Intel·ligència artificial i tecnoètica

Cecilio Angulo
Carissa Véliz

UPCArtsDiàlegs

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Intel·ligència artificial i tecnoètica

UPCArtsDiàlegs 1

Intel·ligència artificial i tecnoètica

Cecilio Angulo
Carissa Véliz

Edició a càrrec d'Antoni Hernández-Fernández

UPC ARTS

UPC UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Traducció: Marta Lorente

Primera edició: abril de 2022

Oficina de Publicacions Acadèmiques Digitals de la UPC
Jordi Girona, 31 edifici K2M 08034 Barcelona
Tel.:934 015 885
www.upc.edu/idp
E-mail: info.idp@upc.edu

Producció: QPPrint
c/Miquel Torelló i Pagès, 4-6
08750 Molins de Rei. Barcelona
www.qpprint.es

ISBN: 978-84-19184-05-4
DL: B 8592-2022

Sumari

Pròleg

Antoni Hernández-Fernández

Amb aquesta obra comença la que desitjo que sigui una prolífica col·lecció a la Universitat Politècnica de Catalunya (UPC): *Diàlegs UPCArts*. El seu recorregut es deu sens dubte a l'ímpetu de Carme Fenoll i a la col·laboració necessària que ha trobat tant en Iniciativa Digital Politècnica, dirigida per Jordi Prats, com en uns quants humanistes còmplices que poblem aquesta universitat. L'objectiu de la col·lecció *Diàlegs UPCArts* és crear un canal de reflexió obert a la comunitat UPC i als lectors en general sobre la relació que hi ha entre les humanitats, la tecnologia, la ciència, les arts i la societat. Quants estudiants, professors o personal de la universitat hi ha que compaginin la vida universitària amb la música, la pintura, el teatre, el cinema, la literatura, el disseny, la dansa, l'arquitectura... independentment dels estudis més o

menys tècnics? Afortunadament, som més dels que ens pensàvem.

Carles Sora, director del CITM-UPC, en una de les moltes reunions virtuals prèvies que va gestar la nova col·lecció de *Diàlegs UPCArts*, va apuntar que aquesta col·lecció havia de ser una *correspondència*. Aprofundim en la metàfora (espero que en Carles em perdoni la dissonància). Per començar, *Diàlegs UPCArts* és una correspondència epistolar entre veus que se senten a través dels ecos de les seves paraules en el paper; és un intercanvi d'arguments, de reflexions i de sentiments que es contraposaran —o no—als del mateix lector; és, paradoxalment, un monòleg interior que és un diàleg, una correspondència biunívoca entre la raó i la passió; és una sinonímia entre humanisme i tecnologia, en una falsa dicotomia, tal com veurem al llarg de les pàgines, ja que la tècnica s'integra en la humanitat des dels nostres orígens ancestrals; i, en darrer lloc, és un intercanvi de cops artístics mediats tecnològicament, per mitjà d'un llenguatge registrat, plasmat en un suport físic, tal com passa des que la història mereix aquest mateix nom, quan la tecnologia va imbricar per fi totes les manifestacions culturals humanes.

La llavor d'aquesta primera correspondència va ser el diàleg que van establir la filòsofa Carissa Véliz i el professor de la UPC Cecilio Angulo, en el cicle de xerrades sobre *Tecnologies emergents i desigualtats* que va tenir lloc la primavera del 2021 al Palau

Macaya de Barcelona[1]. Com a membre del Comitè d'Ètica d'aquesta universitat, de què també forma part en Cecilio, per a mi és un plaer inaugurar *Diàlegs UPCArts* amb una obra que convida a la reflexió tecnoètica.

Es tracta d'un diàleg peculiar sobre un tema candent: la intel·ligència artificial i algunes de les implicacions socials que té. M'il·lusiona especialment editar en català Carissa Véliz per primera vegada. Vaig partir de la traducció d'una selecció dels seus articles a *El País*, mitjà a què agraïm el permís concedit per a aquesta edició. Hem alternat els textos de la Carissa, esmolats i estimulants per al debat, amb les rèpliques asíncrones i els apunts imprescindibles d'en Cecilio, a qui vam encomanar la difícil tasca de ser divulgatiu en un tema complex com és la intel·ligència artificial, a fi d'arribar a un públic ampli, no expert.

Per atzars de la història, entre el primer article de la Carissa —sobre intel·ligència artificial, del juny del 2019— i l'últim —sobre digitalització i vigilància, del desembre del 2021—, ens hem enfrontat a una pandèmia que encara cueja. Entremig, ha nascut i ha començat a madurar el Comitè d'Ètica de la UPC, en què s'han creat molts materials relacionats directament amb l'ètica, en els diversos àmbits universita-

1 Disponible en línia a: https://www.youtube.com/watch?v=Z-c6rEchv4Go&t=8s

ris[2]. Cal agrair a tots els membres del Comitè aquest periple inicial tan fructífer d'aprenentatge i creació, de discussió terminològica i pràctica, i de compartir materials clau per a la reflexió ètica. També durant aquest espai de temps, Carissa Véliz va escriure i publicar *Privacy Is Power* (Penguin 2020), traduïda al castellà per Debate el 2021, obra a què recomano de recórrer per ampliar bona part dels arguments que se sintetitzen als seus articles.

En definitiva, tant de bo gaudeixin d'aquesta correspondència entre la Carissa i en Cecilio. Espero que els susciti algun diàleg posterior, un autèntic *Diàleg UPCArts*, dels que són importants: potser de sobretaula amb els seus éssers estimats, amb porfídia interior amb vostès mateixos, de debat amb els seus estudiants després de proposar alguna lectura a classe, o fins i tot amb desconeguts a les xarxes quan, immersos en un rubor digital, se sembri el dubte: i si fos un *bot* o un algorisme el que dialoga amb nosaltres?

2 Es poden consultar tots a la pàgina: https://comite-etica.upc.edu/ca

Hi pot haver una ètica de la intel·ligència artificial?

La tecnoètica hauria de ser la solució humanista que defineixi una ètica funcional en aquest domini tecnològic

Cecilio Angulo

La intel·ligència artificial és un element trencador de progrés a la nostra societat que no admet cap mena de contesta. No és comparable, però, amb la intel·ligència humana, ni de bon tros, per més que n'insisteixin els titulars sensacionalistes. La intel·ligència artificial i els elements de digitalització on està incrustada tenen un abast enorme de disrupció social perquè permeten la projecció de la societat en un domini paral·lel, el de la ciutadania digital universal. És el mite platònic de la caverna en tot el seu esplendor mediàtic i social.

La intel·ligència artificial, entesa com un mirall o símil de la intel·ligència humana, permet que la societat pugui veure's reproduïda, i de vegades reconeguda, en els entorns digitalitzats creats per artefactes tecnològics, i hi pugui també explorar els seus

límits. Per tant, s'usa i s'abusa del concepte metafòric d'*intel·ligència (artificial)* quan en realitat el debat no s'hauria de centrar en l'element de projecció, sinó que caldria dirigir-lo cap al constructe digitalitzat que crea la tecnologia al seu voltant. Així doncs, la intel·ligència artificial permet fixar la mirada cap a espais digitalitzats on les regles de convivència no tenen per què ser també una projecció d'aquelles pròpies del món analògic, sinó que s'inventen i es construeixen. Hi ha qui afirmarà que aquesta gestió de la convivència és autoorganitzativa, tal com es va dissenyar l'arquitectura d'internet. Tanmateix, la realitat digital no pot estar més allunyada d'aquesta col·laboració entre iguals, amb uns propietaris i uns interessos ben definits, capaços de decidir governs i sotmetre Estats.

I és en aquest nou *Far West* tecnològic en què l'humanisme, ara tecnològic, s'ha de projectar, com a mirall de la societat analògica, en especial a través de la seva dimensió ètica. Ara bé, l'ètica analògica és extensible al domini digital? I en tot cas, projectada a la llum de la intel·ligència artificial, encara seria útil? Cal una nova ètica per a aquest nou espai social? Quina aproximació ètica suportaria millor aquesta projecció de valors entre dominis?

Allò veritablement desconcertant per a la societat, fet que succeeix més cops del que voldríem, és que el que es reflecteix en el domini digital no ens agrada. En conseqüència, es conclou que l'eina de projecció que significa la intel·ligència artificial deforma una

realitat que, sens dubte, no pot ser aquell esperpent que s'aprecia al mirall: es culpa «els algorismes» de les desviacions de la realitat digital esperada. No, no pot ser que aquesta realitat artificial es creï a partir de la intel·ligència humana, ens repetim. No podem ser nosaltres. Sens dubte, els algorismes no estan ben dissenyats, la realitat no és així, ens atrevim a interioritzar.

La tecnoètica hauria de ser la solució humanista que defineixi una ètica funcional en aquest domini tecnològic, ja sigui com una ètica pròpia de la intel·ligència artificial o com una projecció i adaptació de les ètiques «analògiques». És més, tal com estableix la definició d'Stuart Russell d'*intel·ligència artificial*, aquesta hauria se ser una tecnologia que vetlli per construir màquines que facin el que es correcte, que actuïn de manera que és esperable que aconseguiran els seus objectius. I és en allò «correcte» on llavors la intel·ligència artificial pot projectar els valors ètics, en forma de tecnoètica, sobre el constructe digital. Deu voler dir això que es tracta doncs d'una ètica diferent, de quelcom diferenciat? Caldrà analitzar el fet tecnològic des de la perspectiva de les ciències socials i la filosofia per entendre la imbricació que té amb el món analògic i poder continuar avançant.

