Acció contra les GAFAM de La Quadrature du Net

Al novembre de 2017, l'associació francesa La Quadrature du net, va emprendre una campanya per fer visibles **els despropòsits de les grans empreses tecnològiques vers les seves usuàries**.

«Les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) ens fan pagar els seus serveis amb les nostres llibertats.

La nostra llibertat de consciència, les deixa accedir als detalls del nostre esperit per manipular-nos de manera individualitzada i automatitzada. La nostra vida privada i la nostra intimitat, sense la qual ja no podem construir-nos a nosaltres mateixes.

Aquest contracte és il·lícit: en democràcia, ningú vol vendre les seves llibertats fonamentals. Fem que, a partir d'ara, la llei prohibeixi que un servei sigui remunerat amb dades personals.

Per recuperar les nostres llibertats, el 25 de maig, La Quadrature du Net ha iniciat accions col·lectives amb 12.000 persones contra cadascuna de les GAFAM.»

Aquest document és la **traducció al català de l'anàlisi de La Quadrature du net** en la seva «Acció de grup contra les GAFAM» https://gafam.laquadrature.net/

Llicència

Descarrega aquest document a:
https://fedi.cat/fediverse/lqdn-gafam-ca.pdf

Índex de continguts

Cronologia de la campanya

- Novembre de 2017. La Quadrature du Net inicia la campanya anti-GAFAM

- Gener de 2018. Participants del 34c3 munten la web https://www.gafam.info/ per donar suport al projecte: es crea un repositori (gafam-poster-translations) per facilitar la traducció dels pòsters, i un subdomini per a trobar-los i imprimir-los fàcilment (https://library.gafam.info/)

- Febrer de 2018. Es possibilita l'edició online dels pòsters a GAFAM on Weblate

- Abril de 2018. La Quadrature du Net inicia una acció de grup contra les GAFAM gafam.laquadrature.net on analitza cadascuna de les empreses

- Maig de 2018. Es presenta la denúncia col·lectiva que firmen 12.000 persones https://www.laquadrature.net/2018/05/28/depot_plainte_gafam/ I els pòsters ja s'han traduït a 16 idiomes

- Octubre de 2018. Actualització sobre la denúncia col·lectiva https://www.laquadrature.net/2018/10/10/nos-plaintes-contres-les-gafam-avancent/

- Novembre de 2018. Campanya anual de recollida de fons per seguir lluitant contra les GAFAM https://www.laquadrature.net/2018/11/15/soutenons-notre-internet/. I publicació d'un vídeo divulgatiu: https://video.lqdn.fr/videos/watch/dd3db1ae-f7a9-41cb-8db5-c8371977b880. Es poden traduir els subtítols al pad: https://pad.lqdn.fr/p/SRT_soutenons_notre_internet

Google

Google multiplica la seva presència a les nostres vides: és la nova televisió via **YouTube**, ens acompanya a tot arreu amb **Android**, filtra el nostre accés al món al seu **motor de cerca**, analitza els nostres missatges de **Gmail**, ven espais publicitaris a **milions de pàgines d'Internet** i espera interferir a les nostres interaccions físiques demà, a través del seu Assistent integrat a **Google Home**.

Totes aquestes activitats es combinen en una **vigilància de masses**, destinada a refinar el control que té sobre nosaltres...

Aquesta vigilància és **il·legal** perquè es basa en un consentiment que ens ha sigut arrabassat.

Anàlisi de Google

L'empresa Google

Fundada fa 20 anys per Larry Page i Sergueï Brin, creadors del motor de cerca Google, l'empresa compta actualment amb 74 000 empleats i una facturació de 90.600 milions d'euros. El seu model de negoci no es basa exclusivament en la publicitat, tot i que els seus ingressos publicitaris representen el 86% de la seva facturació.

Avui dia, Google és una filial d'Alphabet, l'empresa matriu d'un grup amb seu per tot el món. Els seus serveis s'han multiplicat: gestió dels correus electrònics amb Gmail, calendari amb agenda, emmagatzematge i edició de documents amb Drive i Gsuite, mòbil amb Android, publicació de vídeos amb YouTube, etc.

El que Google sap de nosaltres

Google sotmet tots els seus serveis a un corpus únic de «regles de confidencialitat» que permeten que l'empresa pugui recol·lectar:

- nom, fotografia, direcció de correu electrònic i número de telèfon de les persones que tenen un compte a Google
- Identificador del dispositiu
- informació sobre l'ús dels serveis (vídeo, imatges visualitzades, quan i com) i historial de navegació
- consultes de cerca (a Google, YouTube, Maps, etc.)
- el número de telèfon de les persones a qui hem trucat o contactat per SMS, l'hora, la data, la duració de les trucades, així com una llista de contactes afegits
- la direcció IP des de la que s'utilitzen els serveis
- la ubicació dels dispositius, definida a partir de la direcció IP, les senyals GPS, els punts d'accés a WiFi i les antenes de retransmissió telèfoniques properes
- altres informacions recopilades pels socis de Google

Google explica el fet d'usar totes aquestes dades per millor dirigir-se als seus usuaris amb l'objectiu de proposa'ls-hi anuncis amb més probabilitats de convence'ls en el moment oportú.

Com hem vist amb Facebook, l'anàlisi massiu d'informacions d'aparença anodina permet establir correlacions que se suposa que proporcionen una imatge detallada de la privacitat de cada persona.

Tot i que Google permet limitar la interconnexió de certs tipus de dades sense processar (localització, cerques efectuades i vídeos consultats), no deixa cap control sobre tots els altres tipus de dades. Sobretot, no ens permet bloquejar l'anàlisis feta a les dades derivades (els nostres perfils), que són els més sensibles, i que hem de cedir per utilitzar els seus serveis. L'accés als serveis de Google implica l'obligació de cedir aquestes informacions personals. Aquesta cessió resultant d'un consentiment no-lliure, l'anàlisi d'aquestes dades és il·lícit, i és **el que nosaltres ataquem.**

La quimera del control

No ens hem d'equivocar sobre l'anomenat control que Google ens deixaria sobre la interconnexió de certs tipus de dades (localització, cerques, vídeos). De forma predeterminada, Google recupera i creua una quantitat monstruosa de dades. No és suficient que l'empresa doni la possibilitat de limitar certes mesures per tal que esdevinguin lícites. **Qui ha activat ja les opcions que limiten la recol·lecció de dades personals per Google?** L'empresa intenta rentar la seva imatge deixant a l'usuari, mitjançant un acte voluntari, aquesta possibilitat, sabent molt bé que la majoria dels usuaris no ho faran. El consentiment, per tant, és furtat.

Afortunadament, el Regalment General de Protecció de Dades (RGPD), ha perfectament anticipat aquesta temptativa d'eludir la nostra voluntat. Concretament, especifica que, per ser vàlid, el nostre consentiment té que ser explícit: «no hi pot haver consentiment en cas de silenci, caselles marcades per defecte o inactivitat» (considérant 32). A més, les mesures de vigilància sobre les que Google pretén donar-nos cert control són **«acceptades» per defecte** a través de caselles premarcades. Com no es basen en el consentiment explícit, aquestes mesures són il·lícites – i les ataquem també.

