CAP A UNA CASA SENSE SECRETS?

Quan la nevera o l'escalfador enviïn al núvol què mengem o quan ens dutxem es farà miques la intimitat domèstica. Arriba l'internet de les coses

TEXT__ **GINA TOST/ XAVIER VIDAL**

LES LLARS ESTAN A PUNT DE VIURE UNA REVOLUCIÓ que afectarà la manera de gestionar la nostra intimitat. La connexió a la xarxa de gairebé tot el que ens envolta a casa, fins i tot sense requerir la nostra intervenció, millorarà en molts aspectes la nostra vida. Però també implicarà necessàriament la monitorització dels nostres costums més íntims i de la manera com vivim quan pensem que ningú no ens veu: és un pas qualitatiu. A l'exposició voluntària de privacitat a través de les xarxes socials que fem ara s'hi unirà una radiografia, potser gestionada de manera anònima i impersonal, de la nostra intimitat domèstica. Marc Pous, fundador de l'empresa catalana Thethings.io, que es dedica a facilitar i organitzar la connexió de qualsevol dispositiu a la xarxa, explica que l'internet de les coses (IoT) "està per sobre de la idea del M2M (màquina-a-màquina), que és el procés pel qual dos dispositius parlen entre ells basant-se en protocols preestablerts". L'IoT, que el McKinsey Global Institute defineix com el conjunt de dispositius capaços de "controlar el seu entorn, informar del seu estat, rebre instruccions i prendre mesures basades en la informació que reben", està a punt per instal·lar-se a les nostres cases de manera silenciosa i efectiva.

Fa uns anys, la domòtica significava el futur de la tecnologia. Ara, en canvi, els especialistes comencen a desterrar el concepte perquè l'evolució ha portat els dispositius domèstics cap a una altra banda: l'internet de les coses (IoT). Un matís important marca la diferència. Mentre els aparells domòtics són intel·ligents i poden connectar-se a internet, els dispositius que formen l'IoT es basen en la connexió a internet de bon principi. Això significa que els electrodomèstics *parlin* constantment entre ells i, al mateix temps, cadascun d'ells parli amb un servidor on es guarden les nostres dades.

LA NEVERA I LA CAFETERA "ES PARLEN"

Luis Corrons, director tècnic de l'empresa de seguretat PandaLabs, diu: "Al núvol s'enviarà tota la informació, des de quan s'encenen els llums, quan s'obren les persianes, quan mirem el televisor i quins programes, i fins i tot quin menjar tenim a la nevera o el nostre ritme cardíac". És a dir, ja no és només que la nostra nevera es pugui connectar a la xarxa per demanar formatge quan detecti que s'ha acabat. És que la nostra nevera parlarà constantment amb el seu servidor a l'altra banda del món per explicar-li quins són els nostres costums i les nostres necessitats. I que, a més, també parlarà amb la vitro o amb la cafetera per intercanviar informació, sempre amb l'objectiu de fer-nos la vida més fàcil i agradable. Un exemple de com serà l'IoT és el programa Dash, anunciat per Amazon, que preveu la instal·lació de botons a casa, connectats via wifi. Aquests botons serviran per realitzar comandes automàtiques dels productes que consumim habitualment. Electrodomèstics com rentadores, rentaplats o neveres també podran fer ús d'aquesta tecnologia.

Un exemple del funcionament de l'IoT és l'empresa Efergy, que es dedica a supervisar el consum energètic que fem a la llar per recomanar-nos formes d'estalviar en la factura de l'electricitat. Mitjançant sensors, la companyia estudia què consumeix cada dispositiu i quin ús en fa cada membre de la família. Tota aquesta informació s'emmagatzema en un servidor central a Londres i és accessible a través d'aplis per a dispositius mòbils. Mikel Aguirre, director d'operacions a Europa d'Efergy, assegura que conèixer tota aquesta informació sobre les cases dels seus clients "permet als usuaris veure el consum de l'electricitat en temps real i ajudar-los a descobrir on i com estalviar". A casa nostra, l'empresa catalana Thermea està a punt de treure al mercat un sistema de regulació de la caldera domèstica que monitoritzarà el consum i permetrà regular la temperatura de manera remota. Així podrem fer-ne un manteniment predictiu. Jose Antonio Pérez, director del projecte, explica que es tracta "d'un servei centrat en el benestar i la tranquil·litat de l'usuari a tots els nivells: estalvi, producte i manteniment".