Intel·ligència artificial: progrés o reculada?

No avançarem si el futur digital perpetua els errors del passat. Si per cada euro que s'inverteix en nous algorismes se n'invertís un altre en regulació, hi hauria més raons per ser optimistes sobre el futur

Carissa Véliz
El País, 14 de juny de 2019

Un dels riscos més grans de la intel·ligència artificial és que perpetuï els errors i prejudicis del passat, camuflant-los sota un vernís d'objectivitat. Els sistemes d'intel·ligència artificial s'entrenen a partir de dades que reflecteixen les decisions que hem pres en el passat. Quan la intel·ligència artificial de reclutament d'Amazon va discriminar les dones, no va ser perquè els homes fossin millors candidats per als treballs disponibles. Per mitjà d'una base de dades que contenia un historial de contractació, Amazon va ensenyar al sistema que l'empresa havia preferit contractar homes durant els darrers 10 anys. En altres paraules, l'algorisme va perpetuar un prejudici sexista que estava enregistrat a les dades del passat.

PredPol, el sistema d'intel·ligència artificial emprat per la policia als Estats Units, té problemes semblants. En comptes de predir crims, que és el que se suposa que hauria de fer, reprodueix hàbits policíacs. Allà on patrulla la policia, hi troben crims que fan processar a l'algorisme, que alhora recomana que es continuï patrullant les mateixes zones. A les àrees on hi ha més presència policial, hi ha en conseqüència més arrestos: són zones poblades per minories. El resultat és que aquestes minories estan sent indirectament discriminades.

Una de les grans fal·làcies associades a l'optimisme sobre el *big data* és creure que com més dades tinguem, millor. Caldria revisar les paraules del poeta T.S. Eliot, que va escriure: «On és la saviesa que hem perdut amb el coneixement? On és el coneixement que hem perdut amb la informació?» Recollir més dades no garanteix que siguin precises, ni que estiguin actualitzades i siguin rellevants per acomplir els nostres objectius, ni molt menys que siguem capaços de posar aquestes dades al servei de la justícia, la democràcia, la igualtat i el benestar.

Es diu que el *big data* revolucionarà la ciència. De moment, la intel·ligència artificial manifesta més estupidesa que intel·ligència. Entre moltes altres limitacions, la intel·ligència artificial només és capaç de rastrejar correlacions, cosa que no necessàriament ens porta a entendre millor les relacions de causa i efecte que governen la realitat. El fet que els algorismes detectin correlacions és un altre element que

els fa resistents a reconèixer o impulsar canvis. Dos elements que han estat correlacionats en el passat (per exemple, ser dona i tenir una feina mal pagada) no tenen per què estar correlacionats en el futur, però si els nostres algorismes ens porten a actuar com si les correlacions fossin una veritat objectiva i immutable, llavors és més probable que la intel·ligència artificial no generi prediccions neutrals, sinó profecies autocomplertes.

També es creu que el *big data* té el potencial d'eliminar els biaixos en les decisions humanes; de moment, com hem vist, sembla que està incrementant els biaixos i solidificant l'*statu quo*.

Un factor que possibilita els canvis socials és la capacitat humana d'oblidar allò que ens lliga al passat. Al seu magnífic llibre *Delete,* Viktor Mayer-Schönberger argumenta que tenir una memòria perfecta, ja sigui com a individu o com a societat, pot ser un obstacle per canviar a millor. La nostra memòria biològica és un sistema fantàstic de filtració i organització de la informació: recordem allò important, oblidem allò insignificant, reconstruïm el passat constantment a la llum del present, i donem diferents valors a diferents memòries. La memòria digital ho recorda tot sense reinterpretar-ho ni valorar-ho; és l'antítesi de la nostra memòria biològica, forjada per mil·lennis d'evolució. Les conseqüències de no poder oblidar poden ser desastroses.

Si no som capaços d'oblidar els errors que algú ha comès (i tots cometem errors), o si més no de

tenir-los menys presents, és difícil que li puguem donar una segona oportunitat. És veritat que cal no oblidar les lliçons del passat, però aprendre de la història no és el mateix que mantenir un registre de cada infracció que cada persona comet. Això últim ens porta a tenir una societat implacable, rígida, que eternitza les injustícies del passat. Per això el dret a l'oblit és tan important i un encert del Reglament General de Protecció de Dades (RGPD).

Un altre factor necessari per possibilitar canvis és la capacitat humana de tenir consciència social. Els éssers humans som éssers sentents i agents morals. Com a éssers sentents, sabem què és el patiment i el benestar en la nostra pell, i som capaços de mostrar empatia amb altres que pateixen. Com a agents morals, entenem les conseqüències que les nostres accions poden tenir en altres. Comprenem que de vegades cal fer una excepció a la regla —quan la regla no inclou tots els casos possibles, o quan una persona mereix una segona oportunitat—. Som capaços de reflexionar sobre els nostres valors i actuar en conseqüència.

Els algorismes no són ni éssers sentents ni agents morals. Són incapaços de sentir dolor, plaer, remordiment o empatia. Són incapaços d'entendre les conseqüències de les seves accions: només els éssers que poden experimentar dolor i plaer poden entendre què vol dir infligir dolor o causar plaer. Els algorismes no tenen valors ni són capaços de fer una excepció a la regla. No tenen en compte que moltes

vegades les transgressions humanes són producte de la injustícia (la manca d'oportunitats que duu al crim, per exemple). No poden reflexionar sobre el tipus de vida que volen portar, o el tipus de societat on volen viure, i actuar en conseqüència. Un cotxe autònom no pot decidir fer menys quilòmetres per no contaminar. Un robot de guerra no es pot convertir en pacifista després de reflexionar sobre les conseqüències dels conflictes armats. Els algorismes no poden tenir consciència social.

És un parany creure que la tecnologia pot resoldre per si mateixa problemes que són fonamentalment ètics i polítics. El repte més important que tenim al davant és de governança. Si per cada euro que s'inverteix en intel·ligència artificial s'invertís un altre euro en regulació i governança, tindríem més raons per ser optimistes sobre el futur digital. Ara mateix, els incentius premien l'ús de la intel·ligència artificial per prendre decisions. Si les institucions fan servir algoritmes per prendre decisions, s'estalvien diners a l'hora de pagar menys sous, poden defensar les seves decisions com si fossin objectives, i si alguna cosa surt malament, poden culpar l'algorisme. Quan els que més arrisquen (els ciutadans a mercè dels algorismes) són diferents que els que més es beneficien d'aquest risc (les empreses, els governs), es creen asimetries de poder. El paper dels reguladors és assegurar-se que els incentius de les institucions estiguin alineats amb els interessos de la població. Si la intel·ligència artificial fa malbé els ciutadans, hi ha

d'haver conseqüències proporcionals per a les persones responsables d'aquest algorisme.

Tot i la seva complexitat, els algorismes no són més que eines, i els agents morals som totalment responsables de les eines que creem i utilitzem. Si deixem que els algorismes decideixin basant-se en dades del passat, serem responsables de repetir els nostres errors, de frenar el progrés social fins al punt que comencem a retrocedir.

Hem de parlar d'algorismes, machine learning, deep learning o d'IA?

De la Intel·ligència Artificial a la Intel·ligència Augmentada

Cecilio Angulo

La humanitat, com a concepte global abstracte, ha progressat, durant els últims quatre segles, a partir d'una carrera constant de desafiaments científics i tecnològics, en què el progrés en ciència i tecnologia no pot entendre's l'un sense l'altre: del desafiament de volar de Leonardo a la carrera espacial i l'home a la Lluna; de l'exploració de continents sencers, cims i avencs, als satèl·lits fora del sistema solar; de les primeres fites en higiene i salut pública als nanorobots intravenosos, hi ha hagut un salt. El nou instrument *Misions* del programa europeu *Horizon Europe* dissenyat per Mariana Mazzucato n'és un altre exemple. Vegem-ho.

La creació d'una intel·ligència mitjançant un sistema artificial és un altre d'aquests desafiaments

que serveixen d'excusa o esperó per a l'avenç científic-tècnic. Allò que s'entén per *intel·ligència artificial* és al mateix ADN del repte. En l'origen, en els temps que avui es coneixen com GOFAI (*gold old fashioned AI*), la intel·ligència es va començar entenent com la capacitat de deduir coneixement nou fent servir la lògica. Així, sistemes basats en regles, els denominats *sistemes experts*, havien de permetre, a partir d'uns coneixements inicials o antecedents i una base de regles conegudes, inferir coneixements nous i regles noves des d'una aproximació deductiva. Era l'època en què una màquina capaç de decidir jugades d'escacs i guanyar es considerava intel·ligent. Era l'època de Turing i de les primeres màquines de calcular. La intel·ligència s'aconseguia mitjançant força bruta: moltes regles, molta màquina, molt de temps.

Mentre aquesta primera aproximació *màquina* a la intel·ligència es basava en un llenguatge simbòlic per a la producció de regles i coneixement, a imatge i semblança de les matemàtiques i les ciències experimentals en general, en paral·lel es desenvolupava una aproximació alternativa a la definició d'*intel·ligència*, basada en el repte de crear un cervell electrònic. Igual que el cervell processa la informació a través d'una gran quantitat de neurones i les seves connexions sinàptiques, un ordinador es compon d'un gran nombre de transistors o portes lògiques que estan interconnectades. Així doncs, si som capaços de descobrir com processen les neurones la informació al cervell en forma d'impulsos elèctrics, hipotèticament

es podria extrapolar aquest coneixement als ordinadors i crear un cervell electrònic, que seria la base d'una intel·ligència artificial. Va ser el naixement de les anomenades *xarxes neuronals artificials*, els *sistemes connexionistes* i de l'*aprenentatge màquina* (en anglès, *machine learning*, ML).

