

RISOLUZIONE

Dei sottoscritti Consiglieri del Gruppo Lega Salvini Emilia – Romagna

Premesso che

- La sicurezza in rete dei minori è un tema complesso che coinvolge a cascata le istituzioni di ogni livello. Numerose sono le iniziative volte alla definizione di policy e best practice per tentare di arginare i fenomeni connessi al rapporto, ormai morbosissimo, che i minori hanno con il mondo digitale con il quale entrano in confidenza prima ancora della scolarizzazione;
- Il Ministero dello Sviluppo Economico ha espresso la sua posizione sottolineando l'importanza, in un panorama mediatico sempre più ibrido e integrato, del rispetto dell'equilibrio tra la dimensione produttiva-economica e quella etica e delle implicazioni dei messaggi mediali sui minori (<https://www.mise.gov.it/index.php/it/notizie-stampa/avviato-percorso-condiviso-per-la-tutela-dei-minori-sulle-multiplatforme-digitali>);
- In data 8 dicembre 2020, i ministri responsabili di tutti gli Stati membri dell'UE hanno apposto la loro firma sulla Dichiarazione di Berlino, la quale fa un ulteriore passo avanti rispetto ai principi di centralità dell'utente formulati nella Dichiarazione di Tallinn, rafforzando il ruolo pionieristico delle amministrazioni pubbliche nel guidare la trasformazione digitale basata sul valore delle nostre società europee. La Dichiarazione di Tallinn sull'eGovernment approvò i principi chiave per i servizi pubblici digitali proposti nell'eGovernment Action Plan 2016-2020. La Dichiarazione definisce sette principi chiave con relative linee d'azione politiche a livello nazionale ed europeo:
 - a) Validità e rispetto dei diritti fondamentali e dei valori democratici in ambito digitale;
 - b) Partecipazione sociale e inclusione digitale per plasmare il mondo digitale;
 - c) Empowerment e alfabetizzazione digitale, permettendo a tutti i cittadini di partecipare alla sfera digitale;
 - d) Fiducia e sicurezza nelle interazioni tra i governi digitali, per permettere a tutti di navigare nel mondo digitale in modo sicuro, di autenticarsi e di essere riconosciuti digitalmente all'interno dell'UE;
 - e) sovranità digitale e interoperabilità, come chiave per garantire la capacità dei cittadini e delle pubbliche amministrazioni di prendere decisioni e agire in modo autodeterminato nel mondo digitale;
 - f) Sistemi centrati sull'uomo e tecnologie innovative nel settore pubblico, che rafforzino il suo ruolo pionieristico nella progettazione di tecnologie sicure e affidabili;
 - g) Una società digitale resiliente e sostenibile, che sia in linea con il Green Deal e che utilizzi le tecnologie digitali per migliorare la sostenibilità dei nostri sistemi sanitari.
 - h) <https://www.assemblea.emr.it/europedirect/news/2020/le-amministrazioni-pubbliche-e-la-trasformazione-digitale-firmata-la-dichiarazione-di-berlino-sulla-societa-digitale-e-il-governo-digitale-basato-sul-valore>

Premesso inoltre che

I social media possono essere descritti come un caso speciale di tecnologia persuasiva in cui le leve psicologiche vengono intaccate e spronate più e più volte, spesso senza la consapevolezza dell'utente. Non "si clicca" casualmente: molti progetti sfruttano deliberatamente le vulnerabilità umane più profonde promuovendo comportamenti compulsivi che compromettono la autonomia e il benessere dell'individuo;

Dalla raccolta e analisi dei dati, un algoritmo elabora la strategia in grado di strumentalizzare la mente umana, creando dipendenza da un lato e rischiando di portare a scelte estreme dall'altro, con la stessa logica delle dipendenze da droga o, esempio ancor più evocativo, da GAP: tra le dipendenze 3.0, quelle tecnologiche sono oggi molto frequenti, con la conseguente pericolosa inversione delle dinamiche relazionali che la stessa fase web 3.0 ha generato.

