¿Són abusius, els permisos de les aplicacions?

El 60% d'usuaris han declinat alguna vegada baixar-se'n una després de veure que els demanava massa informació

NEREIDA CARRILLO
BARCELONA

L'any passat, del Google Play se'n van descarregar 200 milions d'aplis, i de l'Apple Store, uns 100 milions, segons les xifres que ha donat a conèixer l'empresa d'analítica mòbil App Annie. I descàrrega rere descàrrega, sempre la mateixa operació: les aplicacions demanen accedir a diverses funcionalitats de l'aparell i a dades personals. Si, per exemple, volem descarregar Instagram, sol·licitarà accedir a les dades del perfil, la llibreta de contactes, la ubicació, les fotos del nostre aparell i també a la càmera i el micròfon. El comportament majoritari és validar l'operació, gairebé per inèrcia, per completar el procés. Però si ens aturem un moment en aquesta pantalla, ens podem preguntar: qui decideix aquests permisos? ¿Són necessaris o abusius? ¿Les dades que s'aconsegueixen es passen a tercers?

Una anàlisi feta l'any passat pel centre de recerca Pew a un milió d'aplis del Google Play Store concloïa que demanaven fins a 235 permisos diferents i que, de mitjana, una aplicació en sol·licitava cinc. El permís més habitual, assenyala l'estudi, és accedir a la connectivitat del telèfon. Dels 235 permisos que va detectar i escrutar la recerca, la majoria –uns 165– feien la petició d'accedir a funcionalitats del maquinari, mentre que la resta eren requeriments de dades personals. L'anàlisi també subratllava que les aplicacions de les categories de Comunicació i Negocis són les que més permisos sol·liciten.

De totes les demandes que ens fan les aplis abans de la descàrrega, Carles Ferreiro, CEO d'AppCircus i fundador dels Mobile Premier Awards, distingeix entre permisos crítics, aquells sense els quals l'apli no funciona, els opcionals, que són "recomanats per treure tot el suc de l'apli", i els injustificats. Per a Ferreiro, hi ha frau en aquells permisos que "el desenvolupador està dient «són altres coses que seria genial saber de tu, encara que no et puc dir per a què»". Genís Margarit, enginyer en telecomunicacions i professor de la Universitat Pompeu Fabra, s'expressa en la mateixa línia i lamenta: "En la majoria de casos, els permisos són abusius perquè els programadors parteixen d'unes plantilles ja preprogramades".

Dades per a tercers

Ramon Querejazu, fundador i CEO de Selftising, una empresa catalana de disseny d'aplicacions, puntualitza que, si bé els desenvolupadors decideixen quines dades volen recollir dels usuaris, en el cas dels permisos depenen de la plataforma. Sobre les dades, Querejazu afegeix: "L'ús que faci el desenvolupador de les dades depèn del pacte a què hagi arribat amb l'usuari". Els experts asseguren que una bona pràctica comporta recollir només les dades dels usuaris que permeten enriquir l'aplicació, saber més sobre l'usuari per donar-li un servei millor; però sovint es recopilen dades que van més enllà del que ofereixen les aplis.

"Les dades haurien de quedar en propietat del desenvolupador per millorar la seva apli –remarca Ferreiro–. No obstant això, hi ha casos en què la informació obtinguda es ven a tercers que busquen conèixer el comportament dels usuaris. Si això respecta les normes de privacitat i propietat, a més de les de les botigues, és legal". Però això no sempre passa. Ferreiro afegeix que es donen casos de frau que, si bé "són molt marginals i anecdòtics, tenen un impacte gran en la desconfiança dels usuaris". Sobre aquestes pràctiques, Margarit assegura: "Trobem algunes aplicacions en què els programadors volen recollir moltes dades dels usuaris perquè presumeixen que, així, si un dia volen intentar-la vendre, tindrà més valor".

Petició
El permís més habitual és per accedir a la connectivitat del telèfon mòbil

Control
L'accés a la llibreta d'adreces és un dels abusos més freqüents

Els permisos que sol·liciten les aplis en el moment de la descàrrega es poden considerar la versió mòbil del "llegeixo i accepto les condicions d'ús" de les webs. Es poden equiparar perquè, tant en un cas com en l'altre, gairebé ningú s'ho mira amb lupa. A poc a poc, però, creix la conscienciació sobre aquests aspectes. Prova d'això és que, segons una enquesta feta també pel centre de recerca Pew, un 60% dels usuaris asseguren que van decidir no instal·lar-se una aplicació quan van descobrir que exigia accedir a molta informació personal. I un 43% afirmen que se'n van desinstal·lar una exactament pel mateix motiu.