A diferència de l'aproximació simbòlica, en aquest cas la regla d'inferència del coneixement no és deductiva, sinó inductiva, és a dir, funciona a partir de dades recollides en observacions. El Sol no sortirà demà al matí perquè hi ha un moviment de translació i rotació de la Terra al voltant del Sol, sinó que sortirà perquè fa set mesos que recullo dades i cada matí es fa de dia i torna a sortir. Per què no hauria de sortir demà altra vegada? La màquina és capaç de descobrir patrons de comportament en les dades, però són les persones qui poden o han d'aplicar la inferència deductiva per crear coneixement. És el que actualment s'anomena *Intel·ligència Augmentada*, amb sistemes d'aprenentatge automàtic que ajuden en la presa de decisions o la creació d'hipòtesis que després un ésser humà ha de validar. Aquest és el punt que no hem d'oblidar: l'ésser humà és l'últim responsable de la decisió.

Deixant de banda les màquines autònomes, que hem decidit anomenar *robots*, com és el cas dels vehicles autònoms, l'evolució computacional actual dels sistemes intel·ligents és el denominat *aprenentatge profund* (o *deep learning*, DL). Sent injust i tendenciós, cosa no tan infreqüent en la comunitat científica,

l'aprenentatge profund és com l'aprenentatge automàtic, però amb més dades, estructures algorísmiques més grans i més processadors a la màquina. Certament, l'aprenentatge profund no aporta res espectacularment nou respecte de la teoria matemàtica i a la metàfora del cervell electrònic, no obstant això, sí que ha trobat un espai d'investigació que ha permès un salt qualitatiu a la resta de dominis.

M'explico. L'inconvenient principal del ML ha estat sempre la denominada *maledicció de la dimensionalitat*. Per treballar amb milions de dades, no només milers, l'estructura algorísmica ha de ser tan complexa que el temps de càlcul es fa inassumible per a qualsevol superodinador. Les estructures convolucionals del DL, en canvi, van permetre aquest salt qualitatiu que feia anys que s'esperava. A més, amb un nivell d'encert en l'aprenentatge sobre aquestes bases de dades enormes molt més gran que els algorismes previs. Com a conseqüència, el DL permet concloure que (1) el coneixement és a les dades més que en l'ajustament dels algorismes, i (2) els algorismes s'han d'adaptar perquè la màquina els pugui processar ràpidament, encara que això impliqui sacrificar comprensió matemàtica i científica de la solució. La primera de les conclusions és música celestial per a les empreses que tenen les dades. Són les propietàries del nou or i s'estan encarregant la mar de bé d'explotar-lo. El segon punt té a veure amb la carrera actual en el disseny i producció de xips nous. A més d'adaptar els algorismes a la màquina, també es

pot treballar per adaptar els processadors a aquests algorismes. La carrera incessant per augmentar la densitat de transistors per centímetre quadrat passa a un segon pla i ara la inversió més gran se centra en el disseny apropiat de noves GPU, TPU NPU.

Davant l'inconvenient que suposa convertir els sistemes de DL en caixes negres, allunyats de la comprensió humana, hi ha un esforç investigador enorme en la creació de sistemes d'explicabilitat que permetin entendre d'alguna manera el funcionament de l'algorisme.

En darrer lloc, i penso que aquest és un puntal del triomf actual i futur del DL com a aproximació a la IA, aquesta mena de sistemes han permès la creació d'estructures d'aprenentatge que van més enllà de les funcions tradicionals de mapatge entre espais o els sistemes estocàstics. Estructures dinàmiques recurrents, d'aprenentatge per reforç, de creació d'informació sintètica, d'autocodificació, generatives adversàries, de transferència d'aprenentatge entre dominis s'han desenvolupat gràcies a aquesta nova manera d'afrontar els problemes i, altre vegada, signifiquen un salt qualitatiu de diversos ordres de magnitud de què la ciència i la tecnologia surten beneficiades.

Els primers sistemes d'intel·ligència artificial, i alguns dels que a dia d'avui es continuen desenvolupant, pretenien l'automatització completa del procés de creació d'intel·ligència d'una manera inductiva/deductiva. Les noves aproximacions ML/DL, però,

mantenen l'aspecte humà, juntament amb el procés automatitzat d'inferència inductiva a partir de les dades. Actuar amb ML/DL com si fos un procés completament automatitzat, aliè a la intervenció humana, significa una delegació equivocada de les nostres funcions.

La privadesa als anys vint

El mal ús de les dades personals gràcies a les noves tecnologies ens posa en risc a tothom

Carissa Véliz
El País, 6 de gener de 2020

Per alguna raó una mica misteriosa, els números rodons solen inspirar els éssers humans a fer un pas enrere i prendre perspectiva sobre els grans temes del nostre temps i les nostres vides. Començar el 2020 és una oportunitat per repensar les lliçons de la dècada passada i replantejar-nos la dècada entrant.

Les primeres dues dècades del segle xxi es van caracteritzar per una pèrdua progressiva de la privadesa. Dos fenòmens van confluir per donar cabuda al monstre de l'economia de les dades: el desenvolupament dels anuncis personalitzats i la preocupació per la seguretat.

L'any 2000, i sota la pressió de trobar un model de negoci sostenible, Google va llançar AdWords (ara Google Ads), una iniciativa que va aprendre a

explotar les dades dels usuaris per vendre anuncis personalitzats. En menys de quatre anys, la companyia va aconseguir un augment d'ingressos del 3590%. Un any després, la Comissió Federal de Comerç dels Estats Units va escriure un *report* per al Congrés recomanant la regulació de les dades abans que es convertissin en un problema. Però l'atac terrorista a les Torres Bessones va sembrar la por, que va donar prioritat a la seguretat nacional. Els governs van veure una oportunitat de vigilància en totes les dades que estaven sent recol·lectades per les empreses tecnològiques. La privadesa va passar a un segon pla, i el capitalisme de la vigilància va néixer de la col·laboració entre institucions públiques i privades.

Ja el 2010, la privadesa havia estat fortament erosionada, malgrat que la majoria de nosaltres encara no ens adonàvem de les conseqüències d'aquesta pèrdua. Va ser aquell any quan Mark Zuckerberg es va atrevir a suggerir que havíem evolucionat més enllà de la privadesa (aquest any, en canvi, va assegurar que «el futur és privat»).

Les grans tecnològiques van ser capaces de corroir les normes de privadesa forjades a través de segles per protegir-nos de possibles abusos. Si a la feina el teu cap no sap que estàs pensant a tenir un fill, no pot discriminar-te per aquesta raó. Si el teu govern no és capaç de preveure qui formarà part d'una protesta, no la pot impedir. Si el teu veí no sap quina religió professes, no et jutjarà per això.

Al món *offline,* hi ha certs senyals, normalment força palpables, que ens ajuden a complir les normes de privadesa i ens alerten quan aquestes han estat trencades. Hi ha poques sensacions tan socialment incòmodes com quan algú et mira fixament quan no vols ser vist. Quan algú roba el teu diari deixa una absència perceptible. L'era digital va destrossar les normes de privadesa en gran part perquè va ser capaç de separar-les d'aquests senyals tangibles. El robatori de les dades digitals no crea cap sensació, no deixa petjada, no queda una absència a percebre. La pèrdua de la privadesa en línia només fa mal una vegada que ens toca carregar amb les conseqüències: quan ens neguen un préstec o una feina, quan ens humilien o assetgen, quan ens extorsionen, quan desapareixen diners del nostre compte, quan manipulen les nostres democràcies.

Estem reaprenent el valor de la privadesa a cop de males experiències. Una de les lliçons d'aquesta dècada és que cada cop hi ha més exemples per il·lustrar que la privadesa, lluny de ser una enemiga, és una part integral de la seguretat tant individual com nacional. La cobdícia per les dades incentiva que l'arquitectura d'internet sigui insegura. Com menys mesures de seguretat tinguin els nostres aparells electrònics, més fàcil és robar les nostres dades. L'any 2000 la ciberseguretat no era un problema que destaqués. És relativament comprensible que els governs hagin pensat que la pèrdua de la privadesa era necessària per garantir la nostra seguretat. Els fets

han demostrat que aquesta suposició és incorrecta. L'any 2020, la ciberseguretat és una de les grans preocupacions de tot govern. El ciberespai és la nova sorra on es lliuraran bona part dels combats geopolítics del segle xxi. I al món digital, la seguretat passa per protegir la privadesa.

Europa pot estar orgullosa d'haver estat la primera institució política que ha començat a regular la privadesa digital amb el Reglament General de Protecció de Dades. La tasca pendent més urgent és atorgar a les autoritats els recursos necessaris per fer complir la llei. No podem ser complaents. El mal ús de les dades personals ens posa en risc a tothom.