Considerato che

Tra i molteplici fattori di rischio in cui incorre la generalità degli utenti "della rete", circostanza tanto più vera e perniciosa quando applicata ai minori, vale la pena qui soffermarsi sui seguenti:

- **Dare valore al banale facendolo sembrare "urgente":** ad esempio con le "notifiche" dei social (vibrazioni, punti rossi, luci lampeggianti, banner) che il più delle volte fungono da falsi allarmi, compromettendo la capacità di occuparsi di ciò che è importante;
- **Incoraggiare la ricerca senza adempimento:** con il risultato di continuare a fare clic e scorrere, consumando inutilmente contenuti, con un comportamento che ci esaurisce, ma alimenta modelli di business basati sul coinvolgimento inconsapevole.
- **Costringere al multitasking:** Le risorse del cervello sono limitate: essendo creature altamente distraibili la qualità della nostra attenzione può essere facilmente compromessa. Nel cambiare spesso l'attenzione da un compito all'altro, si sperimenta un "residuo di attenzione" in cui i pensieri sul compito precedente interferiscono con la piena attenzione al compito attuale. I social media ispirano questo multitasking: queste piattaforme tengono gli utenti continuamente impegnati, innescando comportamenti ripetitivi e automatizzati e indebolendo l'attivazione nelle regioni prefrontali di controllo cognitivo del cervello. Un gruppo di lavoro della National Academy of Sciences ha scoperto che il multitasking dei media tra i giovani e giovanissimi è associato a una memoria più povera, a una maggiore impulsività e a cambiamenti nella funzione cerebrale. Queste prove devono indurre a essere cauti ed evitare di inondare/sollecitare continuamente tutti i canali del cervello.
- **Innescare paura e ansia:** Secondo i ricercatori, le informazioni negative raccolgono più attenzione e modellano le emozioni e il comportamento in modo più potente delle informazioni positive. Non sorprende che i contenuti dei social

media che generano paura, rabbia e disgusto si diffondano molto più velocemente dei contenuti positivi.

- **Spronare a un confronto sociale costante:** L'abitudine umana a misurarsi contro gli altri a volte ispira a migliorarsi, ma i confronti più comunemente portano a emozioni negative: invidia, vergogna, ansia o presunzione. I social media aumentano drasticamente la portata e la posta in gioco nei nostri confronti, e oggi in particolare con giovani e giovanissimi sono gli influencer a stabilire standard di eccellenza: si sentono spronati a collegare la propria immagine a quegli ideali. I "like" ricevuti - che attivano potenti circuiti di ricompensa nel cervello - diventano un commento sulla parte più profonda di sé stessi.
- **Raccontarci quello che vogliamo credere ("ti dico io quello che tu pensi"):** il cervello umano è sensibilissimo ai meccanismi di esclusione sociale. Gli algoritmi intercettano le preferenze, profilando e personalizzando le informazioni che vengono ricevute. Quando sono gli algoritmi a definire "cosa" si vuole credere, si diventa più polarizzati, perdendo il senso di sé stessi quale gruppo sociale coeso con comprensione condivisa.

Considerato altresì che

Per quanto attiene in modo specifico la tutela dei minori on line si ritiene che debbano essere contemplate sostanzialmente due ordini di questioni:

1. **Validità del consenso prestato** dal minore per l'accesso ai servizi (questione di ordine formale, ma che si declina in ordine sostanziale) e meccanismi di Age Verification: i profili di vulnerabilità dei minori sono prevalentemente connessi alla difficoltà di discernere il significato e le conseguenze di ciò che agli stessi viene proposto o suggerito, e alla mancanza/carenza di capacità di attivare un pensiero critico. Tali aspetti sono stati presi in considerazione dell'European data protection board sotto più profili. **Il Considerando del GDPR**, al n. 38, sancisce chiaramente che "I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore."

