App e nuove tecnologie.
Quali rischi per i dati personali?

Relazione:

App ludiche e di intrattenimento. Come tutelare i minori?

Avv. Daniela Bianchini – Componente Commissione Privacy

Studio Legale Bianchini Jesurum

www.bianchinijesurum.it

Cosa sono le app?

- Da circa un decennio le app sono entrate a far parte della quotidianità di un numero sempre maggiore di persone. **Si tratta di programmi molto facili da installare** - in particolare sui dispositivi mobili come smartphone e tablet - e che offrono diverse funzioni: messaggistica, intrattenimento, giochi, operazioni bancarie, fitness, acquisti on line, prenotazione di servizi vari (es. car sharing o bike sharing), calcolo dei percorsi in auto o a piedi e molte altre.
- Ci sono persino app per liberarsi dalla dipendenze
- Il mercato è in sostanza controllato da Google e da Apple, i gestori dei due store che mettono a disposizione le app: Apple per i dispositivi con sistema iOS e Google Play per quelli con sistema Android.
- Per scaricare l'app desiderata basta andare sull'app store presente in ogni dispositivo, scegliere il programma desiderato e cliccare su "installa". Molte tra le app più diffuse sono gratuite, quindi non occorre neppure eseguire il passaggio del pagamento: basta accettare le condizioni del fornitore del programma e nel giro di pochi secondi l'app viene installata sul dispositivo ed è pronta per essere utilizzata.

Sembra tutto molto facile e per di più nella maggior parte dei casi è gratuito. Tuttavia la realtà è ben diversa.

Innanzitutto bisogna essere consapevoli che non si tratta di una vera e propria "gratuità", in quanto il fornitore del servizio riceve sempre quale "corrispettivo" i dati personali dell'utente, una "merce" che per le aziende è sempre più preziosa per fini commerciali.

La società "*appificata*"

Nel corso della 35° Conferenza internazionale dei Garanti privacy (Varsavia, settembre 2013) è stato sollevato il problema dei rischi delle app per la grande quantità di dati personali raccolti

Il Garante privacy italiano è intervenuto più volte, sollecitando gli utenti a prestare una maggiore attenzione, sia nel navigare in Rete che nello scaricare app sui propri dispositivi Cfr. "APProva di privacy. Suggerimenti per usare le app proteggendo i propri dati" (ottobre 2020)

"Le app facilitano e vivacizzano molte delle attività che svolgiamo giornalmente; allo stesso tempo, le app raccolgono anche una grande mole di informazioni personali. Tutto ciò permette un monitoraggio digitale permanente, mentre gli utenti spesso non ne hanno consapevolezza né ne conoscono i fini ultimi". "È fondamentale" – si legge ancora nel documento citato – "*che gli utenti abbiano e continuino ad avere il controllo dei propri dati. Devono poter decidere quali informazioni condividere, con chi condividerle e per quali finalità*"

(Cfr. *Dichiarazione di Varsavia sulla "appificazione" della società*, 2013)

Il pericolo in un “click”

- Nonostante siano passati diversi anni dalla Conferenza di Varsavia, e nonostante i continui inviti alla prudenza da parte del Garante privacy e anche della Polizia Postale, ancora oggi sono numerose le vittime, spesso inconsapevoli, di un trattamento illecito dei propri dati da parte dei gestori delle app.
- È fondamentale capire ***quanti*** e ***quali*** dati verranno raccolti e ***come*** verranno utilizzati, leggendo attentamente l’informativa sul trattamento dei dati personali
- È scorretta e pericolosa l’abitudine diffusa di cliccare su “accetta” senza leggere le condizioni di uso. In particolare, bisogna diffidare di quelle app che non rispettano **il principio della minimizzazione dei dati** (Art. 5, lett. c del GDPR):
- I fornitori dovrebbero richiedere solo i dati strettamente necessari per l’erogazione del servizio. È quindi molto importante sapere per cosa viene prestato il consenso.

Quali possono essere in concreto i pericoli?