El repte als anys vint serà recuperar la privadesa perduda i enfortir la ciberseguretat per protegir les nostres democràcies. És una batalla que cal guanyar si volem preservar les nostres societats liberals. La mala notícia és que és una guerra que mai no es guanyarà del tot. Sempre haurem de continuar lluitant per la democràcia, la justícia i la igualtat. La bona notícia és que és una lluita que es pot guanyar i val la pena. Si al principi del segle xxi la preocupació per la privadesa es va poder percebre (equivocadament) com una cosa del passat, el 2020 és clar que la privadesa és un dels grans desafiaments d'aquesta nova dècada.

Tecnoètica en temps de pandèmia

Cecilio Angulo

La pandèmia provocada per la COVID-19 mata. És un fet incontestable que no admet matisos. La prioritat és contenir-la i erradicar-la aviat. Aquest moment excepcional ha requerit, i encara requereix, mesures excepcionals que han tingut caràcter d'urgència... Ep, ep, espera, quan és que he sentit abans aquest últim discurs? Vora el 2018, amb la crisi financera? I sense anar tan lluny, a finals del 2021, sobre la «situació excepcional» del preu de la llum a Espanya? Jo sí que veig excepcional la factura de la meva companyia elèctrica cada mes.

D'acord, acceptem que en el cas de la pandèmia la correlació entre les mesures preses i la situació sanitària comporta una causalitat. Descartem el negacionisme. I acceptem també que la mesura excep-

cional es pren perquè hi ha una causa excepcional i no a l'inrevés, que la causa es creï per justificar la mesura. Escombrem de cop tota mena d'indici de teoria de la conspiració. En el cas de la pandèmia, semblaria plausible. Sent aquest el cas, en nom del bé comú, quines mesures excepcionals estem disposats a acceptar? Quins drets estem disposats a sacrificar o limitar?

Pensem en tres d'aquestes mesures. La limitació del dret a la lliure circulació no és una qüestió menor. Tampoc no ho és la vacunació massiva, un protocol de salut invasiu i irreversible. I posem com a tercer exemple una cosa aparentment més innocent, com és ara l'ús d'aplicacions de rastreig per delimitar i acotar els contagis. Sense entrar en la valoració de l'efectivitat d'aquestes mesures, totes tres serveixen com a exemple de la diferent temporalitat que comporta l'excepcionalitat. És a dir, un cop passat el moment crític, és d'esperar una presa de decisions que ens reverteixi a la situació anterior a la renúncia de drets i minimitzi l'impacte que han generat. En el cas de la lliure circulació de persones, o el tancament temporal dels negocis, és fàcil determinar si aquestes mesures es retreuran. La segona de les mesures, la vacunació, és obvi que és una mesura definitiva, sense possibilitat de tornada enrere, però veurem si es manté en el temps o bé decau.

La tercera de les mesures, aquella més tecnològica, les aplicacions de rastreig, és la que mereix en aquest cas el focus tecnoètic. Atès que no es tracta

d'una mesura tan òbvia per a la ciutadania, com seria veure carrers sense cotxes, negocis tancats o cues en centres de vacunació, l'observació del seu ús no és del tot opaca però es fa difícil de preveure, quan no impossible, determinar quina finalitat, i durant quant de temps, se li dona a aquestes eines. Resseguim el camí de la dada en una d'aquestes aplicacions. Deu ser ètic fer-la servir? Esclar, es dissenyen per frenar l'avanç de la pandèmia!, es podria afirmar.

Les dades s'haurien de començar a crear quan un ciutadà informa que ha donat positiu en un test de COVID. Quina qualitat té aquesta dada? Hi ha algú que ho validi? Amb quina fiabilitat? Depèn de com sigui l'aplicació de rastreig, o bé el subjecte infectat facilitat una llista de tot el seguit de persones amb qui «ha tingut contacte estret», o bé la mateixa aplicació ha recollit un gran nombre de ciutadans amb qui ha interaccionat aquesta persona a una distància de *bluetooth*. En el primer cas, la persona, de bona o mala fe, relata tota una llista de «sospitosos» sobre els quals s'ha de fer un rastreig. De qui informo? De la meva filla, que no té la pauta de vacunació completa i que ara està amb exàmens? Del cunyat, mira que m'arriba a caure malament!, i així es queda tancat a casa una setmana?

En el segon cas, tant si és un positiu cert com no, la persona porta al mòbil una aplicació que està creant de manera ininterrompuda una xarxa de contactes i de localització de persones que permeten una «actuació preventiva», de futur. Us sona? Això

sí, se'ns dona la total seguretat —creieu-me, que és veritat de la bona!— que només es farà servir aquesta xarxa de contactes si hom dona positiu, i només per a un ús de rastreig per temes de salut pública. Però, ja que les he creades jo, em permeten l'accés a aquestes dades? Em garanteixen que les dades de fa cinc mesos ja s'han esborrat? I si no és així, quin ús en volen donar? L'accés a les dades recollides està controlat? No podria ser que alguna empresa privada ja les tingui a la seva disposició?

Ens podem refugiar en la idea que la decisió de fer servir l'aplicació o no és personal. Però, desafortunadament, això és com Facebook: ningú és lliure que l'etiquetin com a «contacte estret», sense avisar-lo prèviament, amb traïdoria i nocturnitat. La teranyina t'acorrala un altre cop, encara que no vulguis entrar en el joc. Per molt que desitgis escapar del domini tecnològic, t'hi trobes atrapat, com un avi davant d'una sucursal bancària. Quina manera tecnoètica de cuidar la nostra gent gran!

Sí, sí, ja ho sé, l'Estat «et vol cuidar» i «tot ho fa pel teu bé». Però si aquell oleoducte als Estats Units el van piratejar, si el gasoducte que ve d'Ucraïna l'han pogut controlar a distància els russos, si l'agenda i converses per telèfon d'Angela Merkel s'ha convertit en contingut de domini públic, a un pobre mortal, quin nivell de seguretat li asseguraran?

I encara ha d'arribar la segona part de la història. Un cop instaurada la política del Gran Germà, de la col·laboració necessària, sempre «per un bé comú»,

qui desfarà el camí que ja s'ha fet? Qui m'assegura la desconnexió del joc? Un cop cedeixes el dret a la teva privacitat, o l'entorn, ben o mal intencionat, ho fa en nom teu, s'esgota la teva capacitat de decisió personal. Però aquest segon episodi ja serà part d'un altra història.

La privadesa en temps de coronavirus

Les mesures més eficaces contra la pandèmia no passen per apps que afecten els nostres drets

Carissa Véliz
El País, 24 de març de 2020

En una pandèmia la prioritat és contenir la infecció. La pandèmia de 1918 va matar entre 50 i 100 milions de persones. Per posar-ho en perspectiva, a la Segona Guerra Mundial van morir entre 70 i 85 milions de persones. Hi ha molt en joc amb el coronavirus. En aquestes circumstàncies cal posar en pausa alguns drets, com ara el d'associació. És la privadesa un d'aquests drets? No és clar...

Les *telecos* a Espanya estan oferint al govern controlar els moviments de les persones que estan confinades. Algunes comunitats ja han tret pàgines o apps relacionades amb el virus. L'experta en privadesa Gemma Galdón ha ofert algunes crítiques a Twitter. *Coronamadrid*, per exemple, apunta Galdón, no permet ús anònim, no demana consentiment,

no estableix període de retenció de dades, no minimitza dades, i comparteix dades mèdiques sense anonimització.

A la Xina, el govern va prendre mesures tecnològiques extremament intrusives. A Corea del Sud, a més de fer més proves de coronavirus que a cap altre país, han publicat detalls molt específics sobre individus infectats. Israel es planteja fer servir el servei secret per vigilar els ciutadans a través dels seus mòbils. Als Estats Units, el govern discuteix amb les grans tecnològiques desenvolupar mesures que podrien ser semblants.

És necessari lliurar la nostra privadesa a una app per frenar el coronavirus? No és evident. Les mesures més efectives no semblen passar per cap app.

A Wuhan la mesura més efectiva va ser la quarantena generalitzada. Però la quarantena generalitzada és una opció econòmicament cara, i l'economia importa perquè una crisi també causa estralls i morts. Les mesures menys generalitzades volen identificar focus d'infecció per contenir-los deixant la resta de la població lliure per treballar normalment. Hi ha dues maneres d'identificar focus d'infecció: fent proves a tota la població, o fent servir la tecnologia per inferir qui pot ser un risc.

Al poble de Vo', on es va patir la primera mort per coronavirus a Itàlia, hi van fer un estudi. La Universitat de Pàdua va fer proves a tots els habitants. Van descobrir que la gent infectada però

asimptomàtica té un paper fonamental en el contagi de la malaltia. Van trobar 66 casos positius que van aïllar durant 14 dies. Després de les dues setmanes, sis casos continuaven donant positiu al virus, per la qual cosa es van haver d'aïllar més dies. Infecció totalment sota control. No hi ha hagut més casos. No va caldre cap app.

L'opció de recórrer a apps no només és més invasiva des del punt de vista de la privadesa, sinó també molt menys precisa i efectiva. Si només es fan proves a gent hospitalitzada, l'app podrà contactar amb persones que hagin estat en contacte amb les persones infectades i demanar-los que s'aïllin. Però no tothom que hagi estat en contacte amb algú infectat es contagiarà. I els que ja han estat infectats n'hauran contagiat d'altres que alhora n'hauran contagiat d'altres a qui l'app no contactarà perquè són massa lluny a la cadena, i tots aquests casos continuaran asimptomàtics mentre el virus s'incuba. Amb aquesta mena de mètode, hi haurà molta gent que es quedarà a casa i que no tindria per què, i hi haurà gent pul·lulant arreu que hauria d'estar aïllada.