Sotto il profilo della validità del consenso prestato dal minore l'EDPB sostiene che "Nel fornire servizi della società dell'informazione ai minori sulla base del consenso, il titolare del trattamento dovrà compiere ogni ragionevole sforzo per verificare che l'utente abbia raggiunto l'età del consenso digitale, e le misure dovrebbero essere proporzionate alla natura e ai rischi delle attività di trattamento" (Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679 vers. 1.1). Sforzi che devono essere tanto più dettagliati quanto più il rischio connesso al trattamento è alto, e che devono essere realizzati prima dell'inizio del trattamento, in un'ottica conforme al principio di data protection by design. A titolo esemplificativo si rammenta che proprio questo principio

costituisce il punto centrale del **provvedimento** emanato dal Garante per la protezione dati il 22 gennaio 2021 nei confronti di **Tik Tok**, con il quale, ha disposto “la misura della limitazione provvisoria del trattamento, vietando l’ulteriore trattamento dei dati degli utenti che si trovano sul territorio italiano per i quali non vi sia assoluta certezza dell’età e, conseguentemente, del rispetto delle disposizioni collegate al requisito anagrafico”.

Sotto il profilo tecnico sicuramente l’adozione di meccanismi di age verification può costituire una misura astrattamente idonea a impedire l’accesso ai minori a determinati contenuti, ma è fondamentale che il meccanismo non sia in qualche modo “aggirabile” da parte del giovane utente;

2. **Educazione digitale:** quale sia la modalità di effettiva e concreta tutela dei minori nella relazione con servizi/attività on line, e come evitare che la tecnologia digital persuasiva orientata a questo target precipuo (minori, in primis pre-adolescenti) possa tradursi in una minaccia esistenziale. La necessità di tutelare il minore sorge sin dal momento in cui quest’ultimo maneggia un dispositivo con accesso a internet, in quanto la semplice possibilità di navigare in rete dà al minore la possibilità di visualizzare una serie di contenuti non protetti, scandalosi, talvolta macabri oltre che pericolosi per la sua crescita e per la sua integrità psico fisica. In molte piattaforme i contenuti sono visibili da ciascun utente, non richiedendo infatti alcuna registrazione al sito.

La molteplicità delle interazioni, connessa alla vulnerabilità e alla plasmabilità psicologica del minore, spesso orientata a guardare al “web” come vita reale ricca di amicizie e nuove emozioni, a scapito della vita materiale, sempre più vuota e noiosa (durante la fase più dura delle misure di distanziamento sociale si è assistito ad un incremento esponenziale di questo fenomeno), possono essere il veicolo per pedofili e malintenzionati, oltre che per l’emulazione di “challenge” nocive spesso lanciate per il soddisfacimento di sadiche ambizioni.

IMPEGNANO

Il Presidente e la Giunta Regionale

- A far propria la necessità di dare piena rappresentanza ed investimento tramite apposito strumento legislativo ai bisogni educativi digitali dei minori, definendo un proprio modello di alfabetizzazione ed educazione digitale adeguato all’età, incentrato su abilità e competenze per garantire che i minori siano attrezzati per identificare le minacce e possano comprendere appieno le implicazioni del loro comportamento online;
- a promuovere l’educazione civica digitale come strumento a tutela dell’integrità psicofisica dei minori riconoscendo il diritto alla protezione dei propri dati, all’oblio digitale e al diritto all’utilizzo consapevole delle tecnologie informatiche e della rete internet;
- a sollecitare nelle sedi opportune e per quanto di competenza un intervento unitario dell’EDPB che potrebbe consistere nell’adozione di linee guida per la tutela dei minori su internet e sui social network, per far sì che le misure di tutela

e i meccanismi di age verification che verranno adottati possano essere non solo idonei ad assicurare una adeguata tutela dei giovani utenti, ma rispondenti ad una logica coordinata e armonizzata della protezione dei minori su internet.