Gmail

Google es permet a analitzar el contingut dels correus electrònics dels seus usuaris, tan enviats com rebuts. I així, l'empresa es permet també analitzar clarament la correspondència dels seus usuaris. I més furtiu encara, Google llegeix les converses entre els usuaris de Gmail tot i que mai els han donat el seu consentiment i ni tan sols han estat mai informats d'aquesta vigilància.

A més, tot i que Google ha anunciat que ja no vol analitzar el contingut dels correus electrònics amb fins publicitaris, les seves «regles» segueixen permetent-li fer-ho, cosa que fa que les seves declaracions siguin molt superficials.

En qualsevol cas, a més de l'anàlisi amb fins publicitaris, Google pretén seguir analitzant el contingut dels correus electrònics per «nodrir» els seus algoritmes de predicció (i els algoritmes de Google són a llarg plaç, probablement el més valuós de l'empresa).

Així, a Gmail, l'empresa presenta els seus algoritmes com assistents de gestió de cites i connexions, i mostra amb orgull la seva ambició: substituir els humans en la multitud d'opcions que jutja de «secundàries» (amb qui parlar, quan, per dir què), **perquè la humanitat es concentri en allò al que s'ha de dedicar - ser productiva.**

Per últim, en el que respecta a la seva activitat tradicional -la publicitat-, Google no s'amaga pas de seguir analitzant les metadades del correu electrònic (qui parla amb qui, quan i amb quina freqüència) per identificar més precisament els seus usuaris i els seus contactes. Aquest anàlisi també el trobem a l'aplicació de missatgeria instantània Allo: els missatges són per defecte enregistrats als servidors de Google. I encara pitjor, els missatges de veu són escoltats i

transcrits per Google, i l'usuari no s'hi pot oposar.

Aquestes metadades, creades «per màquines, per a màquines», són molt més fàcils d'analitzar automàticament que el contingut dels correus electrònics (escrit per humans, i per tant sotmesos a la subtilitat del llenguatge), i poden revelar informacions igualment íntimes: saber que, de cop, escrius a un especialista en càncer pot revelar més informació sobre el teu estat de salut que el detall del que dius, per exemple.

Aquí, al cor del negoci de Google, no es mira de deixar a l'usuari un mínim de control sobre el que pot ser o no analitzat – per usar Gmail, debem cedir plenament el nostre dret fonamental a la confidencialitat de les nostres comunicacions (així com la dels nostres contactes, malgrat ells).

Google ens rastreja a la Web

El 16% de la facturació de Google prové de les seves activitats de intermediació publicitària, que consisteix en connectar els anunciants amb «més de dos milions» de pàgines o blogs de tercers que volen remunerar-se amb publicitat dirigida. A cadascuna d'aquestes pàgines, és Google qui tècnicament coloca la publicitat, el que li permet posar també galetes i altres rastrejadors gràcies als quals pot seguir la navegació de tot internauta (inscrit o no als seus serveis). Un cop més, no hem consentit mai de manera vàlida aquest seguiment.

De la mateixa manera, Google ens segueix per les innombrables pàgines que utilitzen Google Analytics. Aquest servei, ajuda a les pàgines a analitzar la identitat dels seus visitants, deixant a Google accedir a aquestes informacions.

Un simple anàlisi del trànsit a pàgines com lemonde.fr, lefigaro.fr, hadopi.fr o defense.gouv.fr permet, per exemple, constatar que accedint a aquestes pàgines, diverses sol·licituds són enviades a *doubleclick.net* (gestor publicitari de Google) i/o *google-analytics.com*, permetent a Google conèixer, al menys, la nostra direcció IP, la configuració única del nostre navegador i l'adreça URL de cada entrada visitada a cadascuna d'aquestes pàgines.

Els responsables d'aquestes pàgines són tan responsables com Google d'aquest seguiment il·legal – ho atacarem més endavant – amb el que el gegant publicitari pot perfilar-nos encara més precisament.

Per últim, Google pretén estendre la seva presència a tota la Web, regulant ell mateix la publicitat: configurant el seu navegador Google Chrome (utilitzat pel 60% dels internautes) per tal que bloquegi els anuncis a qualsevol lloc de la Web que no compleixin els criteris (format, ergonomia...) decidits per l'empresa. El missatge és clar: «Si voleu fer publicitat en línia, utilitzeu els serveis de Google, us estalviareu molts problemes!».

Matant dos pardals d'un tret, Google pasa per un defensor de la vida privada (ja que bloqueja certs anuncis intrusius), però per un altre cantó, incita als internautes a desactivar els bloquejadors de tercers (com uBlocks Origin que neutralitza eficaçment gran nombre de rastrejadors de Google), ja que Google Chrome n'integra un per defecte i, finalment, incita encara més als editors de pàgines web a penjar **les seves** publicitats, i així integra **els seus** rastrejadors per tot arreu i en tot moment.

Youtube

La plataforma de vídeo més gran d'Internet (i la segona pàgina més visitada del món, segons Alexa), Youtube, pertany a Google.

Youtube no en té prou amb només allotjar vídeos: es tracta d'un veritable mitja social de continguts multimèdia que posa en relació a individus i en regula les seves relacions.

En efecte, després que un vídeo hagi sigut vist a Youtueb, en el 70% dels casos, l'usuari ha anat a espetegar a aquell vídeo a través de l'algoritme de recomanació de Youtube. Un antic empleat de Youtube, Guillaume Chaslot (veure l'entrevista al número 5 de la revista Vraiment, publicada el 18 d'abril de 2018), exposa les conseqüències d'aquest algoritme. L'objectiu de l'algoritme no és servir a l'usuari si no servir a la plataforma, és a dir, de **fer que restem a la plataforma el màxim de temps possible davant les publicitats**. L'empleat explica que després de penjar un vídeo, es mostra primer a un grup reduït de persones i, només es recomana a altres usuaris, si els del grup reduït han estat suficientment temps davant de la pantalla.

Aquest algoritme no cuestiona el contingut -la seva naturalesa, el seu missatge... A la pràctica, però, l'antic empleat constata que **els continguts més destacats són agressius, difamadors, chocants o complotistes**. Guillaume Chaslot compara: «És una baralla al carrer, la gent es para a mirar».

Necessàriament, entenem que, en resposta a aquest algoritme, el nombre de creadors de continguts s'han espontàniament adaptat, proposant continguts cada cop més agressius.

Amb l'objectiu d'aconseguir el màxim de visualitzacions, Youtube monitoritza la més mínima acció dels usuaris per posar-los en les condicions més favorables per rebre publicitat i exposar-los a aquesta publicitat el màxim de temps possible... però això no és tot!

Youtube, no volent perdre ni un segon de visionat dels seus usuaris, no s'arrisca a recomanar continguts massa extravagants i es contenta en deixar-los a la seva zona de confort. L'antic empleat declara que s'ha refusat diverses vegades modificar l'algoritme de manera que obri a l'usuari contingut no habituals. En aquestes condicions, el debat públic està completament distorsionat, les discussions més subtils o precises, jutjades poc rentables, s'exposen a una censura per enterrament.