Cap app, per més sofisticada que sigui, i per més dades que tingui, pot substituir una prova de coronavirus. La tecnologia digital no és màgia, no resol tots els problemes i no sempre és la millor opció. Didier Raoult, especialista francès en malalties infeccioses, defensa que cal fer proves a tota la població i prioritzar-ne el diagnòstic. Fent proves només als que acaben a l'hospital hi haurà una majoria de gent

infectada que es detecta massa tard, ja amb símptomes i havent-ne contagiat d'altres. Si fem proves a tothom, podem confinar exactament la gent que cal aïllar. Ni més ni menys. La resta pot continuar amb la vida normal i reanimar l'economia.

El que calen no són més apps intrusives, sinó més proves. Per què no estem fent més proves de coronavirus? Per què no està sent aquesta la prioritat? Fer proves a tota la població seria car, sí. Però serà encara menys car que una quarantena generalitzada allargada o que una pandèmia fora de control.

A més de controlar la pandèmia, hem de pensar en el món que quedarà després de la tempesta; el món que estem construint amb cada decisió. La privadesa és important perquè dona poder a la ciutadania. Cal defensar-la. Massa vegades les mesures temporals preses en moments d'emergència arriben per quedar-s'hi. Tots hem de vigilar la democràcia. Les agències de protecció de dades especialment han de muntar guàrdia i assegurar-se que no hi ha cap abús a les nostres dades.

El coronavirus ja s'ha endut i s'emportarà molts éssers estimats. Ens ha robat el somni, està danyant l'economia, ens ha pres els plans. No podem deixar que també ens robi els drets. Cal cuidar la privadesa, fins i tot en temps de pandèmia.

L'era de la desinformació: quina responsabilitat tenen els mitjans, els usuaris i les tecnològiques?

Desinformació i intel·ligència. La intel·ligència artificial va més enllà de la simulació (***fake***) de la realitat?

Cecilio Angulo

La conferència de Dartmouth (EUA), l'esdeveniment que va veure néixer i definí la intel·ligència artificial (IA) el 1956 com una nova àrea del coneixement, en la seva crida a la participació va establir com a hipòtesi en definir la IA que, qualsevol aspecte sobre l'aprenentatge, o qualsevol altra característica de la intel·ligència, es pot descriure de manera que és possibre construir màquines que el simulessin (*to simulate it*) a partir d'aquestes descripcions. Una cosa simulada, seguint la descripció del Cambridge Dictionary per al terme *simulate*, és allò que sembla real però no ho és.

D'acord amb aquest mateix diccionari, *fake*, com a adjectiu, s'entén com una cosa falsa, en el sentit que és creada per semblar real, tot i que no ho sigui;

creat, doncs, amb la intenció d'enganyar la gent. No obstant, *simulate* és un verb, i *fake*, com a verb, admet accepcions com la de *pretend*, és a dir, 'fingir', 'simular', 'fer com si'. D'aquesta manera, la diferència més gran entre les accepcions —la d'*artificial* a *intel·ligència artificial* i la de *fake* a *fake news*— és en la intenció amb què es crea la simulació, ja sigui com a artefacte o com a engany.

Aquesta distància entre conceptes em recorda la que hi ha a l'hora de seguir una teràpia o medicació (*drug*, en anglès) quan parlem d'aferrament (*attachment*), una cosa més que desitjable per a la recuperació d'un pacient, enfront de l'addicció (*addicted*), quan el tractament es converteix en necessitat artificiosa, tal com passa en el cas de l'addicció a la morfina o a alguns aerosols nasals.

Es pot acusar un algorisme de tenir una intenció en ser definit? Es pot acusar la persona que el crea? La persona que l'utilitza? Alguns sospitosos habituals? El professor que genera problemes simulats perquè els alumnes aprenguin alguns conceptes o coneixements els està enganyant fent veure que són de debò? S'haurien de prohibir? El pilot de línies aèries que fa servir un simulador per anar afegint experiència en «hores de vol» abans d'enfrontar-se a pilotar un avió comercial, s'hauria de considerar un engany? Una cosa menys innocent, pensem en la generació de pacients sintètics simulant alguna malaltia: hauríem de negar als metges d'àrees poc poblades la capacitat de formar-se en malalties ra-

rament vistes en la seva àrea de salut? Els hauríem de facilitar dades de pacients reals d'altres hospitals? Com enfrontem el dilema de les dimensions ètiques i legals en aquests casos?

Encara podem acabar de reblar el clau anant més enllà de la definició que s'assigna a *artificial*, encara que sigui una cosa sintètica, impostada, falsa o simulada. La mateixa definició d'intel·ligència, a *intel·ligència artificial*, no deixa de ser una metàfora que habitualment s'ha associat a la idea de cervell, com en el cas de les denominades *xarxes neuronals artificials*, o a la idea de computador, com quan es parla de *cervell electrònic* a les màquines.

I, tanmateix, hi ha una altra possibilitat: la de la intel·ligència com a *false friend* o *fake friend*, en tant que definició de coneixement, en especial extret a partir de les dades o de la informació, tal com passa en els sistemes d'aprenentatge màquina o profund (*machine learning* o *deep learning*). Quan ens referim al CNI com a centre nacional d'intel·ligència, o a la CIA com a agència central d'intel·ligència; quan parlem de la intel·ligència britànica o de serveis de la intel·ligència antiterrorista, de quina mena d'intel·ligència estem parlant? És clara la primera funció d'extreure informació a partir de les dades obtingudes sobre el terreny i, d'aquesta informació, poder inferir un coneixement de la situació. De la mateixa manera es comporten els sistemes inductius d'aprenentatge, discriminant situacions, analitzant dades i etiquetant informació.

Ara sí, sota aquesta mirada metafòrica, també és fàcil definir la segona missió d'aquests serveis: la desinformació com a contramesura davant d'altres serveis d'informació. Així doncs, per què no podríem fer servir la mateixa mena d'eina que permet extreure coneixement com a una arma que injecta desconcert en un sistema antagonista? *Et voilà*, si ajuntem tots dos sistemes, el generador (G) de coneixement i l'antagonista (A) en forma de xarxa neuronal (N), tenim un sistema GAN, que tant pot crear situacions de vol problemàtiques per a l'entrenament de pilots, com vídeos o imatges falsos que permetin desacreditar una persona, institució o situació.

Hem de culpar el dissenyador de l'algorisme GAN per l'ús que se'n faci?, la companyia tecnològica o institució per a qui treballa? Jo no respondria afirmativament. Però, i si parlem de la companyia que entrena un algorisme específic pensat per desinformar? És ètic desinformar davant un atac terrorista? I en unes eleccions generals? En cas de pandèmia, és acceptable desinformar per «tranquil·litzar» la població?

L'últim element de l'equació, perquè un sistema sigui realment efectiu estenent el coneixement o desinformant de la realitat, són els mitjans de comunicació, els que es converteixen en propagandistes de la notícia. A l'era de la postveritat, quan les imatges d'una situació es fan servir per il·lustrar-ne una altra, amb capçaleres de noticiaris emetent vídeos creats a

partir de videojocs per simular/enganyar sobre una situació, les *fake news* són moneda d'alt valor.

De la mateixa manera que Asimov va determinar les lleis de la robòtica, en periodisme hi ha una llei bàsica que consisteix a contrastar la font d'informació. Em temo que fa anys que la gran majoria de mitjans de comunicació desatenen aquesta llei. No diguem ja a les xarxes socials, on la difusió de fets sense contrastar és la norma. Però, un cop hem arribat a aquest punt, deixem que siguin uns altres, des d'una visió més sociològica, els que descriguin fins a quin punt la desinformació mitjançant notícies falses posa en evidència i contrasta l'estupidesa humana amb la intel·ligència artificial.

L'espia a la butxaca

Necessitem lleis més estrictes perquè els mòbils treballin per a nosaltres i no per a d'altres

Carissa Véliz
El País, 25 de juliol de 2020

El teu mòbil és un espia i un *xivato*. Aquest intrús a la butxaca sap més sobre tu que tu mateix. I va explicant a d'altres tot el que veu i sent. L'espionatge als polítics catalans ens recorda com són de vulnerables aquests artefactes en què confiem les nostres dades més íntimes. El teu mòbil sap on vius, amb qui dorms, si dorms bé o malament, a quina hora et despertes, si has trencat les regles del confinament, qui és la teva família, qui són els teus amics llunyans i propers, qui és el teu metge, i pot inferir milers de dades més a partir dels seus sensors.

Gràcies a l'acceleròmetre, el teu mòbil sap si et saltes el límit de velocitat quan condueixes. També sap si camines ràpid o lent; amb aquesta informació es pot inferir la teva esperança de vida, entre d'altres

coses. Aquesta informació podria ser atractiva per a la teva asseguradora. L'acceleròmetre és suficient per identificar-te; resulta que ningú més no es mou ni camina exactament com tu. L'acceleròmetre també sap quan has begut massa alcohol per com canvia la teva manera de caminar.

El giroscopi, que registra l'orientació del teu mòbil a l'espai, és tan precís que una app maliciosa podria inferir les teves contrasenyes simplement accedint a com mous el mòbil quan tecleges. Aquesta informació és molt valuosa per a criminals que volen robar-te o extorsionar-te.

