FEDERPRIVACY

RAPPORTO STATISTICO

App di giochi, minori e tutela della privacy

a cura dell'Osservatorio di Federprivacy

(Settembre 2020)

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 – 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **urp@federprivacy.org**- Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

Lo studio effettuato dall'**Osservatorio di Federprivacy**, analizzando 500 tra le principali app di giochi più diffuse tra i minori, si pone l'obiettivo di fare un **quadro sui rischi privacy a cui possono essere esposti i bambini** sulla base di diverse variabili come la presenza di tracker, di permessi e di advertising, nonché sul trasferimento di dati personali in nazioni non sicure e sulle forme di tutela previste dal Gdpr.

1. Le caratteristiche generali del campione

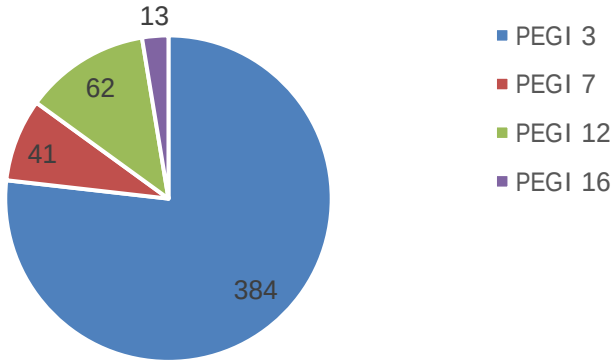
Dal campione delle 500 app di giochi analizzate tra quelle disponibili nel Google Play Store risulta che nell'**85%** dei casi l'indice **PEGI è inferiore a 7**, cioè si tratta di applicazioni con contenuti adeguati a bambini di età inferiore a 8 anni *(fig. 1)*, mentre la quasi totalità, **479 (96%)**, presenta al suo interno **annunci pubblicitari**.

> ***Cos'è l'indice PEGI?***
> *PEGI fornisce una classificazione dei videogiochi in base all'età in 38 paesi europei. La classificazione in base all'età conferma che il gioco è adeguato agli utenti di una determinata età. PEGI esamina l'idoneità di un gioco sulla base dell'età e non del livello di difficoltà.*

Considerando il **numero dei download**, le app campione risultano tra le più diffuse tra i minori *(fig. 2)*. 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.

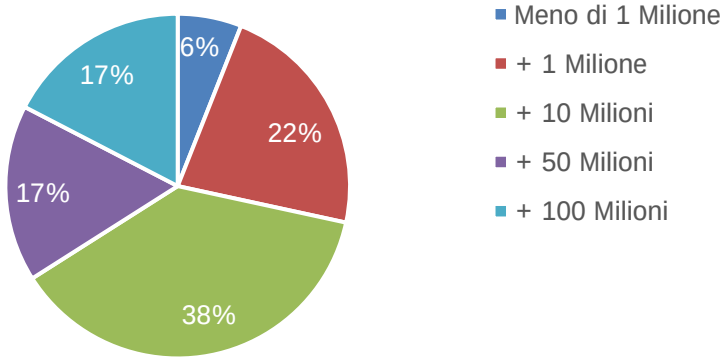
Guardando l'indice PEGI, in 384 casi analizzati è pari a 3. Questo significa che nel 76,8% si tratta di app adeguate per bambini di 3 anni. Questo dato sale all'85% del campione se consideriamo contenuti adatti per bambini di età inferiore a 8 anni (*fig.1*)

fig .1 – Classificazione per indice PEGI



Considerando il numero dei download *(fig.2), il 94% (*470 su 500) registrano scaricamenti superiori al milione. Questo dato conferma che si tratta delle applicazioni più diffuse tra i bambini e ragazzi. Nello specifico, il 72% (358) risulta avere +10milioni di download, mentre solo il 6% (30) hanno meno di 1 milione di download.

fig .2 – Classificazione per download



Inoltre, se si guardano i dati nel rispetto del Gdpr, è possibile affermare che, se da un lato quasi la totalità (oltre il 90%) fornisce una qualche informativa sulla privacy comprensiva di contatti, dall'altro si evidenzia una diffusa **mancanza di un Data Protection Officer (87%)**, cioè un responsabile della protezione dei dati incaricato di vigilare sul rispetto delle norme sulla privacy a cui gli utenti dovrebbero potersi rivolgersi in ogni momento per esercitare i loro diritti.