A més, Youtube es beneficia d'un estatus d'amfitrió i, per tant, *a priori*, no es considera responsable dels comentaris realitzats a la seva plataforma. D'altra banda, però, està obligat a eliminar continguts «manifestament il·lícits» que li hagin estat notificats. Donada la quantitat de continguts que hi ha a Youtube, s'ha decidit automatitzar la censura dels contingut potencialment «il·lícits», infringint així els drets d'alguns «autors», a través del seu *RobotCopyright*, anomenat «ContentID». Per ser reconegut com a «autor» a la plataforma, cal respondre a criteris fixats per Youtube. Un cop que un contingut està protegit per aquest dret atribuït per Youtube (a la pràctica, es tracta majoritàriament de grans cadenes de televisió), la plataforma es permet desmonetitzar o suprimir els vídeos reutilitzant el contingut «protegit» a petició dels seus «autors».

Un altre forma de censura que demostra que Youtube no vol permetre a cadascú d'expressar-se (contràriament al seu eslògan «Broadcast yourself») si no que simplement busca **administrar l'espai de debat públic** per afavorir la centralització i el control de la informació. I per bones raons, **aquesta censura i aquest confinament a un espai de confort és la millor manera d'empresonar els usuaris al seu ecosistema al servei de la publicitat.**

Contràriament al que Google intenta fer-nos creure, la vigilància i la censura no són la condició inevitable per intercanviar vídeos en línia. Podem, perfectament, fer-ho respectant totalment els nostres drets. PeerTube és una plataforma de compartició de vídeos que proposa les mateixes

funcionalitats que Youtube però funciona amb diferents mecanismes. Els vídeos no estan tots allotjats al mateix lloc: qualsevol pot crear la seva instància i allotjar vídeos. Les diferents instàncies estan connectades entre elles. Cada instància té les seves pròpies regles, i no hi ha pas una política de censura unificada com a Youtube, i sobretot, aquestes regles no són dictades per una lògica comercial.

Infiltració de codi obert a Android, el cavall de Troia de la vigilància

Google porta el programa Android, el seu sistema operatiu per telèfons intel·ligents. Al difondre eines reutilitzables amb l'objectiu d'«ajudar» als desenvolupadors de programari a desenvolupar aplicacions mòbils per Android, Google ha aconseguit que les seves «pràctiques» siguin àmpliament adoptades per molts desenvolupadors: **els codis difosos, sovint contenen rastrejadors de Google** i estan integrats a moltes aplicacions que, *a priori*, no tenen absolutament cap raó per revelar informació a l'empresa sobre les seves usuàries.

Això és el que l'associació Exodus Privacy revela perfectament: rastres d'anuncis de Google Ads, Firebase Analytics, Google Analytics ou DoubleClick han estat trobats al codi de més de 3000 aplicacions analitzades, com Deezer, Spotify, Uber, Tinder, Twitter, Le Figaro, L'Equipe, Crédit Agricole, Boursorama o Angry Birds.

Google intenta rentar regularment la seva imatge dins de la comunitat del programari lliure. És per això que les fonts d'Android són lliures de drets. Però això no significa que el seu desenvolupament sigui obert: Google tria gairebé sol les direccions en el desenvolupament del sistema.

D'altra banda, a més del sistema Android *stricto sensu*, Google imposa als fabricants de telèfons intel·ligents posar als seus productes les galetes que són les seves aplicacions. De fet, sent com és el mercat d'aplicacions, els fabricants de telèfons consideren que un telèfon Android no es vendrà pas si no integra la Play Store (tenda d'aplicacions) proporcionat per Google.

A més, per poder accedir a la tenda Play Store, un telèfon ha de tenir les aplicacions de monitorització de Google. Aquests serveis de Google amplien les capacitats del sistema i, de vegades, esdevenen indispensables per fer funcionar algunes aplicacions, el que permet a l'empresa de realitzar un seguiment de les usuàries de telèfons intel·ligents: la geolocalització contínua permet a Google conèixer els hàbits de desplaçament de les seves usuàries; la llista de xarxes WiFi és enviada a Google inclús si la usuària ha desactivat la connexió WiFi del seu telèfon; la Play Store imposa sincronitzar un compte de Google, permetent una verificació creuada de dades encara més detallada.

I, evidentment, aquests serveis Google no són lliures. Android esdevé, doncs, el pretext del codi obert per posar a la butxaca de l'usuari tota una sèrie d'aplicacions Google amb l'objectiu d'espiar. Això no impedeix que l'empresa comuniqui massivament sobre els seus projectes lliures, molt sovint interessats, com la seva darrera eina lliure de seguiment.

Finalment, la integració de Play Store assigna automàticament un identificador publicitari únic a cada usuari. Aquest identificador es posa gratuïtament a disposició de totes les aplicacions i, com si fos una «mega-cookie», permet a les aplicacions de rastrejar el comportament dels seus usuaris a tots els serveis utilitzats. Aquí, les eines de vigilància de Google són oferides gratuïtament als desenvolupadors de tercers amb l'objectiu d'atraure el major nombre possible d'aplicacions a Android -on Google, dalt d'aquesta estructura, podrà vigilar lliurement a tothom.

Apple

Apple, la més rica de les GAFAM, obté els seus beneficis de la venta al públic dels seus aparells (iPhone, Mac, iPad...) equipats pels seus sistemes operatius.

El seu model de negoci es basa en **empresonar els seus usuaris** a la seva plataforma: dissuadir-los a consumir altres aplicacions i empènyer-los a consumir cada cop més Apple.

En aquesta estratègia, Apple proveeix gratuïtament a les aplicacions que arriben a la seva plataforma, una **mega-galeta** que permet rastrejar cada usuari. Però ho fa **sense el nostre consentiment** explícit, cosa que és il·legal.

Anàlisi d'Apple

L'empresa Apple

Apple té un volum de negoci anual de 200.000 milions d'euros i una reserva de tresoreria equivalent (per comparar, el pressupost anual de l'estat francès és d'uns 300.000 milions). A la Borsa, el total de les accions de l'empresa valdria ara 1 bilió de dòlars, el que la converteix en **la major capitalització borsària del món**.

Fundada al 1976, particularment per Steve Jobs i força abans de l'arribada d'Internet, l'empresa es centra en la venta dels seus propis ordinadors, equipats de sistemes operatius que desenvolupa ella mateixa.

Al 1984, Apple anuncia el llançament del seu Macintosh a través d'un vídeo publicitari dirigit per Ridley Scott, ingenuament titulat «1984» i posant l'empresa com a estendard contra una futura societat de vigilància (el vídeo original està disponible a disponible a YouTube, però nosaltres preferim el gir que en fan els nostres amics de la Startuffe Nation!). Així com l'eslògan intern de Google, «Don't be evil» (No siguis malvat), la postura presa a 1984 per Apple no és més que una sinistra **anti-profecia**: l'empresa jugarà un rol decisiu en la transformació de les eines digitals en termes de bloqueig i control.