Es pot inferir si pateixes depressió o si tens problemes de memòria, analitzant com desplaces el dit per la pantalla del mòbil quan escrius i quan busques algú a la teva llista de contactes. Segur que a l'empresa que està pensant contractar-te li interessa saber més sobre el teu estat emocional i les teves habilitats cognitives.

El teu mòbil guarda les teves empremtes digitals, si les fas servir per desbloquejar el telèfon. O una còpia matemàtica de la teva cara, si fas servir aquesta tecnologia biomètrica. Amb aquestes dades algú podria fer-se passar per tu, per robar les dades, els diners, o per cometre crims sota la teva identitat.

El teu GPS i el teu *bluetooth* saben exactament on ets i amb qui. Si vas parlar amb un periodista, si vas visitar una clínica especialitzada en addiccions i desintoxicació, si vas anar a una protesta, si estàs sent infidel a la teva parella, o si visites l'hospital sovint.

Si algú et pirateja el mòbil pot tenir accés a la teva càmera i micròfon, a tots els teus missatges, correus electrònics, converses, contactes, fotos, enregistraments, cerques a internet, i més.

La mala notícia és que, si algú amb prou mitjans i ganes vol violar la teva privadesa a través del mòbil, el més segur és que ho aconsegueixi. Per increïble que sembli, els programes espia (encara) no són il·legals a la major part del món, tot i que haurien de ser-ho. La bona notícia és que hi ha moltes coses que pots fer per dificultar l'accés a les dades que tens al mòbil.

Aquestes mesures no són inútils, encara que no siguin infal·libles. Millorar la teva ciberseguretat és com posar-te un bon pany a la porta de casa. Si la policia vol entrar, entrarà, però si un criminal vol aprofitar-se del primer incaut amb qui s'encreui no seràs tu. Reforçar la teva privadesa també et protegirà que les empreses vulguin aprofitar-se de les teves dades.

El primer: escull bé el mòbil. No compris un mòbil fabricat per una empresa els ingressos de la qual depenen d'accedir a les teves dades personals. El conflicte d'interès de l'empresa entre enriquir-se amb les teves dades i protegir la teva privadesa sempre et posarà en risc.

Compte amb les apps que fas servir. Utilitza només les necessàries, mira de verificar que siguin fiables amb una cerca a internet, esborra les que no fas servir, i no donis a cap app accessos (a la càme-

ra, micròfon, localització o contactes) que no siguin imprescindibles.

Per enviar missatges, fes servir una app que utilitzi encriptació d'extrem a extrem (*end-to-end encryption*). L'app de missatgeria més segura és probablement Signal. Pots triar que els teus missatges desapareguin després de llegir-los. Així et protegeixes, no només d'amenaces externes, sinó també de la persona a qui envies el missatge. Fes servir un correu electrònic segur, per exemple, ProtonMail.

Compte de connectar-te a una wifi gratis. Les teves dades personals quedaran exposades al propietari de la xarxa i a d'altres usuaris connectats a la mateixa wifi. Si cal connectar-te a una xarxa insegura, fes servir una VPN, però assegura't que sigui fiable, perquè rebrà les teves dades.

El que és analògic s'ha tornat més segur que el que és digital. Deixa el teu mòbil en un calaix de tant en tant, o en una bossa Faraday que bloqueja el senyal. Tingues reunions amb amics on estiguin prohibits els espies digitals. Quan passis temps amb la família, que els mòbils es quedin en una altra habitació.

Necessitem lleis més estrictes per assegurar-nos que els mòbils treballen per a nosaltres i no per a d'altres, que actuen a favor nostre i no en contra. Som davant un procés de civilització. Però, mentre domem el *salvatge Oest* d'internet, si realment vols mantenir alguna cosa privada, no ho expliquis al mòbil.

La regulació legislativa, aquesta necessitat en el negoci de les dades personals

Tres exemples de regulació, o desregulació, d'allò que és personal

Cecilio Angulo

Els mitjans de comunicació, les persones expertes en tecnologia, les entitats i administracions públiques del ram, totes, no fan més que repetir-nos que les dades són el nou petroli, el nou or: la matèria primera d'una economia nova i puixant que impacta en el PIB dels països i en el compte de resultats de les empreses. No deixa de ser eloqüent, resseguint el símil del petroli o de l'or, que el temps que ha passat entre l'explotació inicial d'aquests recursos i la regulació posterior portés, en el passat, a èpoques desenfrenades i gens edificants per a la humanitat: el *salvatge Oest*, l'època colonial o el comerç d'esclaus van ser èpoques ben disfressades amb neollenguatge que van passar a denominar-se la conquesta de l'Oest, la conquesta d'Amèrica o la romanització. I tot i així,

quantes guerres no continuen lliurant-se avui dia amb el rerefons d'aquestes matèries primeres?

Sí, la regulació torna a arribar tard. La recol·lecció, explotació i comerç de les dades com a negoci s'ha estat fent, i així continua sent, esquivant una regulació legislativa que posi ordre, potser límit, a les pràctiques abusives que s'estan emprant de manera generalitzada. Els propietaris de les dades, la majoria de vegades els ciutadans del carrer, hauríem de poder decidir sobre el nostre dret a la recol·lecció d'aquesta informació, de quina manera estem disposats que s'explotin i, en darrer lloc, accedir als beneficis derivats del tràfic de dades, o negar-nos a la seva comercialització com a negoci.

El marc regulatori és clau en tots aquests punts per definir quina mena de contractes s'han d'establir. En l'actualitat, el problema més obvi que es planteja és la recol·lecció, explotació i comerç de dades obtingudes per internet. S'ha iniciat una regulació en l'acceptació de *cookies* a les pàgines web que visitem. No obstant, el cert és que no saps a què t'estàs comprometent. El nostre analfabetisme digital, assumit o imposat per la legislació, ens equipara a estar signant X en tots els contractes que ens posen davant. Estem confiant, equivocadament, que l'administració té cura de nosaltres i no permetrà que els contractes que signem en forma de *cookies* permetin segons quina mena d'ús en la cessió de dades. Però no és així: estem signant la nostra esclavitud i servitud.

Davant aquesta realitat, no és d'estranyar que hi hagi veus que s'alcin en contra de qualsevol mena de comerç de les dades, en especial, al·ludint al dret a la privacitat. Per ser honestos, és una opció ràpida i radical que protegeix els ciutadans. No obstant això, l'impacte que té en l'economia és devastador. Per part meva, insisteixo a declarar que es tracta d'un tema de confiança en la legislació i funcionament del sistema. I, si he de dir la veritat, avui dia, ni la legislació regula com cal ni el sistema és confiable. Permeteu-me il·lustrar un tema tan general en tres exemples.

Què hi ha de més personal que el teu propi ronyó? I la gent dona òrgans. Per què? Perquè sap que aquest ronyó a Espanya, a Europa, no acabarà al mercat negre. Es farà servir amb l'objectiu de beneficiar la persona a qui millor s'adeqüi segons la seva necessitat, atenent un criteri purament mèdic. És possible un altre marc regulatori en què la donació comporti remuneració? Sí, hi ha països amb aquesta forma de regulació. Hi podem estar d'acord o no, però, sempre, l'Estat s'encarrega que hi hagi un marc regulatori. Una cosa que és tan evident a un àmbit tan personal, per què no passa amb les dades? Les dades també són personals. No hi hauria d'haver una regulació semblant per a les dades?

Alerta! Cal parar atenció a com s'entén la privacitat de les dades personals. Segons la meva opinió, s'hauria d'entendre des del punt de vista de la intimitat, la privacitat com un element propi i definitori

d'un mateix. Aquí cal anar amb molt de compte a l'hora de distingir la necessitat de regulació del que és privat i d'allò que és privatiu, que sembla que és el punt que interessa a les corporacions. Un gran problema en la regulació de la privacitat és considerar la contraposició amb la transparència. Així doncs, amb l'excusa de preservació de la privacitat, la regulació deriva cap al privatiu, que és justament allò, no només contraposat, sinó contrari al que és transparent.

Així, l'existència d'una regulació de comptes opacs es defineix com a dret a la privacitat, quan en realitat és un dret al privatiu. Un bon exemple d'això, i un gran problema que tenim avui dia, amb persones que ho defensen a capa i espasa, són els *bitcoins*, o criptomonedes en general. La criptomoneda és el mecanisme que fan servir totes les màfies per pagar les seves transaccions il·lícites, ja siguin drogues, armes o diamants de sang. És el recurs que fan servir alguns governs per organitzar les seves clavegueres o evitar sancions internacionals. Criptomonedes que, d'altra banda, estan malbaratant i destruint el planeta amb el procés de minatge. És aquest el model desitjat de negoci per explotar?

La cosa és encara pitjor quan la regulació de l'accés a les dades, establerta per un govern, serveix com a excusa per al bé comú. En l'època de la pandèmia, no van ser pocs els grans centres d'investigació internacional que van intentar aclarir l'evolució de la pandèmia mitjançant les dades facilitades, com no podia ser d'una altra manera, pels governs. Tanmateix, a

tall d'exemple, els caps de setmana no hi havia dades; es restringien. Així, els dilluns es carregaven les dades de la setmana anterior. O bé, per raons espúries, es recomptaven i es traçaven seguint noves mesures, però no es mantenia la comptabilitat anterior. És creïble pensar que l'esforç econòmic i humà que s'estava fent en aquesta època no permetia un servei permanent de recollida d'informació? La restricció de l'accés a les dades deixava ben clar que els governs havien desestimat intentar solucionar el problema i només volien fer veure que l'estaven resolent. La desinformació com a forma d'intel·ligència; la pura estupidesa humana.