Nelle 500 app esaminate si è riscontrato che in 482 casi *(fig.3)* , pari al 96%, è presente un'informativa privacy, in 453 *(fig.4)* , *circa il 90%* , sono presenti dei recapiti di contatto, ma in 413 applicazioni *(fig.5)*, che equivale all'87% del campione, non risulta evidenza della nomina di un Data Protection Offficer (DPO)

fig .3 – Informativa Privacy

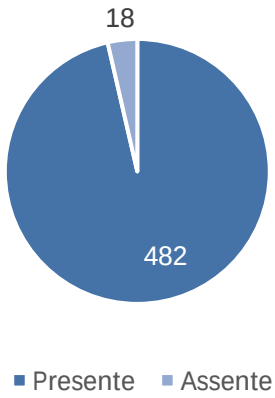


fig .4 – Recapiti di Contatto

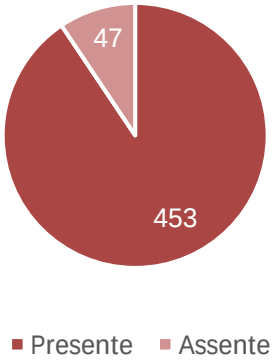
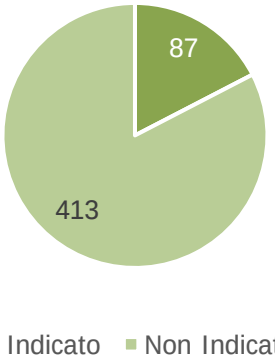
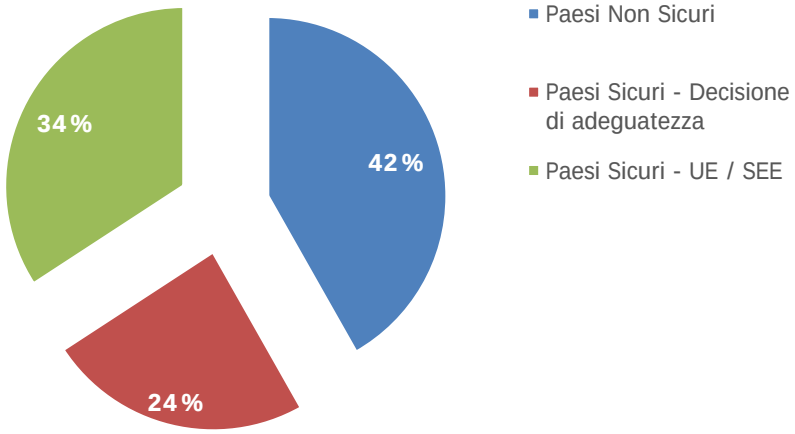


fig .5 – DPO



Spostando l'attenzione sui paesi in cui vengono sviluppate le app e, di conseguenza, trattati i dati, possiamo constatare come nel **42%** del totale le aziende sviluppatrici hanno sede in paesi considerati **non sicuri rispetto alla privacy** *(fig. 6)*. Tra i paesi terzi considerati non sicuri, in base al numero di app sviluppate *(tab.1)*, troviamo nei primi ai posti **Stati Uniti* (11%), Regno Unito[#] (7,4%), Cina (4,6%)** dove sono state sviluppate 115 app pari al 23% del campione, e poi **Singapore (2,4%).**

fig .6 – Sicurezza del paese sulla base della sede degli sviluppatori



Il 34% di app del campione (171) risultano sviluppate in Paesi ritenuti sicuri perché facenti parte della UE o comunque all'interno dello SEE;
Il 24% (120) sono sviluppate in paesi considerati sicuri grazie ad una decisione di adeguatezza della Commissione UE
Per il restante 42% (209), la sede delle aziende sviluppatrici risulta essere in paesi terzi considerati non sicuri riguardo al livello di protezione dei dati personali.