PRIVACITAT O INTIMITAT?

Independentment de l'objectiu, sembla clar que monitoritzar una part tan reservada de la nostra vida implica cedir una gran parcel·la d'intimitat que fins ara no estava registrada i classificada enlloc. El sociòleg David Dueñas ho té clar: "Oferim, de manera inconscient, la nostra privacitat a canvi d'alguna cosa que considerem que ens suposa un benefici, com ara cedir la intimitat de les persones grans vulnerables com a manera de garantir que no els passi res".

Actualment, es calcula que hi ha uns deu mil milions de *coses* o dispositius amb connexió a internet i en cinc anys es calcula que aquesta quantitat es multiplicarà per set. L'increment més significatiu es produirà, probablement, en els aparells domèstics.

Tot aquest immens flux d'informació que es generarà sense que ni tan sols en siguem conscients és el que constitueix la clau de volta d'una realitat tecnològica immersiva que ja pica a la porta de casa nostra. L'IoT planteja un debat interessant sobre la privacitat i la intimitat. Fins ara, la irrupció dels telèfons intel·ligents sempre connectats ha fet que el mateix usuari hagi exposat voluntàriament la seva privacitat. Pengem tota la nostra vida voluntàriament a les xarxes socials, des que sortim al carrer fins que fem l'última copa al local més de moda de la ciutat. Ho fem a canvi de beneficis més sociològics i psicològics que materials. Les retribucions que obtenim amb la publicació van des de millorar la comunicació amb els nostres amics a través d'aplicacions com el Foursquare o l'Instagram fins a millorar l'autoestima penjant la nostra felicitat al Facebook.

Marc Pous té clar que aquesta venda té aspectes molt positius. "En el cas del Gmail i Facebook, s'ha canviat la percepció de la privacitat a canvi d'uns serveis que no existien abans i que han revolucionat la manera com ens comuniquem", afirma. A l'era digital, tenim la sensació que no paguem molts dels serveis que marquen el nostre dia a dia, des de les xarxes socials fins al correu electrònic. Però només és cert en part. Fins ara el pagament no l'hem fet en diners sinó en privacitat. I la implementació de l'IoT a la llar pot comportar que la nova moneda sigui la intimitat domèstica.

GETTY

El gir copernicà que pot suposar l'IoT a casa nostra és que tot el que ens envolta ens observarà i ja no requerirà la nostra intervenció activa per enviar la informació. Ni tan sols serem conscients que els llums de la nostra habitació o el termòstat de la nostra calefacció estaran registrant i enviant al núvol què fem, com ho fem i quan ho fem. En certa manera, ja hem perdut la batalla de la privacitat del que fem fora de casa i ara podria passar el mateix amb la nostra intimitat a casa.

Marc Pous reflexiona: "Ens haurem d'acostumar a viure en una societat molt més transparent, però alhora podrem aprofitar-ho per no-drir-nos d'aquesta informació que generem". Caldrà aprendre a gestionar què volem i què no volem que sigui controlat establint una relació de risc-benefici. Potser serà bo saber què mengem perquè la nevera elabori una dieta sana. Però potser no caldrà que el bany enviï a una empresa de Califòrnia cada quant ens dutxem i a quina temperatura ens agrada l'aigua. Luis Corrons, director tècnic de PandaLabs, introdueix un punt de racionalitat quan afirma: "El fet de tenir una casa completament connectada no ha d'implicar que ella mateixa hagi de publicar a Facebook, Twitter o Instagram la nostra informació". "Dit això, l'experiència ens diu que, si els usuaris tenen l'oportunitat de fer-ho, en un gran percentatge ho faran", reflexiona.

Tenir els mecanismes de control de la informació, com es demostra en l'ús que fem dels telèfons intel·ligents, no implica saber ni voler usar-los. El sociòleg David Dueñas recorda "la idea suggeridora de la societat-risc de Beck, que fa un pas més amb aquesta lògica": "Assumim uns riscos que es deriven de la nostra voluntat d'augmentar la nostra qualitat de vida".