- Di recente la Polizia Postale ha rilevato che sono in aumento i furti di account attraverso le richieste di invio codici pervenute da contatti dell'utente (che però sono del tutto ignari della truffa in atto). I codici vengono inviati alle vittime e poi si chiede loro di inoltrarli di nuovo al mittente, con una scusa.
- Il codice richiesto, una volta inviato, consente ai cybercriminali di impadronirsi dell'account WhatsApp ed utilizzare liberamente il servizio di messaggistica istantanea per compiere ulteriori frodi, attraverso il numero di telefono della vittima, nonché di avere accesso ai contatti salvati nella rubrica, con tutte le immaginabili conseguenze (es. richieste di invio foto o file)

Qualche dato statistico…

Cfr. Osservazioni AGIA sullo schema di regolamento Agcom per la classificazione di opere audiovisive destinate al web e dei videogiochi (06/06/2018)

- Le app più scaricate sono quelle ludiche, seguite dalle app social, di messaggistica e di intrattenimento: tutte app che interessano anche i minori.
- In numerosi videogiochi per smartphone sono stati rinvenuti, al loro interno, codici relativi ad altre società destinatarie dei dati degli utenti, all'insaputa di questi ultimi

- Secondo un' indagine del 2020 condotta dall'Osservatorio di Federprivacy – la principale associazione italiana che ha tra i suoi obiettivi quello di promuovere il rispetto della normativa in materia di privacy – **circa l'87% delle app fra quelle maggiormente utilizzate non rispettano il Regolamento europeo in materia di privacy** (GDPR), ad esempio con riferimento alla nomina del *Data Protection Officer*, vale a dire il responsabile della protezione dei dati previsto espressamente dagli artt. 37 e ss. del GDPR.

Dall'indagine è emerso altresì che la maggior parte delle app per uso ludico risultano essere molto pericolose per i dati degli utenti. Su un campione di 500 app tra quelle maggiormente scaricate, in ben 469 casi sono stati riscontrati tracker di profilazione on line, vale a dire che il 93,8% delle app esaminate aveva dei **sistemi di tracciamento in grado di raccogliere molte più informazioni di quelle necessarie.**
In pratica, si è osservato che **gli utenti di quelle app** – in virtù del "consenso" di volta in volta accordato con il click alla relativa richiesta (posto come condizione per utilizzare il servizio) **venivano spiati nei loro comportamenti, attraverso la memorizzazione del tempo di utilizzo dell'app, la geolocalizzazione, l'accesso ai dati della rubrica o alle foto**
(N.B. spesso vengono poi inviati agli utenti messaggi pubblicitari, anche di giochi d'azzardo)

- Da una recente indagine condotta dal New York Times su 20 app ludiche (10 su Apple e 10 su Google), è risultato che la maggior parte delle società produttrici di app per bambini violando i dati personali dei minori (raccolgono molti più dati di quelli necessari, chiedendo nome, cognome, età, indirizzo, numero di telefono). Inoltre registrano il tempo di utilizzo e di conseguenza la maggiore o minore propensione dell'utente al gioco.
- **I minori vengono avvicinati al gioco d'azzardo** (cfr. stessi meccanismi delle sale da gioco)

Espongono a rischi anche le app utilizzate per modificare foto o video

Il Garante privacy ha invitato alla massima prudenza circa l'uso di tutte quelle app che, grazie **all'intelligenza artificiale**, consentono di modificare foto e video (es. invecchiando i volti o trasformando maschi in femmine e viceversa, come **FaceApp**).

Queste app, che possono sembrare divertenti e che spesso vengono utilizzate come passatempo anche dai minori, **celano in realtà dei grossi rischi:**

- perché **hanno accesso all'archivio delle immagini**
- perché attraverso le fotografie e/o i video è **possibile raccogliere dati biometrici**

- Attualmente l'impiego dei dati biometrici per i pagamenti, per l'accesso ai servizi bancari o in sostituzione di password o codici di accesso (ad esempio per disinstallare l'allarme di casa) non è diffuso, tuttavia si sta andando nella direzione di aumentarne l'uso su larga scala. Ebbene, dal momento che qualsiasi dato personale, una volta messo in rete, può facilmente sfuggire al controllo, **è più che fondato il timore che i dati biometrici raccolti dalle app e trattati in modo non adeguato, anche a distanza di anni, possano essere utilizzati da malintenzionati per gli scopi illeciti più diversi.**