***Nota:** allo stato attuale gli Usa sono considerati un paese non sicuro riguardo la protezione dei dati personali a seguito della sentenza del 16 luglio 2020 della Corte di Giustizia Europea che ha invalidato il "Privacy Shield"*

***[#]Nota**: Dalla mezzanotte del 31 gennaio 2020 il Regno Unito non è più formalmente uno stato membro dell'UE.* A partire da tale data ha avuto inizio il periodo transitorio limitato nel tempo che scade il 31 dicembre 2020, al termine del quale, in assenza di decisioni di adeguatezza il Regno Unito è considerato a tutti gli effetti un Paese terzo.

tab.1 – Elenco per paese dove vengono sviluppate le app e trattano i dati

Nazione sede sviluppatore	N. app	%	Sicurezza del paese
Argentina	5	1 %	Riconosciuto sicuro con decisione di adeguatezza
Australia	8	1,6 %	Riconosciuto sicuro con decisione di adeguatezza
Austria	8	1,6 %	Stato membro UE
Bielorussia	**4**	**0,8 %**	**Paese terzo non sicuro**
Brasile	**3**	**0,6 %**	**Paese terzo non sicuro**
Bulgaria	4	0,8 %	Stato membro UE
Canada	14	2,8 %	Riconosciuto sicuro con decisione di adeguatezza
Cina	**23**	**4,6 %**	**Paese terzo non sicuro**
Cipro	19	3,8 %	Stato membro UE
Corea	**9**	**1,8 %**	**Paese terzo non sicuro**
Danimarca	4	0,8 %	Stato membro UE
Emirati Arabi	**8**	**1,6 %**	**Paese terzo non sicuro**
Estonia	1	0,2 %	Stato membro UE
Finladia	17	3,4 %	Stato membro UE
Francia	23	4,6 %	Stato membro UE
Germania	18	3,6 %	Stato membro UE
Giappone	33	6,6 %	Riconosciuto sicuro con decisione di adeguatezza
Grecia	1	0,2 %	Stato membro UE
India	**5**	**1 %**	**Paese terzo non sicuro**
Indonesia	**1**	**0,2 %**	**Paese terzo non sicuro**
Irlanda	8	1,6 %	Stato membro UE
Isole Cayman	**2**	**0,4 %**	**Paese terzo non sicuro**
Israele	34	6,8 %	Riconosciuto sicuro con decisione di adeguatezza
Italia	8	1,6 %	Riconosciuto sicuro con decisione di adeguatezza
Libano	**1**	**0,2 %**	**Paese terzo non sicuro**
Lituania	5	1 %	Stato membro UE
Lussemburgo	1	0,2 %	Stato membro UE
Malta	11	2,2 %	Stato membro UE
Malesia	**1**	**0,2 %**	**Paese terzo non sicuro**
Messico	**1**	**0,2 %**	**Paese terzo non sicuro**
Norvegia	2	0,4 %	Stato facente parte dello SEE
Nuova Zelanda	3	0,6 %	Riconosciuto sicuro con decisione di adeguatezza
Olanda	4	0,8 %	Stato membro UE
Oman	**2**	**0,4 %**	**Paese terzo non sicuro**
Pakistan	**3**	**0,6 %**	**Paese terzo non sicuro**
Polonia	4	0,8 %	Stato membro UE
Portogallo	1	0,2 %	Stato membro UE
Regno Unito	**37**	**7,4 %**	**Paese terzo non sicuro (dal 01.01.2021)**
Repubblica Ceca	**1**	**0,2 %**	**Paese terzo non sicuro**
Russia	**11**	**2,2 %**	**Paese terzo non sicuro**
Sede non dichiarata	**8**	**1,6 %**	**Paese terzo non sicuro**
Serbia	**2**	**0,4 %**	**Paese terzo non sicuro**
Singapore	**12**	**2,4 %**	**Paese terzo non sicuro**
Slovacchia	2	0,4 %	Stato membro UE
Slovenia	2	0,4 %	Stato membro UE
Spagna	22	4,4 %	Stato membro UE
Svezia	13	2,6 %	Stato membro UE
Stati Uniti	**55**	**11 %**	**Paese terzo non sicuro**
Svizzera	15	3 %	Riconosciuto sicuro con decisione di adeguatezza
Taiwan	**1**	**0,2 %**	**Paese terzo non sicuro**
Taliandia	**1**	**0,2 %**	**Paese terzo non sicuro**
Turchia	**9**	**1,8 %**	**Paese terzo non sicuro**
Ucraina	**7**	**1,4 %**	**Paese terzo non sicuro**
Ungheria	1	0,2 %	Stato membro UE
Vietnam	**2**	**0,4 %**	**Paese terzo non sicuro**
Totale	**500**		