Homo homini lupus. Thomas Hobbes defensava el contracte social per assolir la pau social: una autoritat absoluta que protegeixi la societat. Un marc regulatori que protegeixi l'home d'ell mateix. Ara bé, volem una societat monolítica com a la Xina?, una autoritat dictada pel mercat, a l'americana?, la hipocresia europea? Mentre ens decidim, recorrem a allò senzill, culpem la dada, discutim sobre l'ètica d'aquesta dada, el biaix que té, o la seva gestió, com si la dada, a diferència de l'or o del petroli, no fos més que obra de la mateixa societat.

Prohibir l'economia de dades

No és massa tard per recuperar el control de la nostra privadesa i de les nostres democràcies

Carissa Véliz
El País, 2 d'octubre de 2020

El documental de Netflix *The Social Dilemma* pinta un quadre aterridor del mal que la tecnologia digital està causant en els individus i les societats. L'addicció a la pantalla, l'augment dels índexs de suïcidi i les interferències electorals només són alguns dels problemes que cal agrair a *Silicon Valley*. Però el que el documental no emfatitza prou és el motor que impulsa aquesta destrucció social: un sistema econòmic basat en la violació massiva i sistemàtica del nostre dret a la privadesa.

Els exemples anteriors són força preocupants, però són només la punta de l'iceberg quan es tracta de les implicacions de la pèrdua de privadesa. Només hem de mirar la història de la targeta perforada d'IBM, i com va permetre a les autoritats nazis

explicar i categoritzar els ciutadans europeus, per veure com aquesta mena de tecnologia de vigilància és perfecta per ser desplegada per un règim opressiu. Si les companyies tecnològiques i els governs volen estar al costat correcte de la història, farien bé de protegir la nostra privadesa.

Fins i tot a les societats més capitalistes estem d'acord que certes coses no són a la venda: les persones, els vots, els òrgans, els resultats dels partits esportius. En aquesta llista hi hauríem d'afegir les dades personals. Que permetem que les empreses es beneficiïn del coneixement que algú té una malaltia, o fins i tot de si ha estat víctima d'una violació, és monstruós.

Per entendre el que l'economia digital significa realment per a la privadesa necessitem veure les dades personals com un actiu tòxic. La recol·lecció de dades personals enverina els individus perquè ens fa vulnerables a la discriminació injusta, a la humiliació pública, al robatori de la identitat, i més. Enverina les societats, perquè posa en perill la igualtat i la democràcia. Els ciutadans no estem sent tractats com a iguals. A cadascun de nosaltres se'ns tracta d'acord amb les nostres dades. No veiem el mateix contingut, no paguem el mateix preu pel mateix producte, no se'ns ofereixen les mateixes oportunitats.

La tecnologia no necessita comerciar amb les dades personals per funcionar bé. L'economia de dades només és un model de negoci. La bona tecnologia hauria de funcionar per als ciutadans, no per

als anunciants o els agents de dades. Ens hauria de respectar els drets i les democràcies liberals, i protegir la nostra privadesa.

Prohibir la comercialització de dades personals no és ni radical ni extrem. El que és radical i extrem és un sistema econòmic sustentat en la violació de drets.

Actualment som al començament d'un procés civilitzador similar al que va fer que la nostra vida analògica fos més amable, més habitable. La regulació es va assegurar que els aliments que es venguessin fossin comestibles, que els clients poguessin tornar els productes defectuosos, i que els cotxes tinguessin cinturons de seguretat. El moment històric actual és crucial si volem domar el *salvatge Oest* d'internet. Les regles bàsiques que establim ara per a les dades personals determinaran aspectes fonamentals de les nostres vides durant les properes dècades. És crític que fem les coses bé. Frenar el costat fosc de la tecnologia requerirà canviar el model de negoci dels voltors de dades que viuen de les nostres empremtes en línia. Els experts i la ciutadania han d'enviar un missatge clar als governs sobre el que cal: la fi de l'economia de dades; una prohibició completa del comerç de dades personals.

També necessitem solucions regulatòries per assegurar-nos que les nostres dades només es facin servir en el nostre interès, i mai en contra. Els deures fiduciaris hi són per protegir els individus en una posició de debilitat contra els professionals que se

suposa que els han de servir, però que podrien tenir conflictes d'interessos. Així com els metges, advocats i assessors financers estan obligats a complir aquests deures, qualsevol que tingui les nostres dades personals ha d'estar obligat a fer-les servir en benefici nostre. Així mateix, cal prohibir el contingut personalitzat. Quan cadascú veu una realitat segmentada, la societat es fragmenta.

Si haguéssim prohibit el comerç de dades a temps, i haguéssim regulat els controladors i processadors de dades adequadament, no ens hauríem de preocupar que la propaganda personalitzada *en línia* influís en les eleccions, o de la possibilitat que les aplicacions de rastreig de contactes fessin un mal ús de les nostres dades. Però no és gaire tard per recuperar el control de les nostres dades personals, i amb això, les nostres formes de vida i les nostres democràcies.

Com defenso al meu llibre, *Privacy Is Power* ('La privadesa és poder'), és temps de prohibir la comercialització de dades personals.

Noves atraccions en la investigació científica: les regulacions frenen la ciència?

Cap a una forma de generació de confiança en el progrés científic i tecnològic

Cecilio Angulo

Els avenços científics i tecnològics sempre plantegen el dubte de cap a on i fins on té sentit progressar. En salts qualitatius com el de la digitalització, la nova zona d'estudi és tan desconeguda, i comporta unes novetats tals, que es fa molt difícil mantenir el sentit comú en tots els casos. I això, suposant que el que entenem per sentit comú, segons la nostra experiència històrica, sigui extrapolable a aquest nou domini.

La sensació en aquests moments, per als que treballem en digitalització, és similar a la d'haver-nos colat en un nou parc d'atraccions amb totes les atraccions a punt per poder-les posar en marxa. Uns poden identificar el toro mecànic, d'altres la roda, però què és aquest habitacle amb seients? Un simulador de realitat virtual? Una recreació de gravetat

zero? No hi ha muntanyes russes, però veiem vagons al bell mig d'una zona clarejada.

Ara que ja hi som a dins, qui determina amb quines atraccions comencem? Qui es posa al comandament de les atraccions? Qui prohibeix ningú que explori noves atraccions? Què passa quan les regles aplicades en unes atraccions no funcionen en d'altres? Hi ha un límit mínim d'alçada? Pes màxim o nombre d'ocupants?

En aquestes circumstàncies, per a molts, algú que aposti per una regulació en la investigació i ús d'aquestes noves atraccions no deixa de ser un aixafaguitarres. Que no és l'assaig i error una forma efectiva d'investigació? Doncs ja s'autoregularà l'ús de les atraccions. El primer que hi arriba, la prova i decideix què en pot fer. Sempre hi ha gent disposada a muntar. La promesa de la diversió és més forta que la por d'acabar amb una costella trencada. Allò d'aquells que van sortir commocionats era una altra atracció. Amb aquesta no fa pas la sensació que pugui passar res de dolent, oi?

Estic segur que si ens imaginem cinc amigues i amics en aquesta situació, cadascun d'ells actuaria diferent a l'hora de gestionar les seves expectatives i pors. I si ens imaginem el comportament per grups? Dels grups que ja hi existien abans d'entrar al parc o de tots els nous que de ben segur es faran a la vora de cada atracció. A l'estil de les empreses. I els governs? Podran fer servir les mateixes armes de pressió i control social en aquesta nova situació?

Sens dubte, regular la investigació en aquesta situació és car en termes de pèrdua d'oportunitats, però la desregulació o autoregulació no són l'alternativa, són la ruïna. La tecnoètica, l'humanisme tecnològic, o tal com es vulgui definir el fet d'impregnar de valors universals l'exploració científica i tecnològica, han d'establir les bases d'aquesta regulació. Per això és important assegurar-se que els científics i els tecnòlegs han tingut accés a aquests valors universals, i que han estat conscienciats de la seva validesa permanent i atemporal, durant l'etapa de formació acadèmica. És així actualment?

De la mateixa manera, és cert que moltes regulacions analògiques s'han de desaprendre en aquest nou domini, ja que suposen una arbitrarietat que restringeix el pensament científic i tecnològic. Però hi ha uns valors constants independents de l'entorn i que s'han de mantenir en tot moment. Per exemple, el consentiment dels usuaris de pujar a una atracció o que en puguin baixar quan vulguin. O la transparència en les normes d'ús, que han de tenir un llenguatge clar i entenedor.

La intel·ligència artificial, com la robòtica, només són dues d'aquestes àrees en el parc d'atraccions. Potser són les més visibles, extenses o preferides, aquelles que de seguida ens venen al cap quan pensem en la seva necessitat de regulació, ja sigui sobre els biaixos dels resultats i recomanacions, el tractament de les dades o per la manera com afecten el mercat laboral. Les criptomonedes, les cadenes de blocs

(*blockchain*), la ciberseguretat o la computació d'altes prestacions són algunes de les atraccions incorporades recentment al nou parc de la digitalització.