A partir de llavors, Apple no deixarà de brillar per les seves **estratègies de comunicació, tan confuses com insidioses**: el seu famós lema **«Think different»** (Pensa diferent) no dient-nos «què» seria pensar diferentment, ens demana sobretot, i en realitat, que pensem diferentment «sobre nosaltres mateixos» (sobre la nostra singularitat) per «pensar Apple» i fondre'ns en un «cool» (guai) molt comú.

Al 2007, fa poc més de 10 anys, es va llançar l'iPhone. Les seves venten han emplaçat l'empresa a la seva situació econòmica actual, i representa el 70% de la seva facturació (l'altre 30% es reparteix equitativament entre les ventes d'iPad, de Mac i de serveis). Avui dia, al voltant d'**un telèfon intel·ligent de cada cinc** venut al món és venut per Apple.

El model Apple

El model econòmic d'Apple, centrat en la venta al públic de dispositius, reposa en el bloqueig dels seus clients: assegurar-se que només compraran material Apple. Per això, l'empresa manté un control total sobre l'ús que els seus clients poden fer dels productes que compren.

Els sistemes operatius de les màquines Apple - **iOS i Mac OS** - **són pures caixes negres**: el seu codi font es guarda en secret, impedint que es pugui prendre consciència del seu funcionament per adaptar-lo a les nostres necessitats, fora del control d'Apple.

La seva App Store és també una perfecta il·lustració d'aquesta presó daurada: Apple **limita el programari descarregable segons els seus propis criteris**, assegurant-se que els usuaris només tinguin accés a serveis de tercers «de qualitat» - conforme al seu model econòmic i a la seva estratègia d'empresonament (Apple s'emporta el 30% del preu de venta de les aplicacions de pagament, així que hi ha molt interès a afavorir-les).

Per últim, un cop que els seus usuaris han pagat per utilitzar els diversos programari no-lliures a través de l'App Store, els és força difícil, econòmicament, de recórrer a altres sistemes que no siguin Apple, o l'accés a certs d'aquests programes no seria ja possible, o es malgastaríem els diners volent comprar-los.

L'empresonament és perfecte.

Un tancament (també) material

Desafortunadament, el model d'empresonament d'Apple no es limita només al programari: la connectivitat dels iPhones no és compatible amb l'estàndard Micro-USB utilitzat per tots els altres fabricants, el que obliga a comprar cablejat específic. De la mateixa manera, els darrers models iPhone no tenen entrada pels auriculars, el que obliga a comprar un adaptador suplementari si no es desitja utilitzar els auriculars Bluetooth d'Apple.

L'última caricatura a aquest model és el nou altaveu d'Apple, HomePod, que requereix un iPhone per instal·lar-se i **només pot reproduir música principalment proveïda pels serveis d'Apple** (iTunes, Apple Music...).

Per últim, una vegada que Apple pot controlar totalment l'ús dels seus aparells, el camí és obert per **programar l'obsolescència** i empènyer a la compra d'aparells més recents. Així, el passat hivern, acusada per observadors exteriors, l'empresa es va veure obligada reconèixer que les actualitzacions havien ralentitzat deliberadament els models vells dels seus telèfons.

Apple ha explicat que aquest canvi es va fer per protegir els telèfons més antics amb bateries gastades. Però la seva resposta, sigui sincera o no, només posa en relleu el veritable problema: els iPhone són concebuts per no permetre ni reparacions ni simples canvis de bateria. Ralentitzar els vells models només és «útil» en la mesura en que **no són concebuts per durar**.

Vida privada: un fals amic

Apple ven sobretot aparells, i la vigilància massiva no és *a priori* tan útil per ella com per les altres GAFAM. És per això que l'empresa aprofita l'oportunitat per presentar-se com una defensora de la privacitat. Per exemple, el seu navegador web, Safari, les galetes de tercers, que són utilitzades per rastrejar l'activitat d'una persona a diferents llocs d'Internet, estan bloquejades per defecte. L'empresa presenta això com una mesura de protecció a la privacitat, i és veritat, però és també per ella, una manera de portar el mercat de la publicitat vers el sector de les aplicacions mòbils, on no solament **el rastreig no està bloquejat, ans el contrari, és directament ofert per Apple.** Això és el que nosaltres ataquem.

Una definició «fora de la llei» de les dades personals

En el seu «acord de confidencialitat», que estem obligats a acceptar per utilitzsar els seus serveis, Apple s'autoritza a usar les nostres dades personals en alguns casos limitats, donant-se la imatge d'empresa respectuosa amb els seus usuaris.

Tot i així, i d'immediat, Apple s'autoritza a **«recol·lectar, utilitzar, transferir i divulgar dades no personals amb qualsevol fi»**, incloent entre aquestes dades:

- «el lloc de treball, l'idioma, el codi postal, l'indicador regional, l'**identificador únic** de l'aparell, l'URL de referència»;
- «la **localització** i el fus horari des dels quals un producte Apple és utilitzat»;
- L'ús de serveis Apple, «comprèn les **cerques** que feu», aquestes informacions no són associades a l'adreça IP de l'usuari, «excepte en casos molt excepcionals per assegurar-se la qualitat dels nostres serveis en línia»

Aquesta llista rebel·la que la definició de «dades personals» utilitzada per Apple és **ben diferent a aquella utilitzada pel dret europeu**. Al dret europeu, una informació és una dada personal des del moment que pot ser associada a una persona única, poc importa que la identitat d'aquesta persona sigui coneguda o no. Tot i així, l'identificador únic de l'aparell, l'adreça IP o, en alguns casos també, les cerques efectuades o la localització, es poden associar a una persona única per elles mateixes.

Així mateix, l'empresa precisa que «si associem les dades no-personals a dades personals, les dades combinades seran tractades com dades de caràcter personal». De fet, les dades que ella anomena «no-personals» i que associa juntament **constitueixen ja dades personals**, que el dret europeu prohibeix d'utilitzar «amb qualsevol fi». Però és el que Apple ens demana d'acceptar per utilitzar els seus serveis (i sense que sapiguem fins a quin punt utilitza o utilitzarà aquest xec en blanc).

La mega-galeta

A part de la immensa incertitud respecte als poders que Apple s'atorga a través de la seva errònia definició de «dades no-personals», un perill és ja perfectament actual: l'**identificador publicitari únic** que Apple proporciona a cada aplicació.

Com ja hem vist a Google (el funcionament és idèntic), Apple associa a cada aparell un identificador únic amb fins publicitaris. Aquest identificador és accessible a cada aplicació instal·lada (l'usuari no és convidat a autoritzar-ne l'accés, que es dóna automàticament).

Aquest identificador, **encara més eficaç que una simple «cookie»** (galeta), permet individualitzar cada usuari i, així, rastrejar detalladament les seves activitats a totes de les seves aplicacions. Apple, doncs, proveeix a altres empreses (a tercers) d'una eina decisiva per establir el perfil de cada usuari – per sondejar el nostre esperit amb la finalitat de millor manipular-nos, d'enviar-nos la publicitat adequada en el moment adequat (exactament de la mateixa manera que ho descrivim en relació a Facebook).

És fàcil comprendre l'interès d'Apple: **atraure el major nombre d'aplicacions a la seva plataforma**, amb el fi que elles atraguin al major nombre d'usuaris possible, que es trobaran atrapats al sistema Apple.