I minori corrono più rischi degli adulti …

- Visione di immagini inadeguate all'età (***sexting***)
- Lettura di testi che richiederebbero spiegazioni da parte di un adulto.
- **Adescamento in rete da parte di pedofili che** sfruttano i canali di comunicazione utilizzati dai giovanissimi - come **video giochi on line** o app all'apparenza innocue - per ottenere dai giovani utenti contenuti a sfondo sessuale o addirittura per incontrarli (***grooming***)
- **Dipendenza dalla rete e isolamento** (***hikikomori***)

  (cfr. Commissione bicamerale per l'infanzia e l'adolescenza, seduta del 13/01/2021**)**
- **Sfide pericolose**
- **Cyberbullismo**

Sono tutte situazioni della cui pericolosità spesso le vittime non si rendono neppure conto, o se ne rendono conto troppo tardi.

È quindi fondamentale il controllo da parte dei genitori

- **Cfr.** Dichiarazione del Garante infanzia e adolescenza (in occasione del parere del 23/04/2018 sul GDPR): «*Serve che le **agenzie educative** e le istituzioni predispongano e attuino un programma, accompagnato da uno studio sulla necessaria **consapevolezza digitale da parte delle persone di minore età***»
- **Cfr.** Garante privacy, "*Minori e nuove tecnologie. Consigli ai «grandi» per un utilizzo sicuro da parte dei «piccoli»*" (Febbraio 2021)

Ci sono poi i rischi legati all'uso eccessivo di smartphone, pc e tablet…

Secondo le recenti ricerche dell'Osservatorio Nazionale Adolescente e del Telefono Azzurro

- La sovraesposizione alla tecnologia al di sotto dei 12 anni può causare **gravi conseguenze per lo sviluppo del bambino**
- **I rischi diminuiscono in modo significativo al di sopra dei 12 anni**, ossia, più precisamente, quando inizia lo **sviluppo cerebrale della corteccia pre-frontale** deputata al controllo degli impulsi e alla consapevolezza delle conseguenze delle azioni proprie ed altrui

I minori sono sempre più connessi ….

Secondo i dati Istat-Commissione parlamentare per l'infanzia e l'adolescenza, "*Indagine conoscitiva sulle forme di violenza fra i minori e ai danni di bambini e adolescenti*" (1 giugno 2020):

- Nel 2019, l'87,3% dei ragazzi tra 11 e 17 anni di età ha **utilizzato quotidianamente il telefono cellulare** e fra questi **3 su 4 hanno navigato in rete tutti i giorni**
- **Nell'arco di soli 4 anni,** il numero dei minori fra gli 11 e i 17 anni connessi alla rete **è aumentato di circa il 20%**
- Le ragazze utilizzano il cellulare e navigano in rete più dei ragazzi: l'88,6% usa il cellulare quotidianamente e il 75,8% accede a Internet tutti i giorni. **(N.B. le ragazze sono anche le più colpite dal cyberbullismo)**
- **Per navigare in rete i minori utilizzano soprattutto gli smartphone** e soltanto il 25,2% dei ragazzi usa il pc tutti i giorni per navigare in rete

(mentre nel 2014 l'uso del pc rispetto allo smartphone era del 40,5%)

… e diminuisce l'età del primo accesso alla Rete

Società Italiana di Pediatria

- Da anni mette in guardia sui **rischi per la salute fisica e mentale dei bambini** determinata dall'uso eccessivo di smartphone, tablet e pc.
- Tra i genitori è sempre più diffusa la **scorretta abitudine di intrattenere i figli con smartphone e tablet già a partire dal primo anno di età** e otto bambini su dieci nell'età compresa fra i 3 e i 5 anni sono soliti usare il cellulare dei genitori.
- Soltanto il 29% dei genitori secondo i dati raccolti dalla Società Italiana di Pediatria, chiede consiglio ai pediatri sull'uso dei dispositivi tecnologici da parte dei bambini
- Con la pandemia la situazione è peggiorata (**aumento delle dipendenze da smartphone e problemi psicofisici legati all'uso eccessivo dei dispositivi elettronici)**

