fronteggiare sfide complesse legate all'uso delle piattaforme online. Tra le principali preoccupazioni figurano il cyberbullismo, la diffusione di fake news e la manipolazione delle informazioni, problematiche particolarmente gravi poiché i minori, in piena fase di sviluppo cognitivo ed emotivo, risultano più vulnerabili alla disinformazione (Durazo et al., 2023). In questo contesto, il rischio di esposizione a contenuti inappropriati, violazioni della privacy e fenomeni di cyberbullismo colpisce in modo significativo i minori, mettendo a rischio il loro benessere. Studi indicano che, già alcuni anni fa, il cyberbullismo coinvolgeva fino al 46,3% degli adolescenti, con conseguenze potenzialmente gravi sul piano psicologico e sociale (Zhu et al., 2021). Nonostante questi rischi, sarebbe riduttivo demonizzare completamente i social network, che offrono opportunità documentate per l'apprendimento, lo sviluppo della creatività e l'acquisizione di competenze digitali sempre più cruciali. Per tali motivi, il presente contributo, attraverso una rassegna della letteratura presente su IEEE, Scopus e Web of Science, si propone di approfondire le problematiche e le sfide emergenti legate all'intelligenza artificiale, con particolare attenzione alle questioni cruciali che sorgono in materia di tutela della privacy dei minori nel contesto digitale. Si intende esaminare, inoltre, i metodi e le modalità con cui avviene il trattamento dei dati personali dei minori online, soffermandosi sui potenziali rischi e sulle misure di sicurezza che devono essere adottate per garantire un'adeguata protezione. Tale analisi mira a considerare anche gli aspetti normativi e le eventuali lacune legislative, con l'obiettivo di valutare l'efficacia degli attuali strumenti giuridici nel salvaguardare i diritti dei minori in un ambiente digitale sempre più complesso e dinamico, caratterizzato dall'uso crescente di tecnologie avanzate e dall'espansione delle piattaforme online.

2. La personalizzazione dei contenuti tramite AI e i rischi per i minori

Come precedentemente evidenziato, l'evoluzione delle tecnologie di intelligenza artificiale (AI) ha apportato un impatto significativo sulla gestione dei contenuti da parte delle piattaforme digitali. Gli algoritmi impiegati, in particolare nel contesto dei social media, sono progettati per analizzare in tempo reale le preferenze, le interazioni e i comportamenti degli utenti, consentendo la creazione di flussi di contenuti altamente personalizzati. Tale meccanismo, sebbene possa risultare estremamente coinvolgente, presenta potenziali criticità, soprattutto in relazione ai minori. In tale contesto, la capacità degli algoritmi di adattare i contenuti sulla base del comportamento online dell'utente incrementa il rischio di esposizione dei minori a fenomeni di manipolazione informativa, rendendoli vulnerabili alla diffusione di disinformazione, comunemente nota come fake news. Queste ultime, spesso presentate in modo accattivante o apparentemente innocuo, possono risultare difficili da discernere per un giovane utente, specialmente in un contesto di sovraccarico informativo.

Un ulteriore aspetto critico riguarda le modalità con cui le piattaforme social personalizzano la presentazione delle notizie. I dati personali, raccolti tramite la profilazione del comportamento (ad esempio, l'interazione con contenuti quali "like", "click", "seguire" o "non seguire" specifici account, o l'uso di motori di ricerca), spesso con l'ausilio di tecnologie di AI, includono informazioni sensibili come preferenze, abitudini di navigazione e persino dati biometrici. I minori, che potrebbero non avere piena consapevolezza dei meccanismi di raccolta e utilizzo dei loro dati, risultano particolarmente esposti a queste pratiche. La trasparenza delle politiche di trattamento dei dati personali e della privacy è spesso limitata, e i meccanismi di consenso – come l'accettazione dei termini di servizio – possono risultare ambigui o difficilmente

comprensibili per un pubblico giovane. Questa situazione comporta il rischio che i minori condividano inconsapevolmente una quantità significativa di dati personali, che possono essere sfruttati non solo a fini commerciali, ma anche per influenzare il loro comportamento online (Mercenier et al., 2021). Le tecnologie basate sull'AI sollevano inoltre rilevanti questioni legate al monitoraggio e al controllo dell'accesso ai social media da parte dei minori. Le piattaforme tentano di impiegare strumenti basati sull'AI per identificare contenuti inappropriati o potenzialmente dannosi, e per prevenire l'accesso a determinati contenuti da parte dei minori. Tuttavia, questa forma di sorveglianza comporta implicazioni rilevanti per quanto concerne la protezione dei dati personali. Gli algoritmi di monitoraggio richiedono infatti un accesso costante ai comportamenti online degli utenti, inclusi quelli dei minori, il che implica una raccolta e un'analisi continua di tali dati. Tale prassi solleva preoccupazioni circa la tutela della privacy e il rischio di sfruttamento delle informazioni raccolte.