Com ja s'ha mencionat, s'anima a les empreses terceres a anar a l'App Store (tenda d'aplicacions Apple) ja que Apple els impedeix usar les saboroses «galetes de tercers» a la web, - que Safari bloqueja de forma predeterminada. De fet, quin sentit té lluitar contra Apple per controlar la població a les pàgines d'Internet si la mateixa empresa ofereix gratuïtament els mitjans per fer-ho a les seves aplicacions? La protecció oferta per Safari sembla cínica.

Un identificador il·legal

Contràriament a la mega-galeta oferta per Google a Android, la d'Apple és pot desactivar: l'usuari li pot donar valor «0». Al fer-ho, Apple pretén «deixar l'opció» de sotmetre's o no a la vigilància massiva que permet.

Tot i així, aquesta elecció és il·lusòria: al moment d'adquirir i d'instal·lar un aparell, la mega-galeta d'Apple **s'activa per defecte**, i l'usuari no és convidat a fer cap mena de decisió en el que això respecta. Només més tard, si l'usuari és conscient de l'opció apropiada i en comprèn el funcionament i el valor, pot realment prendre aquesta decisió. I Apple sap molt bé que la majoria dels seus clients no tindran aquesta consciència o aquesta comprensió, amb el que, en realitat, no se'ls hi haurà donat cap opció.

I això és que el la llei exigeix. La directiva «ePrivacy» exigeix el consentiment de l'usuari per accedir a les informacions contingudes a la seva màquina, com el de la mega-galeta. El reglament general sobre protecció de dades (RGPD) exigeix que aquest consentiment sigui donat de forma explícita, mitjançant una acció expressa per acceptar l'accés a les dades. Tot i així, Apple no demana mai aquest consentiment, considerant que ha estat donat per defecte.

Per respectar la llei, al moment de la instal·lació de l'aparell, hauria d'exigir **que l'usuari triés si vol o no ser associat a un identificador publicitari únic**. Si l'usuari refusés, hauria de poder acabar la instal·lació i usar lliurement l'aparell. I això és el que nosaltres exigirem col·lectivament davant la CNIL.

A més, la solució que nosaltres exigim és la mateixa que va ser adoptada per Microsoft l'estiu passat per tal que Windows 10 complís la llei quan el CNIL el reprovà amb crítiques similars a les que estem fent avui. Si Apple vol veritablement respectar els drets dels seus usuaris, com avui pretén hipòcritament, **el camí és mostra ben clar**.

Si no pren aquest camí, serà la GAFAM amb la sanció més rentable d'Europa, amb un import màxim de **8.000 milions d'euros**. I així, començaríem a reequilibrar les conseqüències de la seva **evasió fiscal**, que ja li ha costat una multa de 13.000 milions d'euros al 2016, però que encara està per pagar (per aprofundir en aquest aspecte, més enllà de la nostra acció centrada sobre a les dades personals, recomanem les accions conduïdes per ATTAC).

Facebook

Com que la nova llei europea entrarà en vigor properament, Facebook s'aferra a les seves posicions i defensa el seu model econòmic anunciant que els seus serveis seguiran sent **accessibles per als usuaris que es neguin a ser atacats**.

És aquest contracte il·legal, aquest intercanvi de «servei contra llibertats» del que Facebook és el més flagrant dels exemples, la llavor de les nostres accions de grup.

Més enllà de la il·legalitat del seu model, vegem conseqüències concretes de la seva activitat sobre les nostres llibertats.

Anàlisi de Facebook

L'empresa Facebook

Facebook va ser creat fa 14 anys per Mark Zuckerberg, -el seu actual director general-, i compta amb 25 000 treballadors. La seva facturació de 30 000 milions d'euros deu el seu 98% a la publicitat proposada a **2 200 milions d'usuaris actius**. La pàgina web de Facebook seria la tercera més visitada d'Internet (segons Alexa), però l'empresa també és propietària de WhatsApp i Messenger (serveis de missatgeria), així com d'Instagram (xarxa per compartir imatges i vídeos, i dissetè lloc més visitat d'Internet).

L'empresa explica sense pudor el seu funcionament: les persones que volen difondre un missatge (una publicitat, un article, un esdeveniment, etc.) designen un públic objectiu a Facebook segons determinats criteris socials, econòmics o de comportament, i paguen a l'empresa per tal que difongui el missatge a aquest públic en les millors condicions.

Aquest funcionament implica dues coses: **conèixer** cada usuari, i penjar els missatges al bon moment i en el bon format per tal d'**influenciar** millor el públic objectiu.

Anem a detallar com ho fa Facebook.

El que Facebook analitza

Facebook explica a la seva Política d'utilització de dades que analitza les informacions següents:

- els continguts públics (text, imatge, vídeo) que es difonem a la seva plataforma (és el més evident, però no és pas aquest el contingut més útil per a l'empresa)
- els missatges privats enviats a Messenger (qui diu què, a qui, quan, amb quina freqüència)
- la llista de persones, pàgines i grups que seguim o «ens agraden», així com la manera que interactuem amb elles
- la manera que utilitzem el servei i accedim als continguts (els articles, les fotos i els vídeos que veiem, comentem o «ens agraden», en quin moment, amb quina freqüència i quanta estona)

- les informacions de l'aparell amb el qual accedim al servei (adreça IP, identificador publicitari de l'aparell, nom de les aplicacions, fitxers i plugins instal·lats, moviments del ratolí, punts d'accés Wi-Fi i torres de telecomunicació properes, accés a la localització GPS i a la càmera de fotos)

L'empresa explica, sempre sense pudor, que analitza les dades per proposar-nos continguts de pagament de la manera més «adaptada» (a saber: de la manera més subtil, per captivar la nostra atenció).

Com veiem, la majoria de les dades analitzades per Facebook no són les que publiquem espontàniament, però sí aquelles que **sorgeixen de les nostres activitats**.

De l'anàlisi de totes aquestes dades resulta un nou joc d'informacions, que són les més importants per Facebook, per això l'empresa no ens deixa tenir cap control sobre elles. Aquest joc d'informacions són el conjunt de les característiques socials, econòmiques i de comportament que la xarxa associa a cada usuari amb l'objectiu d'aconsellar-lo millor.

El que Facebook sap de nosaltres

Al 2013, la universitat de Cambridge va realitzar l'estudi següent: 58 000 persones van respondre a un test de personalitat, i aquest test va ser creuat amb tots els seus «m'agrada» a Facebook. Només amb els «m'agrada», la universitat de seguida va poder estimar **el color de la seva pell** (amb un 95% de certesa), la seva **orientació política** (85%) i **sexual** (80%), la creença religiosa (82%), si fumaven (73%), bevien (70%) o consumien altres drogues (65%).

Aquesta estudi ha permès posar llum al profund funcionament de l'anàlisi de masses: quan moltes informacions poden ser creuades en un gran nombre de persones (més de 2 000 milions a Facebook, recordem-ho), **nombroses correlacions** apareixen, donant l'esperança, -fundada o no-, de revelar automàticament (sense anàlisi humà) el detall de la personalitat de cada individu.