Indagini Istat

- (cfr. **quella condotta per Save the Children nel 2017**):
  - **Accesso sempre più precoce alla Rete** da parte dei bambini**, già a partire dai sei anni**: nel 54% dei casi i bambini usano la Rete internet di casa, e **sono in aumento i bambini che hanno uno smartphone nell'età compresa fra i 6 e i 10 anni** (cfr. la "moda" di regalare lo smartphone per la Prima comunione)
- (cfr. **quella pubblicata il 6 aprile 2020**):
  - nel 2019, tra gli adolescenti di 14-17 anni che hanno usato internet negli ultimi 3 mesi prima dell'intervista, **due su tre sono risultati con competenze digitali scarse o comunque basilari**, mentre meno di tre su dieci (pari a circa 700 mila ragazzi) hanno manifestato livelli alti di conoscenza

Minori e smartphone: una questione *anche* di età

I genitori sempre più di frequente si chiedono quale sia l'età giusta per **acquistare uno smartphone ai figli** (va ormai di moda regalarlo ad es. per la Prima comunione)

soprattutto nel caso di genitori separati la questione è **spesso oggetto di discussioni e conflitti, anche nelle aule di tribunale**, in quanto è legata **all'educazione del minore**, al rispetto del suo **superiore interesse** e alla **responsabilità genitoriale**

- Non esiste un'età oggettivamente "giusta" o stabilita per legge: molto dipende dalle singole situazioni familiari e personali.
- Tuttavia, come è emerso dagli studi della Società Italiana di Pediatria, è stata individuata una fascia di età sotto la quale (12 anni) l'uso eccessivo dei dispositivi tecnologici espone i minori a **seri rischi per la salute e per l'equilibrato sviluppo psicofisico.**

RIFLESSIONE

Se i minori di anni 14, per legge, non possono ad es. andare in giro da soli (cfr. art. 591 c.p. "*Abbandono di persone minori o incap*aci"), per quale motivo dovrebbero allora avere un proprio smartphone, posto che fuori casa saranno sempre accompagnati da un adulto?

Come tutelare i minori?

Sia il Garante privacy che il Garante per l'infanzia e l'adolescenza hanno in più occasioni sottolineato l'importanza del ruolo di vigilanza dei genitori, **anche in collaborazione con la scuola**

È importante innanzitutto essere consapevoli dei rischi che possono correre i minori (sia nel navigare in Rete e nello scaricare le app, sia per l'uso eccessivo e precoce di smartphone, pc e tablet)

- Cfr. Garante privacy, "*APProva di privacy*" (ottobre 2020)
- Cfr. Garante privacy, "*Minori e nuove tecnologie*" (febbraio 2021)
- Cfr. Garante privacy con Telefono Azzurro, spot "*Se non ha l'età, i social possono attendere*" (febbraio 2021)
- Cfr. Garante per l'infanzia e l'adolescenza, "*Cyberbullismo, cos'è e come difendersi*" (gennaio 2020)

… l'accesso dei minori alla Rete va monitorato

Il Garante privacy

- Nel febbraio 2021, in collaborazione con il Telefono Azzurro, ha realizzato lo spot "*Se non ha l'età, i social possono attendere*", con l'obiettivo di richiamare i genitori a svolgere un ruolo attivo di vigilanza.
- Inoltre ha aperto un procedimento su TikTok ed ha chiesto al Comitato europeo per la protezione dei dati personali (EDPB) di affrontare la questione nella riunione plenaria del 28/02/2021 e di attivare una specifica *task force* a tutela dei dati personali dei minori

Il Garante per l'infanzia e l'adolescenza

ha insistito:

- sulla necessità che **i gestori delle piattaforme siano costretti ad accertare l'età degli utenti** (cfr. art. 8 GDPR e relativo parere AGIA del 23-04-2018);
- **sull'urgenza di attivare la Consulta dei diritti e dei doveri del bambino e dell'adolescente digitale** di cui alla Legge n. 92 del 2019 (educazione civica)
- sull'urgenza di dare attuazione alla **Direttiva europea sui servizi dei media audiovisivi** (il termine di recepimento negli Stati era fissato al 19/09/2020)