Ancora, altro elemento di complessità è dato dal fatto che le piattaforme operano spesso in giurisdizioni differenti, il che può consentire loro di aggirare i requisiti normativi locali o internazionali in materia di trattamento dei dati personali, creando una zona d'incertezza nella quale diviene difficile garantire una protezione effettiva dei diritti dei minori. Inoltre, molte tecnologie di AI, come i sistemi di raccomandazione dei contenuti, operano attraverso algoritmi opachi, il che rende difficile comprendere i meccanismi decisionali riguardanti i dati degli utenti. La problematica si aggrava ulteriormente se si considera che l'AI può essere utilizzata per identificare e sfruttare le vulnerabilità cognitive degli utenti più giovani. Gli algoritmi di machine learning, infatti, possono riconoscere pattern comportamentali che indicano fragilità emotive o difficoltà cognitive, utilizzando tali informazioni per proporre contenuti che massimizzano l'engagement, senza però necessariamente tutelare il benessere psicologico del minore. Questo può avere effetti a lungo termine sulla psiche dei giovani, influenzando la loro percezione della realtà e il modo in cui interagiscono con il mondo esterno.

3. L'avvento del GDPR e il consenso dei minori

In questo contesto, si inserisce la necessità di creare una regolamentazione che garantisca la protezione dei loro diritti alla privacy e all'uso corretto dei dati personali. Una delle principali sfide legali, infatti, riguarda il modo in cui le piattaforme digitali gestiscono l'accesso ai propri servizi da parte dei minori. Il Regolamento Generale sulla Protezione dei Dati (GDPR), in vigore dal maggio 2018, ha introdotto nuove regole per il trattamento dei dati, con particolare attenzione ai minori, i quali sono riconosciuti come soggetti vulnerabili nel mondo digitale. Sono previste, infatti, specifiche disposizioni sul consenso dei minori, stabilendo limiti d'età e responsabilità per i genitori o i tutori. Secondo i dettami del Regolamento, ogni trattamento dei dati personali deve essere basato sui principi espressi dagli articoli 5 e 6 del GDPR, i dati devono essere trattati in modo lecito, devono essere raccolti per finalità determinate, legittime ed esplicite. Il trattamento dei dati, inoltre, deve essere adeguato, pertinente e limitato a quanto necessario rispetto alle finalità del trattamento stesso. In relazione ai primi articoli del GDPR, emergono questioni critiche riguardanti la legittimità del trattamento dei dati personali. In particolare, il trattamento è considerato lecito in diverse circostanze: qualora l'interessato fornisca il proprio consenso; se necessario per l'adempimento di un contratto; per ottemperare a un obbligo legale a carico del titolare; per l'esecuzione di un compito di interesse pubblico o legato all'esercizio di pubblici poteri; per la salvaguardia degli interessi vitali dell'interessato; o infine per il perseguimento di un legittimo interesse del titolare. Una problematica centrale concerne la validità del consenso, come delineato dall'articolo 8 del GDPR; il consenso del minore è valido solo se il soggetto ha compiuto sedici anni. Di conseguenza, tutti i minori di età inferiore ai sedici anni sarebbero esclusi da questa modalità di trattamento. Tuttavia, in deroga all'articolo 8 il GDPR consente ai singoli Stati di fissare una soglia inferiore, che non sia inferiore, però, ai tredici anni. Per tale motivo il Codice della Privacy italiano, modificato dal D. Lgs. 101/2018, ha fissato questa soglia a quattordici anni (art. 2-

quinquies). Inoltre, la normativa richiede che il titolare del trattamento fornisca informazioni relative al trattamento in un linguaggio chiaro, semplice, conciso e comprensibile per il minore, affinché il consenso espresso risulti significativo. Tuttavia, tale complessità normativa può essere risolta solo se il consenso è prestato dai genitori, comportando così una significativa limitazione del diritto all'autodeterminazione del minore. La questione si complica ulteriormente in assenza di una normativa specifica riguardante l'utilizzo del metaverso (Toto, 2024), che solleva dubbi di legittimità sull'applicazione della normativa vigente. Anche in virtù dei diritti riconosciuti agli interessati dagli articoli 15-21 del GDPR, permane la preoccupazione che i genitori possano non essere in grado di tutelare adeguatamente gli interessi dei propri figli in un contesto così complesso, a causa della loro mancanza di formazione specifica in materia.