Avui, Michal Kosinski, l'investigador que va dirigir aquest estudi, continua denunciant els perills de l'anàlisi de masses automàtic: explica (EN) que, en un determinat anàlisi de masses, simples imatges podrien revelar l'orientació sexual d'una persona, les seves opinions polítiques, el seu coeficient intel·lectual o la seva predisposició criminal. La rellevància de les correlacions resultants d'aquests anàlisis de masses és el mètode de funcionament d'empreses com Cambridge Analytica, que ha tingut **conseqüències polítiques** rellevants.

Una aplicació -tan reveladora com inquietant- d'aquests mètodes és l'ambició (EN) declarada de Facebook per detectar automàticament les persones amb **tendències suïcides**. Més enllà d'aquesta discutible iniciativa (ja que, lluny de ser una empresa social, es dedica a vendre publicitat), Facebook revela aquí l'amplitud i el detall de les informacions sobre nosaltres que espera deduir dels anàlisis massius que porta a terme.

Com Facebook ens influencia

Un cop que l'empresa s'ha fet una idea bastant precisa de qui som, dels nostres desitjos, de les nostres pors, del nostre mode de vida i les nostres febleses, té el camí lliure per proposar-nos

els seus missatges al bon moment i amb el bon format, quan més puguin influenciar la nostra voluntat.

L'empresa s'ha banat de l'amplitud de la seva influència. Al 2012, va sotmetre 700 000 usuaris a una experiència (sense demanar el seu consentiment ni informar-los). Facebook modificava el mur d'aquestes persones de manera que es mostraven en primer lloc continguts que influenciarien el seu humor, esperant posar-los més contents en alguns casos i més tristos en altres. L'estudi concloïa que «els usuaris començaven a **usar paraules més negatives o positives** en funció del contingut al que havien estat «exposats».

Aquest experiment no ha fet més que revelar el normal funcionament de Facebook: per tal d'influenciar-nos, **jerarquitza les informacions** que podem consultar als seus serveis (el mur d'activitat només representa una petita part dels continguts difosos per les persones a qui seguim, i aquests continguts són seleccionats i triats per Facebook).

Aquesta jerarquització de la informació no en té prou amb esclafar la nostra llibertat de consciència personal: també vol **distorsionar totalment el debat públic**, en funció de criteris purament econòmics i opacs, com la sobre-difusió de «fakenews» que només és un dels nombrosos símptomes.

En el seu estudi anual de 2017, el Consell d'Estat francès es va posar en guarda contra la pretesa neutralitat dels algoritmes implicats en la tria de continguts: els algoritmes estan al servei de la maximització econòmica en benefici de les plataformes, així que són concebuts per afavorir els beneficis i no pas la qualitat de la informació.

Per què és il·legal?

A les seves condicions d'ús, revisades per l'entrada en vigor de la LOPD, Facebook explica que es considera autoritzat a controlar i influir en els seus usuaris amb l'argument que han donat el seu consentiment a un contracte que així ho preveu. Però aquest contracte no és suficient per garantir la legalitat d'aquestes pràctiques.

La RGPD estableix que el nostre consentiment no és vàlid perquè no és lliure, «si l'execució d'un contracte, inclosa la prestació d'un servei, està subjecta a un consentiment pel tractament de les dades de caràcter personal que no sigui necessari per l'execució del contracte» (article 7, considerant 43 del RGPD, interpretats pel grup de l'article 29).

Aquest requisit de lliure consentiment afecta la validesa de les disposicions del contracte amb Facebook que permetrien a l'empresa vigilar-nos i influir en nosaltres.

Al 2017, la CNIL ha condemnat a Facebook amb 150 000 euros de multa per haver realitzat les seves operacions de tractament sense base legal, considerant que «l'objectiu principal del servei és la creació d'una xarxa social [...], que la combinació de dades dels usuaris tingui **finalitats publicitàries no correspon ni a l'objectiu principal del contracte** ni a les raonables expectatives dels seus usuaris [i que, per tant, és responsabilitat de Facebook] de vetllar per tal que els drets de les persones siguin respectats i, en particular, a que l'execució d'un contracte no les porti a renunciar-hi». Així, la CNIL «considera que les empreses no poden basar-se en l'obtenció del consentiment dels seus usuaris [ni] de la necessitat lligada a l'execució d'un contracte».

Donat que el contracte amb Facebook no permet la monitorització descrita anteriorment, és il·legal, i aquest és el nucli de les nostres accions de grup! Desafortunadament, les malifetes de Facebook van més enllà del seu propi lloc web.

Com Facebook col·labora amb tercers

Facebook ja no amaga la seva activitat de seguiment una mica per tot arreu de la Web, ni tan sols de les persones que no hi tenen compte (i a les que se'ls hi crea «perfils fantasma»).

Els mètodes de seguiment són nombrosos:

- les *cookies* o **galetes** (fitxers enregistrats al vostre aparell que permeten a Facebook identificar-vos d'un lloc a un altre
- els botons **«m'agrada»** o **«compartir»** que apareixen a nombroses pàgines (aquests botons, allotjats als servidors de Facebook, són directament descarregats per l'usuari, indicant així, automàticament, la seva adreça IP, la configuració única del seu navegador i la URL de la pàgina visitada
- Els **píxels invisibles** (imatges transparents de 1x1 píxels) que funcionen com els botons, i que el seu únic objectiu és ser descarregats per transmetre a Facebook les informacions de connexió
- el **login de Facebook**, que alguns llocs web o aplicacions tenen (Tinder, per exemple) s'usen com a eina per identificar els seus usuaris

Rarament s'informa les persones, i el seu consentiment no és obtingut. Facebook evita aquesta responsabilitat traslladant-la als altres llocs o aplicacions que han integrat els seus rastrejadors. Tot i que aquests llocs són jurídicament responsables, Facebook ho és també, ja que l'empresa ha estat **regularment condemnada** per aquest seguiment il·lícit sense, per tant, posar-hi remei:

- del 2015 al 2018, la CNIL a més de la justícia belga, li han demanat de posar-hi remei, amb una multa de 250 000 euros per dia
- al 2017, la CNIL francesa l'ha condemnat a 150 000 euros de multa (import màxim a l'època)
- al 2017, la CNIL espanyola l'ha condemnat a 1 200 000 d'euros de multa

Facebook et rastreja també al mòbil

L'empresa no només s'interessa en els hàbits de navegació dels internautes. Les aplicacions de telefonia mòbil són igualment un objectiu. Proveint una sèrie d'eines als desenvolupadors d'aplicacions, Facebook s'incrusta en aquest nou món. Tan aviat com una aplicació vol connectar-se a Facebook per una raó o altra, un cert nombre de dades personals són transmeses, sovint sense relació directa amb l'objectiu inicial de l'aplicació i, sovint també, sense que l'usuari no en sigui informat.

