Fronte comune sulla soglia

Consulenti, esperti privacy e associazionismo di settore schierati per una soglia di almeno 14 anni per iscriversi da solo a un social network. È il risultato di un sondaggio di Federprivacy effettuato in 107 province italiane su un campione di 2975 partecipanti.

I risultati, ottenuti intervistando professionisti della privacy ed enti del privato sociale impegnati nella cura dei minori, non sono poi così distanti dai risultati di una ricerca svolta per la Polizia di stato da Generazioni Connesse, il Safer internet center italiano, coordinato dal ministero dell'istruzione, curata da Skuola.net, Università degli Studi di Firenze e Sapienza Università di Roma - Cirmpa.

Quest'ultima indagine ha coinvolto una platea diversa (2.475 adolescenti delle scuole secondarie), per i quali l'età giusta per iniziare a utilizzare i social network da soli, con un proprio account, è 14 anni. Entrambe le ricerche, sia quelle tra professionisti e associazioni sia quelle con gli interessati, evidenziano che i più piccoli non possono essere lasciati solo davanti a uno schermo.

Si tratta, comunque, di risultati da inserire in un quadro complesso, descritto così da **Nicola Bernardi**, presidente di Federprivacy: «Negli ultimi decenni i social network di maggiore successo hanno raggiunto fatturati annui da miliardi di dollari offrendo servizi apparentemente gratuiti agli utenti, ma in realtà quando ci iscriviamo a un social paghiamo con i nostri dati personali, che vengono spesso sfruttati in modo indiscriminato per finalità di marketing e altri scopi poco trasparenti che un adulto esperto e maturo non riesce a comprendere pienamente neanche se si prende il tempo per leggere le lunghissime e complicate informative sulla privacy che gli vengono sottoposte quando intende aprire un account. La faccenda diventa ancora più pericolosa quando a poter ottenere qualcosa di gratis con un semplice click è una persona inesperta e vulnerabile come lo è un bambino, che navigando sul web si trova di fronte a una sorta di «paese dei balocchi» in cui non è tutto oro quello che luccica». In sostanza il mondo del web ha bisogno di regole, a maggior ragione quando si tratta di bambini. Spiega Bernardi: «Purtroppo osserviamo che allo stato attuale il web non si presenta come un ambiente sicuro di cui gli utenti possono avere fiducia, ma come una specie di giungla in cui il pericolo è sempre dietro l'angolo, specialmente per i minori. In molti casi app e social vengono presentati a bambini e adolescenti come innocui giochi e passatempi, ma spesso raccolgono massivamente informazioni profilando su larga scala i loro comportamenti online senza rispettare pienamente le regole. Una nostra ricerca ha evidenziato che il 93,8% delle app rivolte ai bambini contengono tracker che li spiano e quasi la metà di queste trasferiscono i dati in paesi non sicuri per la privacy, ma nell'87% dei casi non vengono neanche pubblicati i contatti di un Data protection officer a cui un genitore avrebbe diritto di rivolgersi per tutelare il proprio figlio». Peraltro, alcuni social continuano a indicare in 13 anni la soglia minima per usare una piattaforma social, ma in controtendenza con le aspettative dei professionisti del settore e con la società civile. Prosegue Bernardi: «Il recente intervento del Garante della privacy su TikTok e la campagna informativa dell'autorità per sensibilizzare i genitori rappresentano un importante primo passo per la tutela dei minori on-line. Tuttavia ciò non toglie le legittime preoccupazioni e le perplessità di chi ha a cuore il benessere psicofisico dei propri bambini, e nel sondaggio che abbiamo condotto assieme ai nostri delegati in 107 province italiane abbiamo riscontrato che il 95,3% dei genitori intervistati non è d'accordo sul fatto che ai loro figlio basti aver compiuto 13 anni per iscriversi da solo a un social network. Anzi, nel 68,5% dei casi riterrebbe giusto attendere che abbia compiuto 16 anni per consentirglielo». Ma controllare l'età di chi clicca non è certo facile. La ricerca della Polizia postale evidenzia i consigli suggeriti direttamente dagli utenti alle piattaforme social per controllare l'identità di chi accede: solo per 1 su 5 basterebbero solo delle raccomandazioni. Per gli altri servirebbero ben altro tipo di verifiche, come il controllo del documento di identità (1 su 3), sistemi di identità digitale certificata (1 su 3) o di intelligenza artificiale per riconoscere l'età dell'utilizzatore (1 su 4), oppure il patentino (1 su 5).

Ma i pericoli di una facile elusione sono dietro l'angolo. Conclude Bernardi: «Allo stato attuale basta veramente poco a un bambino che abbia anche meno di 13 anni per aggirare i blandi sistemi di controllo dei social in cui basta dichiarare di avere un'età maggiore per riuscire a iscriversi senza alcuna vera barriera. Ovviamente, spetta ai genitori la principale responsabilità di vigilare sui propri figli, ma di fronte a un permissivismo generalizzato è comprensibile che anche i più premurosi si trovino arresi».

Le app nascondono insidie e tranelli per i piccoli

Le app per i bambini contengono pubblicità; quasi tutte tracciano i piccoli utenti e usano strumenti a distanza per controllare i loro telefonini e computer. Gran parte dei gestori delle app hanno sede all'estero, in paesi in cui non ci sono valide leggi sulla privacy, e non hanno un responsabile della protezione dei dati. È la sintesi della ricerca elaborata da Federprivacy. Ecco altri dettagli.