4. Il caso TikTok e le criticità del consenso informato

Per comprendere a pieno la complessità dell'argomento del consenso dei minori, si prenda ad esempio la vicenda risalente al 2021 che ha visto come protagonisti l'Autorità Garante della Protezione dei Dati Personali Irlandese e il celeberrimo social network "TikTok".
In particolare, nel 2021, l'Autorità Garante della Protezione dei Dati Personali Irlandese ha sanzionato TikTok per diverse violazioni del GDPR, focalizzandosi sul trattamento dei dati personali degli utenti minorenni e sull'acquisizione del consenso al trattamento dei dati. Inoltre, l'informativa sulla privacy fornita da TikTok è stata considerata insufficiente per garantire trasparenza, violando così l'articolo 12 del GDPR, nella parte in cui richiede che le informazioni siano fornite in modo conciso, trasparente e facilmente comprensibile, in particolare per gli utenti minorenni. Ancora, il Garante Irlandese ha ritenuto che le misure di sicurezza adottate da TikTok per proteggere i dati personali fossero inadeguate, violando l'articolo 32 del GDPR che prescrive quelle che sono le misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio. Infine, ci sono state preoccupazioni riguardo alla protezione dei diritti degli utenti, come previsto dagli articoli 15, 16 e 17 del GDPR, che trattano rispettivamente del diritto di accesso, del diritto di rettifica e del diritto di cancellazione. Tali motivi hanno portato alla decisione di sanzionare TikTok con una multa di 345 milioni di dollari, evidenziando la responsabilità delle piattaforme digitali nel garantire un ambiente sicuro e conforme alle normative per i minori (Raffiotta, 2022).
Da quanto sinora esposto appare chiaro che la crescente integrazione della tecnologia digitale nella vita dei minori ha reso urgente la necessità di una regolamentazione robusta che protegga i loro diritti alla privacy e all'uso corretto dei dati personali. Il GDPR, in vigore dal maggio 2018, ha rappresentato un passo significativo in questa direzione, introducendo disposizioni specifiche per la protezione dei minori, riconosciuti come soggetti vulnerabili nel contesto digitale. Tuttavia, la sua applicazione presenta complessità e ambiguità che sollevano questioni giuridiche importanti (Yavor, 2023). Uno dei problemi più evidenti riguarda la facilità con cui i minori possono aggirare i sistemi di verifica dell'età attualmente in uso. Basta inserire una data di nascita falsa per creare un profilo, rendendo di fatto inefficaci i meccanismi basati esclusivamente su autocertificazioni. Questo sistema non solo si dimostra inadatto a tutelare i minori, ma evidenzia anche come le piattaforme preferiscano spesso favorire una *user experience* fluida piuttosto che implementare procedure di controllo più rigorose. Le piattaforme si trovano, da un lato, la necessità di offrire agli utenti un'esperienza semplice e accessibile; dall'altro, la paura che un accesso troppo macchinoso possa disincentivare l'utilizzo della piattaforma, apparendo invasivo e complicato. Nel bilanciare questi interessi, le piattaforme tendono a privilegiare l'esperienza utente, mantenendosi il più vicino possibile ai limiti imposti dalla normativa senza però impegnarsi in misure realmente efficaci per proteggere i minori. Non va dimenticato, infatti, che l'obiettivo principale delle piattaforme rimane economico, e le normative vigenti rappresentano spesso solo dei confini entro cui operare, piuttosto che dei veri deterrenti per comportamenti irresponsabili. (Ballell, 2018). L'esempio di TikTok ha dimostrato come, in assenza di una regolamentazione adeguata, le piattaforme cerchino di ampliarsi rendendo l'accesso disponibile al pubblico più vasto possibile, inclusi i minori. Le normative attuali, nonostante gli intenti di protezione, lasciano ancora

margini troppo ampi che permettono alle piattaforme di evitare responsabilità reali. Limitare l'accesso dei minori alle piattaforme digitali deve quindi diventare una priorità per i governi, attraverso politiche nette che disincentivino le piattaforme dal raccogliere consensi in maniera superficiale, ma che richiedano di verificare l'età degli utenti in modo rigoroso e trasparente. È, inoltre, necessaria l'introduzione di sistemi di controllo più affidabili e tecnologicamente avanzati. Tra le possibili soluzioni, vi sono diverse tecnologie già disponibili che potrebbero rendere i controlli più stringenti e accurati. Queste includono:

- l'inserimento di documenti d'identità durante la registrazione, per garantire che l'utente soddisfi i requisiti di età;
- affidare l'accesso all'identità digitale, un sistema che potrebbe offrire un controllo più sicuro e personalizzato dell'accesso alle piattaforme, garantendo che i minori non possano aggirare i requisiti di età.