L'associació Exodus Privacy ha posat en evidència l'omnisciència d'aquests rastrejadors a les aplicacions mòbils. Si bé alguns rastrejadors mostren les seves intencions (arribar als usuaris amb finalitats publicitàries), altres funcionen de forma totalment opaca. Així, hem pogut observar que l'aplicació Pregnancy + recol·lecta les informacions privades de l'infant a nàixer (amb l'objectiu d'acompanyar les famílies en la seva naixença) i les transmet a Facebook (setmana d'embaràs i mes de naixement esperat). Al seu lloc web, l'aplicació explica simplement que transmet a tercers certes dades per assegurar el bon funcionament del servei. **Gràcies a Pregnancy +, el vostre infant ja pot tenir compte a Facebook fins i tot abans de nàixer!**

Un altre flagrant exemple: analitzant les dades emeses per l'aplicació Diabetes:M, es constata que envia a Facebook «l'identificador publicitari» de l'usuari, donant així a Facebook una **llista de persones amb diabetis**. Però al seu lloc web, l'aplicació es limita a explicar que treballa amb xarxes publicitàries, sense més detall...

Whatsapp i Instagram

Evidentment, la vigilància exercida per Facebook s'estendrà a les seves grans filials: a la seva missatgeria, WhatsApp; i a la seva xarxa social d'imatge i vídeo, Instagram.

La compra de WhatsApp ha aportat llum al comportament de la casa mare. La Comissió Europea ha sancionat Facebook amb una multa de 110 milions d'euros en virtut de la llei de competència, i després la CNIL francesa s'ha pronunciat en termes de dades personals. El desembre passat, va demanar a Facebook que deixés d'exigir als usuaris de WhatsApp que acceptessin que la seva informació de l'aplicació de missatgeria es transfereixi a la xarxa social.

Un cop més, fou el **consentiment explícit** el que mancava: WhatsApp no podia ser utilitzat sense donar el seu consentiment a mesures purament publicitàries. I això, avui, està totalment prohibit.

Com sobreviuria Facebook si no es financés amb les nostres dades?

El model econòmic de Facebook està sent posat en dubte. Ja no està permès remunerar un servei que va en contra de les llibertats fonamentals de les seves usuàries. Facebook potser no desapareixerà, però ja no podrà seguir obtenint els seus recursos de la mateixa manera.

Però, què importa?: **no necessitem a Facebook** per continuar utilitzant serveis gratuïts i de qualitat. Ja existeixen nombroses alternatives als serveis de les GAFAM que són realment gratuïts (és a dir, que no impliquen «monetitzar» les nostres llibertats), perquè el seu finançament reposa sobre el model original d'Internet: la **descentralització**, que permet la mutualització de les despeses d'emmagatzematge, càlcul i ample de banda.

Per exemple, La Quadrature du Net proveeix a 9 000 persones l'accés a la xarxa Mastodon, una alternativa a Twitter lliure i descentralitzada. Nosaltres proveïm d'aquest accés a Mamot.fr, que és un dels milers de nodes de la xarxa que interconnecten entre si. Això permet **repartir les despeses** entre nombrosos actors que poden sostenir la infraestructura més fàcilment (sense haver-se de finançar a través de la vigilància de masses).

Unir-nos col·lectivament a aquestes alternatives és l'objectiu final de les nostres accions, però creiem que només podrem aconseguir-lo un cop que totes i cadascuna de les persones siguin alliberades del control de les GAFAM. Llavors, podrem construir la Internet dels nostres somnis, -**lliure i descentralitzada**-, que el nostre aliat Framasoft ja està construint dia a dia!

Microsoft

Vam anar a conèixer la Julie, que havia treballat per una empresa encarregada de «millorar» el funcionament de Cortana, l'assistent vocal de Microsoft, **escoltant una a una diverses paraules** captades per la màquina (voluntàriament o no).

Compartim aquí el seu inspirador testimoni. Qui escolta les vostres converses quan utilitzeu un assistent vocal com Cortana? Qui mira les vostres cerques quan utilitzeu motors de recerca com Bing? "Ningú", us asseguren els creadors d'aquests dispositius, «són màquines les que ho fan». La realitat és una altra, com ens explica aquest testimoni: una noia que, sense contracte de treball i sense cap acord de confidencialitat, ha **transcrit milers de converses privades**, cerques d'informació, noms i dades personals de persones que utilitzen productes de Microsoft.

Testimoni de la Julie: transcriure per Cortana

Som de camí per anar a veure la Julie, que ha treballat per a una empresa que ha ajudat a desenvolupar Cortana, l'assistent vocal de Microsoft. Esperem que ens pugui explicar com funcionen aquests tipus de serveis.

-Julie, bon dia

-Bon dia

-Has contactat La Quadrature du Net comentant que havies treballat per aquesta empresa. En què consistia exactament la feina?

-El nostre treball es basava en les dades que recol·lectava Cortana. Quan la gent s'adreçava a Cortana, ella ho enregistrava tot i Microsoft donava les dades a la companyia per a la que jo treballava. Nosaltres, els i les transcriptores, ens connectàvem a una plataforma de treball on teníem accés a totes les transcripcions, a tots els discs durs enregistrats per Cortana, i les havíem de tractar una per una, escoltant un a un tots els enregistraments que Cortana havia fet de les usuàries franceses. Es mostrava un text adjunt amb el que Cortana havia entès i havíem de corregir totes les faltes que havia fet, siguessin de comprensió, d'ortografia, de gramàtica, i a més, havíem de detallar els element sonors que hi havia a l'enregistrament.

-A quin tipus d'informació tenies accés?

-Hi havia de tot, qualsevol cosa. Hi havia enregistraments de cerques en línia, algunes coses poc importants com «Ei, Cortana, quin temps farà avui?» o «Quin temps farà demà?». Hi havia tot tipus dades perquè es recol·lecta molta cosa. Hi havia converses en línia, ja siguessin amb els serveis Xbox de la gent que juga en xarxa, o també de converses de Skype de les persones que usen el servei de traducció instantània. Així que teníem accés converses privades, de vegades a coses molt personals i íntimes. Hi havia també les cerques a Internet on les converses eren directament amb Cortana. Hi ha gent que parla a Cortana i li pregunta coses com «Ei, Cortana, és que puc ser feliç sol?». De vegades, hi ha gent que se sent terriblement trista i parla a Cortana per pujar la moral. Per les recerques a Internet hi havia realment una pila de coses, i com us podeu imaginar, també hi havia les cerques pornogràfiques dels usuaris, que demanaven «Ei, Cortana, busquem vídeos d'aquesta categoria o d'aquesta altra». Hi havia moltíssimes adreces perquè la gent programava el seu GPS també amb això, així que podíem veure l'adreça de casa seva, del seu metge o del seu advocat. Realment, tot passava per les nostres orelles. Un cop, hi havia una dona que treballava d'advocada i teníem accés als noms de les persones per a qui treballava. La dona dictava informes on, tot i ser fragmentaris podia haver-hi detalls rellevants.

Sovint, Cortana enregistrava sense que ningú li demanés, amb el que escoltàvem converses que no havien de ser enregistrades: gent que es discutia al cotxe o amb els fills, gent menjant o anant al lavabo. Hi havia gent que se n'adonava i s'enfadaven molt, així que sentia sovint «Puta Cortana!» i ho havia de transcriure. Hi havia moltes dades d'enregistraments no sol·licitats però, tot i així, Microsoft recol·lectava la informació.