«Occorre potenziare l'educazione digitale dei bambini, dei ragazzi e degli stessi genitori, sempre più spesso alle prese con piattaforme e comportamenti in rapido cambiamento» (Garante per l'infanzia e l'adolescenza in occasione del Safer Internet Day 2021)

Safer Internet Centre

- **Dal 2012 è stato attivato il progetto "Safer Internet Centre-Generazioni connesse"** co-finanziato dalla Commissione Europea e coordinato dal MIUR.
- Il Progetto è finalizzato alla promozione di un uso sicuro e positivo del web
- **Il Safer Internet Day**, è la Giornata mondiale per la sicurezza in Rete che si celebra il secondo martedì del mese di febbraio e che è stata istituita dalla Commissione europea con l'obiettivo di favorire fra i ragazzi riflessioni sull'uso consapevole della Rete e sul ruolo di ciascuno per rendere Internet un luogo più sicuro.

Quanto vigilano i genitori?

Società Italiana di Pediatria

- **nel 2020 ha rilevato che:**
- Il 72,6% dei ragazzi intervistati ritiene giusto ricevere regole per usare la Rete
- Tuttavia solo nel 55% delle famiglie (+7,4% rispetto al 2018) **vengono date limitazioni sull'uso della Rete o regole di comportamento**
- l'80% dei ragazzi riferisce che l'unica limitazione ricevuta è legata al tempo di utilizzo, oltre a quella di non visitare siti porno e di mantenere chiuso il proprio profilo social

Safer Internet Centre

- Da una ricerca del 2020-2021 condotta dal Safer Internet Centre in collaborazione con l'Università di Firenze e l'Università di Roma La Sapienza (su un campione di 5386 ragazzi di età media 16 anni) è emerso che:

- Il 60% dei ragazzi intervistati non ha mai sentito parlare del Regolamento europeo per il trattamento dei dati personali;
- Il 42% ha preso misure;
- Il 31% si è detto preoccupato ma non sa come proteggersi;
- Il 27% non si pone il problema di navigare in Rete in sicurezza

<u>Sui possibili rischi on line</u> (in relazione anche alla DAD):

- il 27% ha riferito di non aver avuto spiegazioni da nessuno
- Il 23% ne ha parlato a scuola negli anni precedenti
- Il 15% ha trovato informazioni in Rete da solo
- Il 12% ne ha parlato con i docenti a scuola
- Il 9% ne ha parlato con i genitori
- L'8% ne ha parlato con gli amici/compagni di classe
- Il 6% altro

I genitori:
… devono dare il buon esempio, evitando comportamenti scorretti, soprattutto davanti ai bambini

… devono educare ed istruire i figli *anche* all'uso corretto dei social e della tecnologia

- **I genitori devono formare i figli *anche* all'uso consapevole della tecnologia**, affinché questi siano consapevoli dei pericoli, dei diritti e dei doveri relativi alla comunicazione digitale
- **I minori devono sapere come comportarsi in Rete**, sia per tutelare se stessi, sia per evitare di recare pregiudizio ad altri (es. pubblicazione di foto e video propri o altrui)

… devono controllare smartphone e tablet dei figli

- I genitori hanno l'OBBLIGO di controllare i messaggi scambiati dai figli on line, sia per evitare loro pregiudizi, sia per evitare che i propri figli rechino danni ad altri
  (cfr. **atti di cyberbullismo subiti** o **posti in essere**; diffusione di foto o video on line propri o altrui, partecipazione a sfide ecc.)
- **L'obbligo di vigilanza dei genitori prevale sul diritto alla riservatezza dei figli**

- **Cfr. Trib. Min. Caltanissetta, sent. 8 ottobre 2019 (WhatsApp)**
- **Cfr. Trib. Parma, sent. n. 698 del 5-08-2020 (parental control)**