In questo contesto, sebbene l'AI possa svolgere un ruolo importante nel monitoraggio e nella protezione dei minori, non può essere l'unico strumento su cui fare affidamento. È fondamentale combinare l'uso di tecnologie avanzate con politiche normative più rigide e un aumento della consapevolezza digitale da parte dei genitori e dei tutori. Ad esempio, richiedere documenti di riconoscimento per creare un account potrebbe essere percepito come un'evoluzione sociale importante, ma richiede anche che i genitori e i tutori abbiano un livello sufficiente di media literacy per comprendere l'importanza della protezione dei dati online, altrimenti potrebbe avere un effetto inverso e apparire come una nuova arbitraria ingerenza delle piattaforme. Allo stesso tempo, è necessaria una volontà politica per introdurre normative più stringenti che obblighino le piattaforme a rispettare standard elevati di trasparenza e sicurezza (Capilli, 2024). Fino a quando queste misure non verranno adottate, è improbabile che le piattaforme modifichino autonomamente le loro politiche di accesso. Più realistico è pensare che le piattaforme continueranno ad operare senza apportare cambiamenti significativi, finché non saranno soggette a sanzioni che colpiscano duramente il mancato rispetto dei requisiti legali.

5. Conclusioni

In conclusione, il bilanciamento degli interessi dei minori e la loro protezione online è una sfida complessa che richiede un approccio multidimensionale. Sebbene il GDPR abbia introdotto regole importanti per la tutela della privacy, queste non si sono rivelate sufficienti a garantire la sicurezza dei minori nell'ambiente digitale in continua evoluzione. Le piattaforme digitali devono essere rese responsabili non solo attraverso normative più rigide, ma anche tramite audit periodici e una maggiore trasparenza delle loro pratiche di raccolta e trattamento dei dati. In quest'ottica anche l'educazione digitale gioca un ruolo altrettanto cruciale: genitori, tutori e istituzioni educative devono essere preparati e informati su come proteggere i minori dalle insidie del mondo digitale, formando futuri cittadini più consapevoli. Solo unendo normative solide e un'educazione diffusa sarà possibile garantire un ambiente online sicuro e protetto per le nuove generazioni (D'Agostino, 2021).

Bibliografia

- Agcom. (2018). *Libro Bianco Media e Minori 2.0*. Autorità per le Garanzie nelle Comunicazioni.
- Ballell, H. (2018). Il paradigma della responsabilità degli intermediari digitali nel contesto di una economia di piattaforme (platform economy). *Diritto comunitario e degli scambi internazionali: 1/2*, 2018, 203-221.
- Boyd, D. (2014). *It's Complicated: The Social Lives of Networked Teens*. Yale University Press.

- Buckingham, D. (2003). *Media Education: Literacy, Learning and Contemporary Culture.* John Wiley & Sons.
- Capilli, G. (2024). *Minori in rete tra consenso e verifica dell'età. Analisi comparata e proposte di adeguamento al GDPR*. MEDIA LAWS.

  D'Agostino, L. *Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di compliance.* La desinformación y la responsabilidad de las plataformas. Obligaciones y formas de compliance Disinformation and Platforms Liability. EDITORIAL BOARD, 2021.
- Di Pietro, R., & Cresci, S. (2021, December). Metaverse: Security and privacy issues. In 2021 third IEEE international conference on trust, privacy and security in intelligent systems and applications (TPS-ISA) (pp. 281-288). *IEEE*.
- GDPR, G. D. P. R. (2016). General data protection regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- Ireland Data Protection Commission. Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation. 2023.
- Istat. (2023). Rapporto ISTAT "Indagini Bambini e Ragazzi". Consultabile al seguente link: https://www.istat.it/it/files/2024/05/Bambini-e-ragazzi-2023.pdf.
- Ito, M., Gutiérrez, K., Livingstone, S., Penuel, B., Rhodes, J., Salen, K., Schor, J., Sefton-Green, J., & Watkins, S. C. (2013). Connected Learning: An Agenda for Research and Design. *Digital Media and Learning Research Hub.*
- Kahne, J., Middaugh, E., & Allen, D. (2015). Youth, new media, and the rise of participatory politics. *From voice to influence: Understanding citizenship in a digital age*, 35.
- Livingstone, S. (2008). Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-expression. *New Media & Society*, 10(3), 393411.
- Mercenier, Heidi & Wiard, Victor & Dufrasne, Marie. (2021). Teens, Social Media, and Fake News: A User's Perspective. 10.1002/9781119743347.ch12.
- Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon*, 9(5), 1-6.
- Raffiotta, E. C., & Baroni, M. (2022). Intelligenza artificiale, strumenti di identificazione e tutela dell'identità. *BioLaw Journal-Rivista di BioDiritto*, (1), 165-179.
- Raghavendra, P., Newman, L., Grace, E., & Wood, D. (2013). 'I Could Never Do That Before': Effectiveness of a Tailored Internet Support Intervention to Increase the Social Participation of Youth with Disabilities. *Child: Care, Health and Development*, 39(4), 552-561.
- Savino, F. P., De Santis, A., D'Emilio, E., & Monacis, D. (2023). Digital literacy e digital divide: due facce della stessa medaglia. *MIZAR*, *18*, 101-113.