Després, les transcripcions es fragmentaven en petites porcions anònimes pels transcriptors, així que no teníem identificadors dels usuaris de Microsoft però sempre hi havia detalls de noms, d'adreces o de números de telèfon. Mai de números de targeta de crèdit però sí de la seguretat social.

-Així que teníeu informació de tot tipus de gent. Dels infants també?

-Sí, n'hi havia molts als enregistraments que teníem. Moltíssims. De vegades quan jugaven en línia o feien les seves cerques a Internet.

-Imagino que vas haver de signar un contracte amb una clàusula de confidencialitat.

-No, no teníem cap contracte. Jo mai he firmat un contracte de confidencialitat, només calia inscriure't a la plataforma i allà acceptaves les condicions d'ús. De fet, abans d'acceptar no sabia ben bé en què consistia la feina.

-Com vas trobar aquesta feina?

-Buscava feina i vaig veure una oferta. Les condicions eren de comprendre anglès perquè totes informacions estaven en anglès, i d'escriure bé francès. Hi havia una formació en línia i passaves un examen. No havies de donar el currículum ni hi havia entrevista personal amb ningú. Realment, no demanaven res. Passaves l'examen i ja tenies accés a tot.

-Quin tipus de contracte vas signar?

-Jo treballava sense contracte de treball i en règim d'autònoms, així que no hi havia ni contracte de treball ni de confidencialitat. Tampoc cotitzàvem i no teníem cap protecció social, així que era un treball precari on havíem de fer almenys deu hores de treball per setmana. Però en podíem 45 o més, tantes com volguéssim perquè no hi havia restriccions en aquest sentit. En general, se'n feien unes 20 o 25 perquè no es poden fer 35 hores de transcripció, és una feina molt intensa que requereix molta concentració. I n'havíem de fer, de mitja, de 120 a 160 transcripcions per hora, així que era molt, sobretot per trobar totes les faltes gramaticals, i d'ortografia, i verificar els noms... No és fàcil...

-A partir de treballar amb aquesta empresa, et vas adonar que alguna cosa no anava bé? Hi ha molta gent que fa aquesta feina... No només per Cortana, sinó per altres assistents vocals que funcionen exactament de la mateixa manera. Tot i així, ets la primera a denunciar això.

-Sí, molta gent fa aquesta feina. Quan vaig començar buscaven 50 transcriptors francesos. Però també en buscaven per moltes altres llengües com àrab o el francès canadenc. I sí, ho trobava una xocant però era una feina pràctica i podies tenir molta llibertat.

-Quan veus gent que usa aquest tipus de servei, què et vindria de gust dir-els-hi?

-Els diria que paressin perquè, realment, es recol·lecta moltes dades personals. I no és normal que hi hagi gent que pugui tenir accés a tota aquesta informació, ja sigui gent com jo que no he signat cap contracte de confidencialitat, o inclús les empreses com Microsoft. És massa personal i explotable perquè es poden fer moltes coses amb aquestes dades i la gent no té consciència que no només hi ha robots i ordinadors rere aquestes recol·leccions, hi ha humans com jo que

tracten totes aquestes informacions, que escolten i teclegen...

Els humans darrere Cortana, per Antonio Casilli

Com ens recorda Antonio Cassilli a continuació, aquest relat subratlla exactament les pràctiques **«molt humanes»** que es troben a la massa sota els miralls enganyosos de l'anomenada **«intel·ligència artificial»**. *Antonio Casilli, membre de La Quadrature du Net, es investigador a l'EHESS i professor a Télécom ParisTech (mirar la seva pàgina web).*

La seva feina? Ensinistradora d'Intel·ligència Artificial (IA)

Malgrat el que en diuen els seus productors, els assistents virtuals dels aparells connectats que coronen els nostres menjadors o que nien en les nostres butxaques, instal·lats en els nostres telèfons intel·ligents, **no neixen intel·ligents**. Han d'aprendre a interpretar les cerques i els costums dels usuaris.

Aquest aprenentatge està guiat per humans, que verifiquen que les respostes que donen els assistents virtuals als seus propietaris siguin pertinents. Però encara més sovint, els humans «entrenen» els dispositius donant dades ja tractades, cerques amb les respostes ja fetes (ex. «Quin temps fa avui?» : « Avui estem a 23 graus» o « Està plovent») o frases per les quals donen una interpretació (ex. saber en quin context «cap» es refereix a «la part del cos» o a «una persona o objecte no existent»). Aquests ensinistradors d'intel·ligència artificial són a vegades teletreballadors pagats per hora per empreses especialitzades. En altres casos són feines a preu fet, pagades per unitat, que es contracten en serveis web que s'anomenen plataformes de micro-treball.

La de Microsoft es diu UHRS i proposen remuneracions de 3, 2, o fins i tot 1 cèntim de dollar per micro-tasca (transcriure una paraula, etiquetar una imatge, ...). A vegades les persones que trien les vostres cerques, miren les vostres fotos, escolten les vostres paraules estan al vostre país, fins i tot en la vostra ciutat (podria ser el veí de sota?). En d'altres casos són treballadors precaris de països en els que es parla la mateixa llengua. En el cas de França poden ser països com Tunísia, Marroc o Madagascar (que en els últims temps s'ha imposat com a «lider francès de la intel·ligència artificial».

Els programes d'activació vocal com Cortana, Siri o Alexa són agents conversacionals que posseïxen un gran component de feina no-artificial. Aquesta implicació humana introdueix riscos socials específics. La confidencialitat de les dades personals utilitzades per entrenar les solucions intel·ligents està en risc. Aquestes IA pressuposen enviar grans quantitats de dades de caràcter personal i existeixen en **una zona grisa tan legal com ètica**.

Mentre que els usuaris d'aquests serveis no estiguin al corrent de la presència d'humans entre els bastidors de la IA, estaran infravalorant el risc que pesa sobre la seva vida privada. De forma urgent s'han d'estudiar les violacions de la privacitat i la confidencialitat associades amb aquesta forma de treball digital, per tal de veure'n el seu abast i poder informar, sensibilitzar i protegir millor les persones més exposades.

Amazon

Per donar suport a aquesta iniciativa, hem traduït els textos disponibles sobre Google, Apple, Facebook i Microsoft, del francès al català. Per Amazon, ens van informar que no havien tingut temps de generar el contingut, i és per això que manca aquesta empresa a les traduccions al català.

Igualment, enllacem a dos documentals en francès. No tenim cap dret sobre les obres però les enllacem perquè són d'interès general.

Documental France 2

«Faut-il avoir peur d'Amazon?» https://video.tedomum.net/videos/watch/63a398f6-4ce1-475a-ab56-f2220189faec

Documental Arte

«L'irrésistible ascension d'Amazon» https://invidious.snopyta.org/watch?v=n8ZN1SWxDFo

Recursos

Cronologia d'elaboració pròpia a partir de les dades publicades a: https://www.gafam.info/ , https://gafam.laquadrature.net/ i https://www.laquadrature.net/donnees_perso/

Textos originals en francès: https://gafam.laquadrature.net/

Cartells en català: https://ptrace.gafam.info/unofficial/pdf/black/lqdn-gafam-poster-ca-black.pdf

Com imprimir els cartells: https://gafam.info/