App. **Federprivacy ha analizzato un campione di 500 app giochi disponibili nel Google Play Store, che dichiarano di essere adatte anche alla fascia dei più piccoli: l'85% ha un indice Pegi inferiore a 7, cioè si tratta di applicazioni con contenuti che si dichiarano adeguati a bambini di età inferiore a 8 anni. Le app campione, considerando il numero dei download, risultano tra le più diffuse tra i minori. Infatti solo nel 6% dei casi hanno un numero di download inferiore al milione, per il restante 94% il numero di scaricamenti è maggiore con punte superiori a 50 milioni nel 34% dei casi analizzati.**

Pubblicità. **Anche se dichiaratamente adatte ai più piccolini, tutte le app hanno pubblicità. Delle 500 analizzate, 479 (il 96%) presentano annunci pubblicitari.**

Tracker. **I minori sono schedati e tracciati nella navigazione online. Nella maggioranza delle applicazioni (94%) è presente almeno un tracker, cioè un meccanismo che ti scheda, ti profila e ti geolocalizza. Inoltre, se consideriamo il numero di tracker, nel 62% delle app sono presenti da 6 a 20 tracker. Nelle 500 app analizzate sono stati riscontrati 4.860 tracker che corrispondono a un valore medio di 9,72 tracker per singola applicazione. I tracker di Google risultano presenti nella maggioranza dei casi (92%) mentre quelli di Facebook superano la metà (54%).**

Permessi. **Le app usate aprono le porte per controllare computer e dispositivi, tramite i cosiddetti permessi, con i quali si consente al gestore delle app di accedere alla posizione segnalata dal telefonino, alla rubrica, ai contatti, ai file, al microfono, alla funzione vibrazione, alla fotocamera e così via. Nella quasi totalità delle applicazioni (99,6%) è presente almeno una richiesta di permesso al dispositivo. Se si considera il numero di permessi più dell'80% delle app hanno più di 10 permessi. Nelle 500 app analizzate sono stati riscontrati 5.108 permessi che corrispondono a un valore medio di 10,2 per singola applicazione.**

Paesi non sicuri. **Federprivacy ha seguito a ritroso le app per accertare i paesi in cui vengono sviluppate e, di conseguenza, trattati i dati. Nel 42% del totale le aziende sviluppatrici hanno sede in paesi considerati non sicuri rispetto alla privacy. Ai posti Stati Uniti (11%), Cina (4,6%) e Singapore (2,4%).**

Dpo. **La quasi totalità delle app (oltre il 90%) fornisce una qualche informativa sulla privacy comprensiva di contatti, ma si evidenzia una diffusa mancanza di un Data protection officer (87%), cioè il responsabile della protezione dei dati, e cioè un supervisore, previsto dal regolamento Ue sulla privacy.**

Il marketing deve stare alla larga

Un bambino non può dare il consenso all'uso dei suoi dati per marketing, ricerche di mercato, profilazione e vendita diretta. Certo in base alla legge, per dare il consenso a trattare i dati (purché non si debba stipulare un contratto) in Italia, il limite minimo è 14 anni.

Ma questo consenso del quattordicenne, stando all'articolo 8 del Gdpr e all'articolo 2-quinquies del Codice della privacy, copre il trattamento dei dati riguardante l'offerta diretta di servizi della società dell'informazione ai minori. Non copre il marketing. L'offerta diretta di un servizio, infatti, per quanto si cerchi di estendere il significato della parole, non vuol dire marketing e simili. La conclusione è che chi elabora dati di bambini per marketing e, magari, costruisca profili commerciali, viola il regolamento Ue sulla privacy.

Commette una violazione del Gdpr e del codice della privacy italiano anche chi, limitandosi alla offerta di servizi online, tratta, senza consenso dei genitori, dati di bambini di età minore di 14 anni. Stessa violazione c'è per chi pretende di trattare dati di un minore di 18 anni sulla base di un contratto concluso dal solo minorenne.

Chi fa una di queste cose accetta il rischio giuridico di una causa per invalidità del contratto e per invalidità del consenso e conseguente richiesta di risarcimento del danno (anche immateriali). E tutte queste cause sono di competenza del giudice italiano (articolo 10 del dlgs 150/2011).

Peraltro, c'è anche una tesi che sostiene che tutte le volte in cui si verifica uno scambio di «servizi contro dati» si conclude un contratto (vedasi Tribunale amministrativo regionale per il Lazio, sezione prima, sentenza n. 261/2020): stando a questa tesi tutte le volte che un minore di età aderisce a una app online, anche quelle gratuite, si conclude un contratto, con la conseguenza che, in Italia, in applicazione dell'ultimo paragrafo dell'articolo 8 Gdpr, si conclude un contratto ogni volta che taluno acconsenta al trattamento del dato. Se non si vuole aderire a questa tesi (limite di 18 anni per andare su internet), bisogna comunque limitare la possibilità per il maggiore di 14 anni di dare il consenso. L'ultraquattordicenne dovrebbe avere capacità di dare da solo il consenso «privacy», ma solo per due tipi di servizi: 1) servizi che non sono l'oggetto di un accordo; 2) servizi che sono palesemente rivolti alla sua crescita, alla sua educazione e alla sua maturazione.

L'imprenditore online che si rivolge ai bambini deve impostare il servizio ed evitare di strutturare il rapporto come un accordo che preveda il sorgere di obbligazioni, anche eventualmente a carico di una sola parte. L'imprenditore non deve avere i dati come corrispettivo («pagamento») del servizio, ma solo per ragioni collegati alla fruibilità del servizio. Quello stesso imprenditore, infine, nell'ambito della documentazione privacy aziendale, deve assumersi la responsabilità di dichiarare se il trattamento dei dati del minore avvenga o non avvenga nell'ambito di un accordo contrattuale.