- Twenge, J. M. (2017). iGen: Why Today's Super-Connected Kids Are Growing Up Less Rebellious, More Tolerant, Less Happy–and Completely Unprepared for Adulthood–and What That Means for the Rest of Us. Simon and Schuster.
- Toto, G. A. (2024). *Verso 1 Meta*. FrancoAngeli.
- Valkenburg, P. M., Peter, J., & Walther, J. B. (2017). Media Effects: Theory and Research. *Annual Review of Psychology*, 67(1), 315-338.

  Yavor, Olha & Piddubna, Viktoriia & Ruban, Olena. (2023). Legal concerns regarding the protection of minors' personal data in compliance with national legislation and GDPR requirements. *ScienceRise: Juridical Science*. 23-34. 10.15587/2523-4153.2023.286647.
- Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures. *Frontiers in Public Health*, 9.
- Zozaya Durazo, Luisa & Sádaba, Charo & Feijoo, Beatriz. (2023). "Fake or not, I'm sharing it": teen perception about disinformation in social networks. *Young Consumers*. 25. 10.1108/YC-06-20221552.

EMANUELE D'EMILIO

Emanuele D'Emilio è un Dottorando di Ricerca iscritto al dottorato nazionale in "Learning Science And Digital Technologies". I suoi ambiti di ricerca consistono principalmente sul Diritto D'Autore e Copyright, applicati nel contesto della Scienza Aperta.

MICHELE CILETTI

Michele Ciletti studia e fa ricerca nell'ambito delle Digital Humanities. Laureato in Lettere e Cultura Digitale, collabora con il Learning Sciences institute dell'Università di Foggia. Tra i suoi interessi di ricerca ci sono gli studi letterari digitali, il text mining, l'interazione uomo-macchina, la citizen science, il public engagement e le tecnologie per l'educazione.

FRANCESCO ANTONIO SANTANGELO

Francesco Antonio Santangelo è sviluppatore web e docente universitario. Laureato in ingegneria informatica, cura da diversi anni la progettazione web e grafica di importanti aziende, nonché di portali e piattaforme digitali di e-commerce ed e-learning. È specializzato nello sviluppo frontend, con particolare attenzione all'interfaccia utente, all'usabilità e all'accessibilità. Appassionato di tecnologie web ed impegnato nel garantire esperienze digitali inclusive, segue rigorosamente gli standard di settore per creare soluzioni efficienti ed accessibili. La sua missione è migliorare l'interazione tra persone e tecnologie attraverso un design semplice e funzionale

FRANCESCO PIO SAVINO

Francesco Pio Savino è Dottorando di Ricerca in "Learning Sciences and Digital Technologies", laureato in Scienze Giuridiche della Sicurezza e specializzato nel settore della privacy; si occupa di tematiche relative alla privacy applicata nell'ambito scolastico. Il suo principale tema di ricerca riguarda nuovi metodi efficaci per aumentare la digital literacy della popolazione in generale, con un focus particolare sui minori.

FRANCESCA CANGELLI

Francesca Cangelli è docente ordinaria di Diritto Amministrativo presso l'Università di Foggia, dove ha ricoperto anche il ruolo di Pro-Rettore Vicario. Laureata in Giurisprudenza alla LUISS di Roma, ha conseguito un PhD presso l'Università di Ferrara e ha svolto parte della sua formazione accademica presso il University College of London e l'Institute of Advanced Legal Studies di Londra.