S.E.&.O

2. Tracker

Prima di esporre i risultati dell'analisi, è necessario dare una definizione di tracker.

Cos'è un Tracker?

Un tracker è un software il cui compito è raccogliere informazioni sulla persona che usa l'applicazione, su come la usa o sullo smartphone che viene utilizzato. Un tracker è solitamente distribuito dalle aziende come SDK (Software Development Kit), una sorta di toolkit già pronto, con l'obiettivo di rendere più facile per gli sviluppatori di applicazioni. Da notare: i tracker 'open source' esistono, il loro codice è disponibile e aperto a tutti.

Tutti i tracker sono uguali?

No, tutti i tracker non hanno la stessa funzione e possono presentare diversi livelli di intrusione (della privacy).

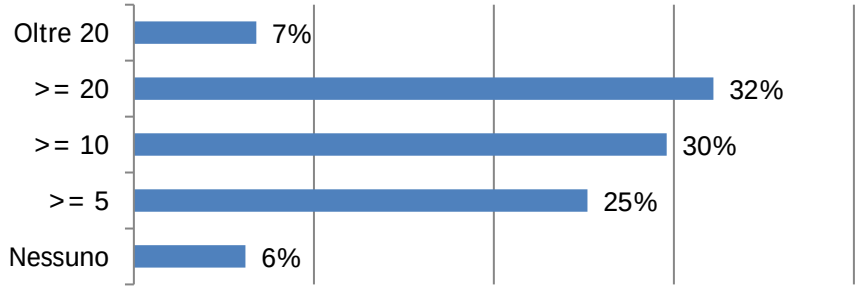
- ***Segnalatori di crash:*** *questi tracker sono specializzati in segnalazioni di crash dell'applicazione. In altre parole, il loro obiettivo è quello di informare gli sviluppatori dell'applicazione che un'app ha riscontrato un problema. Pertanto, le informazioni raccolte nel momento in cui l'applicazione si è bloccata consentiranno allo sviluppatore di correggere il bug.*
- ***Analisi:*** *questi tracker sono pensati per raccogliere l'utilizzo dei dati e consentire allo sviluppatore di conoscere meglio il proprio pubblico (ad esempio, per sapere quale pagina hai visitato, o per quanto tempo sei rimasto su una determinata area della pagina).*
- ***Profilazione:*** *l'obiettivo di questi tracker è di raccogliere quante più informazioni possibili sull'utente che utilizza una data applicazione, in modo tale da costruire un profilo virtuale dell'utente stesso. A questo scopo, il tracker si concentrerà ad esempio sulla cronologia di navigazione internet, sulla lista delle applicazioni installate, e così via.*
- ***Identificazione:*** *I tracker sono responsabili della determinazione della tua identità digitale. Questa identità può riferirsi a un'identità ufficiale oppure a un'identità astratta, fittizia (Nickname, Pseudonimi, ecc.). Lo scopo è, ad esempio, essere in grado di correlare le attività online dell'utente a quelle offline.*
- ***Ads:*** *I tracker mirano a creare un profilo dell'utente in modo tale da mostrargli annunci pubblicitari mirati. Questo è possibile/rilevante solo se l'utente ha già un profilo digitale disponibile. Il fine ultimo del creatore del tracker è quello di monetizzare la sua applicazione guadagnando, ad esempio, tramite la pubblicità.*
- ***Localizzazione:*** *i tracker sono progettati per determinare la posizione geografica del dispositivo mobile. Per farlo, i tracker sfruttano diversi sensori: chip GPS, celle a cui si connette il cellulare, le reti wi-fi presenti nelle vicinanze, i dispositivi Bluetooth nelle vicinanze o persino suoni specifici trasmessi da altoparlanti.*