Saber quan anem a dormir, quan usem l'ordinador, quan ens dutxem o quanta estona llegim un llibre abans de dormir pot ser una informació valuosa. Mikel Aguirre, director d'operacions a Europa d'Efergy, no creu, però, que la irrupció de l'IoT comporti un risc gaire elevat per a la nostra intimitat individual. Segons Aguirre, la tecnologia dels gegants de la informació que analitzarà tot el doll de dades que sortirà de les nostres llars "ho farà de manera agregada, per conèixer tendències globals, perquè l'accés a la informació personal no té tant valor comercial".

En aquest context, la pregunta clau potser és qui serà l'encarregat de gestionar les dades sobre els nostres costums i com ho farà. David Dueñas n'és conscient: "De la mateixa manera que nosaltres obtenim més informació en temps real sobre el funcionament de les coses, aquesta informació també salta al núvol, on desapareix en els aiguamolls del *big data* i en perdem el control".

La tendència sembla que apunta a aparells que centralitzin tota la informació procedent dels diferents dispositius a casa nostra. És un mercat nou en el qual Google s'ha posicionat amb un termòstat intel·ligent anomenat Nest, que és molt més que un simple regulador de temperatura. El Nest podrà recollir variables d'altres dispositius i electrodomèstics, endreçar-les i enviar-les a un servidor central a través d'internet. El termòstat de Thermea té un funcionament semblant. Noves empreses catalanes, com ara Thethings.io, del Marc Pous, també ofereixen "un núvol que accepta dades en temps real a través de diversos protocols de comunicació dels diferents dispositius que es connecten a internet".

QUI MIRA PEL FORAT DEL PANY?

Al marge de qui recollirà, emmagatzemarà i analitzarà les dades, un punt cabdal és quin ús se'n farà i com s'evitarà que un botí de tant de valor caigui en mans inadequades. Luis Corrons afirma: "El risc més gran que existeix és que algú ens robi la identitat, aconsegueixi les nostres claus d'accés al sistema en el núvol i accedeixi a la informació fent-se passar per nosaltres". És bàsic, per tant, saber com es farà segur tot el *big data* que dibuixarà la nostra intimitat domèstica.

Corrons explica que és important "per a les dades més sensibles dels usuaris, com ara contrasenyes o dades personals, que les empreses les guardin en un format *hash* (un d'àlies alfanumèric) en comptes de la dada real". Així s'evita que, si les dades són robades, es puguin llegir i vincular a una persona concreta". En el cas de la catalana Thermea, la seguretat de les dades monitoritzades també és una prioritat. "S'emmagatzemen segons els estàndards de la Comunitat Europea, viatgen encriptades en tot moment i només s'utilitzaran per millorar el servei amb el consentiment de l'usuari", explica Jose Antonio Pérez, director del projecte.

Com s'ha demostrat, però, la seguretat total no és fàcil d'aconseguir quan actors tan poderosos com agències d'intel·ligència ens poden espiar pel forat del pany. Corrons assenyala: "Tenim governs amb àmbies voraces d'informació".

L'any passat, Hewlett-Packard va realitzar un estudi de seguretat entre una desena de dispositius connectats, com ara panys, televisions o alarmes. L'estudi va descobrir que vuit de cada deu no requerien contrasenya complexa i enviaven la informació a través d'internet sense codificar i també que la majoria permetien a un atacant reiniciar la contrasenya. Potser sí que les dades estan segures quan arriben al núvol però pel camí hi ha molts ulls que les poden llegir. Jose Antonio Pérez de Thermea explica: "Els riscos són equivalents als que ja tenim avui en dia a casa si perdem la clau o un lladre ens obre una finestra, però en format digital".

David Dueñas alerta: "La intimitat la posem en risc perquè no som capaços de determinar a qui l'estem oferint". És a dir, que no podem tenir la certesa de qui hi ha a l'altra banda analitzant el que fem. Probablement, per tant, l'ús comercial de les nostres dades domèstiques íntimes no seria el pitjor de tots els usos que se'ls podrien donar.

Com va passar amb els telèfons intel·ligents en relació a la privacitat, sembla evident que caldrà aprendre a gestionar la intimitat en l'era de l'internet de les coses. Marc Pous exposa: "Connectar dispositius domèstics a internet no implica que tothom els hagi d'usar com uns autòmats: hem d'entendre quin valor ens genera i usar-los en cas que ens siguin útils". David Dueñas comenta: "Si cedim involuntàriament les nostres dades al núvol, com a mínim, hauríem de ser conscients que ho estem fent".■