"Els usuaris fan bé de desinstal·lar-se aplicacions que no afegeixen valor o es converteixen en un problema", comenta Ferreiro. Tot i que dades com aquestes –que estudien usuaris nord-americans– indiquen que alguns estan començant a prendre'n consciència, els experts creuen que el canvi encara és lent i poc estès. Si això fos generalitzat, opina Margarit, "les aplicacions més famoses estarien canviant la seva conducta". Querejazu assenyala com a principal problema el "desconeixement" dels usuaris, que "donen les seves dades de posicionament sense saber què hi ha més enllà".

Càmera i geolocalització

Margarit subratlla tres tipus d'excessos que considera els més freqüents. En primer lloc, indica l'accés a la llibreta d'adreces com un dels permisos en què els desenvolupadors més s'extralimiten. En segon lloc, assenyala l'accés al micròfon i a la càmera; afegeix que s'empra molt en el cas dels videojocs i pot ser perjudicial per als infants: "El que es pretén –explica Marga-

rit– és que si un dia fas una partida molt bona et puguin fer una fotografia o gravar una salutació i posar-ho al portal per a tothom. Els menors d'edat no són gaire conscients d'aquest consentiment i acaben despullant la seva intimitat".

El tercer permís que opina que sovint excedeix els límits és la geolocalització. En aquest cas, Margarit puntualitza que hi ha usos positius, com ara les aplicacions bancàries que "empren la geolocalització com un doble factor d'autentificació", és a dir, si algú intenta pagar o treure diners d'una targeta i es detecta que el mòbil no és al mateix lloc, es pot interpretar que la targeta ha sigut sostreta i es bloqueja l'operació. En altres casos, però, per a aquest enginyer informàtic, amb la geolocalització habilitada es poden donar a conèixer dades sensibles com ara on vivim, on treballem o quins són els nostres hàbits.

Cada dia es descarreguen milers d'aplis als telèfons mòbils. GETTY

Conscients o no de la quantitat d'informació que les aplicacions arriben a acumular dels seus usuaris, el cert és que qui vulgui descarregar-les al seu dispositiu no es pot negar a atorgar aquests permisos. "Com més informada estigui la gent de què es pot fer amb les seves dades –assegura Querejazu–, més barreres posarà". Per a Margarit, no hi ha encara una cultura gaire estesa de rebuig a les aplis que s'extralimiten amb els seus requeriments. Si bé l'usuari no es pot negar a permetre l'accés a determinades funcionalitats de l'aparell i dades personals, Margarit proposa una alternativa viable: "Deshabilitar aquestes prestacions a nivell de sistema operatiu". Això vol dir, per exemple, deshabilitar la càmera si volem baixar una aplicació que n'exigeix l'accés però ho considerem injustificat.

Algunes aplicacions i webs útils... o esfereïdores

Si remenem una mica, trobem aplicacions i pàgines web que ajuden a conscienciar-nos sobre la quantitat de permisos que exigeixen les aplis i també sobre com de perillós pot ser revelar informació sensible a través d'aquestes eines.

Dcentral1

Vols saber els permisos que has concedit?

És una eina disponible per a dispositius Android que va avisant l'usuari dels permisos que necessiten les aplis que té instal·lades al mòbil. Periòdicament li va fent recordatoris i li pregunta si vol desinstal·lar aquella apli o si, al contrari, encara hi confia i la vol seguir tenint al telèfon.

One Million Tweet Map

Una web que et pot treure de polleguera

Els que no són conscients de la quantitat de dades personals que es poden difondre amb la geolocalització poden visitar aquesta web. Segurament els canviarà el punt de vista. El professor Genís Margarit n'explica el funcionament: "T'ensenya tots els tuits que, en temps real, s'estan enviant arreu del món amb la gent que té la geolocalització habilitada al seu mòbil". En el moment d'escriure aquest reportatge, en un minut, hi havia a tot Catalunya 6.000 piulades en temps real de les quals es podia estirar el fil de la seva ubicació.

Creepy

L'empremta que deixem a les xarxes socials

Es tracta també d'una eina relacionada amb la geolocalització. Com el seu nom indica, també pot resultar "terrorífica", ja que rastreja les diferents xarxes socials d'usuaris que tenen la geolocalització habilitada. Disposa tota aquesta informació en un mapa que pot resultar molt revelador.