Fonte: Exodus Privacy

Definito cos'è un tracker, vediamo quanto gli SDK (Software Development Kit) di questi sono presenti all'interno del campione analizzato. Il dato è sicuramente poco rassicurante in quanto nella maggioranza **delle applicazioni** (**94%**) è **presente** almeno un **tracker**. Ma questo non è tutto, infatti, se consideriamo il numero di tracker *(fig. 7)* possiamo affermare che nel **62% delle app sono presenti da 6 a 20 tracker.**
Nelle 500 app analizzate sono stati riscontrati **4.860 tracker** che corrispondono ad un **valore medio di 9,72** tracker per singola applicazione.

Sul totale delle app analizzate, solo in 34 (6%) non sono presenti tracker. Nel 55% (274) ne sono presenti meno di 10. Mentre nel 39% (195) sono presenti più di 11 tracker, con punte fino a 36 in un'unica applicazione.

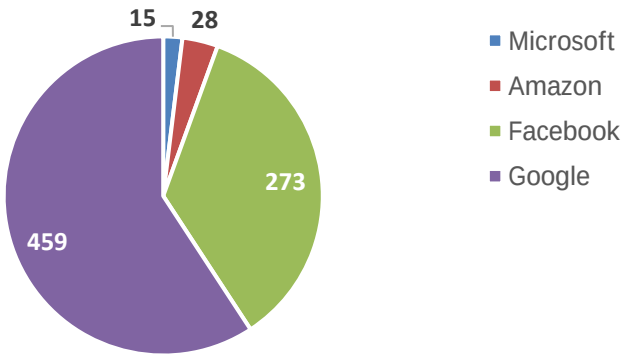
fig .7 – App per numero di tracker presenti



Ma di chi sono quelli principali? I **tracker di Google** *(fig. 8)* risultano presenti nella maggioranza dei casi **(92%)** mentre quelli di Facebook superano la metà (54%). Molto distanziati Amazon e Microsoft, rispettivamente con il 6% e 3%.

Google e Facebook sono presenti in più della metà delle app analizzate.
In particolare è Google a primeggiare in questa particolare classifica con 459 app (92% del totale). Poco presenti invece Amazon e Microsoft.

fig .8 – Tipologia di tracker



3. Permessi

Come fatto nel precedente paragrafo, prima di vedere i risultati, è necessario dare una definizione di permesso.

Cos'è un Permesso?

I permessi sono diritti di accesso che l'app chiede di accedere sul tuo telefono.

Che tipo di permessi?

Possono riguardare varie funzioni o parti di informazioni, come l'accesso alla tua geolocalizzazione, i tuoi contatti, i tuoi file, il tuo microfono, la funzione vibrazione, la fotocamera e così via. Le analisi di Exodus Privacy ti permettono di sapere, per ogni app, quali permessi sono richiesti.

Fonte: Exodus Privacy

Definito cos'è un permesso, vediamo quanto questi sono presenti all'interno del campione analizzato. Come per i tracker, anche qui il dato è non è rassicurante in quanto **la quasi totalità delle applicazioni** (**99,6%**) è **presente** almeno una richiesta di **permesso** al dispositivo. Ma questo non è tutto, infatti, se consideriamo il numero di permessi *(fig. 7)* possiamo affermare che più dell'**80% delle app hanno più di 10 permessi.**
Nelle 500 app analizzate sono stati riscontrati **5.108 permessi** che corrispondono ad un **valore medio di 10,2** per singola applicazione.

Sul totale delle app analizzate, solo in 2 (0,4%) non sono presenti permessi. Nel 65% (326) ne sono presenti meno di 10. Mentre nel 33,6% (168) sono presenti più di 11 permessi, con punte fino a 35 in un'unica applicazione.

fig .7 – App per numero di permessi presenti