È fondamentale l'alleanza scuola/famiglia

Cfr. Legge n. 92 del 2019 "*Introduzione dell'insegnamento scolastico dell'educazione civica*"

- **Art. 5 "Educazione alla cittadinanza digitale"**: conoscenze ed abilità digitali essenziali:

1) Capacità di valutare criticamente le fonti di dati e contenuti digitali;
2) Individuazione dei mezzi digitali appropriati in base al contesto;
3) Capacità di partecipare al dibattito pubblico attraverso l'uso dei servizi digitali;
4) Conoscenza delle norme di comportamento da osservare in ambienti digitali;
5) Capacità di creare e gestire l'identità digitale;
6) Conoscenza delle politiche di tutela della riservatezza dei dati on line
7) Capacità di evitare rischi per la salute e minacce al proprio benessere psicofisico (con particolare attenzione al cyberbullismo)

Per dare attuazione a quanto sopra è stata prevista l'istituzione della

Consulta dei diritti e dei doveri del bambino e dell'adolescente digitale

- **Art. 7 "Scuola e famiglia"**

«Al fine di valorizzare l'insegnamento trasversale dell'educazione civica e di sensibilizzare gli studenti alla cittadinanza responsabile, la scuola rafforza la collaborazione con le famiglie, anche integrando il Patto educativo di corresponsabilità…»

- **Art. 8 "Scuola e territorio"**

*«L'insegnamento trasversale dell'educazione civica è integrato con esperienze extra-scolastiche, a partire dalla **costituzione di reti anche di durata pluriennale con altri soggetti istituzionali**, con il mondo del volontariato e del Terzo settore, con particolare riguardo a quelli impegnati nella promozione della cittadinanza attiva»*

N.B. Importanza delle attività svolte negli oratori, già da tempo, in collaborazione con scuole e famiglie

Le sfide on line: sono sempre più diffuse e costituiscono un serio pericolo per i minori che navigano in Rete

- **Numerosi bambini ed adolescenti, in tutto il mondo, sono stati vittime di sfide on line, che in alcuni casi si sono rivelate mortali.**

ES:

- Foto scattate nell'atto di gettarsi da un'auto in corsa,
- video girati in situazioni pericolose
- camminare sul cornicione di un palazzo o sporgersi da un ponte
- Assumere dosi massicce di antistaminici o di alcolici

sono solo alcuni degli esempi di **challenge pericolose** che girano sui social e in particolare su TikTok, la piattaforma cinese che (anche in seguito al lockdown) ha in poco tempo visto aumentare in modo esponenziale il numero degli iscritti.

- L'algoritmo di TikTok, come quello di altri social simili, è stato studiato per tenere il più possibile on line gli utenti: la piattaforma, grazie ad un sofisticato modello matematico in grado di riconoscere il successo dei contenuti e di catalogarli, offre in continuazione agli utenti video che rispondono ai loro interessi.

Cyberbullismo

Legge n. 71 del 2017 *"Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"*

Definizione

Art. 1, comma 2:

«… per cyberbullismo si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo»

Linee di orientamento per la prevenzione e il contrasto in ambito scolastico

Art. 4, comma 5:

«…le istituzioni scolastiche di ogni ordine e grado, nell'ambito della propria autonomia e nell'ambito delle risorse disponibili a legislazione vigente, ***promuovono l'educazione all'uso consapevole della rete internet e ai diritti e doveri connessi all'utilizzo delle tecnologie informatiche****, quale elemento trasversale alle diverse discipline curriculari, anche mediante la realizzazione di apposite attività progettuali aventi carattere di continuità tra i diversi gradi di istruzione o di progetti elaborati da reti di scuole in collaborazione con enti locali, servizi territoriali, organi di polizia, associazioni ed enti»*

"Meglio evitare che i minori possano scaricare e utilizzare app da soli. I più giovani, infatti, sono meno consapevoli dei pericoli e più esposti al rischio di una raccolta e diffusione incontrollata di dati propri o dei familiari"

(Garante privacy, *APProva di privacy*, ottobre 2020)

Grazie per l'attenzione

Martedì 23 febbraio 2021 h. 12.00-14.00

Webinar - Ordine degli Avvocati di Roma