Hem d'aconseguir, mitjançant la regulació, que totes siguin confiables per fer-les servir. El marcatge d'un iogurt amb la data recomanada de consum, la declaració nutricional dels components i el textet en un idioma oficial són mesures que donen confiança al consumidor a l'hora de decidir-se pel producte, més enllà del color de l'etiquetatge, el gust o la textura final del mateix comestible. D'una manera semblant, l'etiquetatge CE de les joguines que comprem per als nostres fills no ens assegurarà amb total certesa que no es poden manipular o que no els farà cap mal, però ofereix confiança al consumidor: s'ha considerat evitar peces petites que es poden empassar, no es fan servir materials ni colorants tòxics, són fàcilment higienitzables i van amb una guia d'instruccions o d'usuari.

La incorporació d'aquestes mesures de confiabilitat i seguretat en el producte n'eleva el cost i redueix les possibilitats creatives en el disseny i fabricació. És cert. Com també ho és que els nens abans continuaran jugant amb una capsa de cartró que amb la joguina que empaquetava, i els adults farem el nostre quèfir a casa, sense cap mena de control sanitari. Són algunes d'aquestes decisions personals que prenem, més enllà de qualsevol regulació i que són part de la nostra vida, encara que sigui menys segura. Això

també és part de la tecnoètica i de l'humanisme tecnològic.

Entenguem els comitès d'ètica, o les regulacions administratives, com una manera d'assegurar la confiança en productes que poden ser utilitzats per o sobre tercers, i no com una manera de coartar o frenar la investigació científica i tecnològica. Pugem a les atraccions, però amb seguretat.

Protegim les nostres dades. No oblidem com les feien servir els nazis

El Tercer Reich va utilitzar informació aportada pels ciutadans per sentenciar-los a mort

Carissa Véliz
El País, 12 de setembre de 2021

A les dades personals se'ls pot donar, se'ls dona i se'ls continuarà donant un mal ús. I alguns dels usos abusius de les dades personals són més mortífers que no pas l'amiant.

Un dels exemples més letals d'abús de les dades va ser el règim nazi durant la Segona Guerra Mundial. Quan els nazis envaïen un país, de seguida s'apoderaven dels registres locals com a primer pas per controlar la població i, en particular, per localitzar els jueus. Hi havia molta variació entre països, tant pel que fa al tipus de registres que portava cadascun com a la reacció que mostraven davant aquella set nazi de dades. La comparació més extrema és la que ofereixen els Països Baixos i França.

Jacobus Lambertus Lentz no era nazi, però va fer més pel règim nacionalsocialista alemany que la majoria dels més fervents antisemites. Era l'inspector de registres de població d'Holanda i la seva feblesa eren les estadístiques demogràfiques. El seu lema era «Registrar és servir». El març del 1940, dos mesos abans de la invasió nazi, va proposar al govern del seu país la instauració d'un sistema d'identificació personal que obligués tots els ciutadans a portar un carnet d'identitat. La targeta feia servir tintes translúcides que desapareixien a la llum d'un llum de quars, així com un paper amb marca d'aigua, tot amb el propòsit de dificultar-ne la falsificació. El govern va rebutjar la seva proposta amb l'argument que un sistema així seria contrari a les tradicions democràtiques holandeses, ja que equivaldria a tractar les persones comunes com si fossin delinqüents. Lentz es va emportar una gran desil·lusió. Uns mesos més tard, va tornar a proposar la mateixa mesura, encara que, aquesta vegada, a la *Kriminalpolizei* del Reich. Les forces d'ocupació van estar encantades de posar-les en pràctica.

Tots els adults holandesos van passar a tenir l'obligació de portar un carnet d'identitat. A les targetes que portaven els jueus s'hi estampava una J: una sentència de mort a les butxaques.

A més dels carnets, Lentz va emprar màquines Hollerith —aparells tabuladors venuts per IBM que es valien de targetes perforades per gravar i processar dades— per ampliar la informació enregistrada

sobre la població. El 1941 es va emetre un decret que obligava tots els jueus a inscriure's a la seva oficina local del cens. Durant dècades, els holandesos havien recopilat ingènuament dades sobre la religió i altres detalls personals dels seus ciutadans amb la idea de crear un sistema que pogués fer un seguiment de cada individu «des del bressol fins a la tomba». Lentz i el seu equip de col·laboradors van fer servir les màquines Hollerith i tota la informació de què disposaven per facilitar als nazis el seguiment de persones.

A França, a diferència del que passava als Països Baixos, els censos no recaptaven informació sobre religió per raons de privadesa. L'últim cens que havia recopilat dades d'aquesta mena datava del 1872. Henri Bunle, cap de l'oficina d'estadística general francesa, va deixar clar a la Comissió General sobre Afers Jueus el 1941 que França desconeixia quants jueus tenia i, encara més, on vivien. A més, França no tenia l'àmplia infraestructura de targetes perforades de què disposaven els Països Baixos, cosa que dificultava la recopilació de noves dades. Si els nazis volien que la policia portés un registre de la població, ho hauria de fer manualment, amb formularis de paper i fitxes de cartolina.

Sense les tabuladores Hollerith no hi havia manera de classificar i computar la informació que es recopilava sobre els ciutadans. Els nazis estaven desesperats. René Carmille, que, a més d'auditor general de l'exèrcit francès, era un entusiasta de les targetes

perforades i tenia diverses màquines tabuladores (incloses algunes Hollerith), es va oferir com a voluntari per posar ordre en aquell caos i lliurar els jueus de França als botxins.

Carmille va desenvolupar un número nacional d'identificació personal que funcionava com un codi de barres descriptiu de cada individu; va ser el precursor de l'actual número de seguretat social francès. Es van assignar diferents números per representar característiques personals com la professió. Carmille també va preparar el cens del 1941 per a tots els ciutadans francesos d'entre 14 i 65 anys. A l'onzena pregunta es demanava als jueus que s'identifiquessin a través dels seus avis paterns i materns, i la religió que professaven.

Van passar els mesos i les llistes de jueus que els nazis esperaven que Carmille els facilités no arribaven. Els nazis s'impacientaven. Van començar a practicar batudes contra jueus a París, però, sense les tabulacions de Carmille, depenien que els jueus es lliuressin ells mateixos o fossin delatats per veïns. Van passar més mesos i les llistes van continuar sense arribar.

Els nazis no ho sabien, però René Carmille no havia tingut mai cap intenció de trair els seus conciutadans. Era un dels més alts càrrecs de la Resistència francesa. La seva operació va crear unes 20.000 identitats falses, va fer servir les seves tabuladores per identificar persones que estaven disposades a combatre contra els nazis. Les respostes a la pregunta nú-

mero 11 sobre si els enquestats eren jueus no es van tabular mai. Els forats corresponents mai no van arribar a perforar-se i aquestes dades es van perdre per sempre. Fins avui, s'han descobert més de 100.000 d'aquelles targetes perforades adulterades; targetes que no van arribar a lliurar-se als nazis. Centenars de milers de persones van ser salvades per una sola persona que va decidir no recopilar les dades, les dades tòxiques.

Sembla raonable suposar que Carmille sabia que acabarien per descobrir-lo si no lliurava les dades que havia promès. Les SS el van arrestar el 1944. El van torturar durant dos dies i després el van enviar a Dachau, on va morir d'extenuació el 1945.

La col·lecció de dades pot matar. Els holandesos van patir la taxa de mortalitat d'habitants jueus més gran a l'Europa ocupada: un 73%. D'una població estimada de 140.000 jueus holandesos, més de 107.000 van ser deportats, i 102.000 van ser assassinats. La taxa de mortalitat dels jueus a França va ser del 25%. D'una població estimada d'entre 300.000 i 350.000, 85.000 van ser deportats i a 82.000 els van matar.

El millor indicador que alguna cosa passarà en el futur és que hagi tingut lloc en el passat. Aquestes històries no són una galàxia llunyana d'un univers de ficció. Són històries reals sobre allò què hem d'aprendre per no repetir els mortífers errors del passat.

Imagina un règim autoritari contemporani apropiant-se de totes les dades personals. Els dèspotes del passat disposaven de retalls d'informació en comparació amb els milers de dades a què es pot accedir avui sobre qualsevol persona al món, amb només uns clics. Un govern autoritari podria conèixer tots els nostres punts febles sense necessitat de posar-hi gaire interès. Si poguessin predir tots els nostres moviments, podria ser el començament d'un règim invencible. Perquè et facis una idea de com són de perilloses les dades personals, imagina't un règim com el nazi, però actualment, amb accés a dades en temps real sobre la teva ubicació, el perfil facial, la manera de caminar, la freqüència cardíaca, les idees polítiques, l'afiliació religiosa i moltes coses més.

Educar en la digitalització

La digitalització no planteja problemes nous, sinó que permet precisar, en una nova realitat, els que ja hi ha

Cecilio Angulo

La digitalització del nostre entorn, de la nostra vida, és un procés imparable. Evitable, mitigable, sí, però ineludible. És una mena de canvi que aporta beneficis enormes, però també deixa víctimes al llarg del camí. És una època trencadora que ja hem viscut altres vegades. Qui pot dir avui que viu d'esquena a la industrialització? O a la urbanització? Només les societats que no n'han tingut oportunitat o els col·lectius, molt petits, que hi senten rebuig.

Com tot procés desafiant amb l'*statu quo*, l'educació és la millor eina per entendre'l i decidir com hi podem conviure o viure-hi sense. Es pot oblidar una mare d'explicar al seu fill què és un semàfor i quin n'és l'ús adequat? Permetrem que una jove es posi al volant d'un vehicle sense que abans hagi demostrat

l'habilitat que té a l'hora de conduir i la comprensió de les regles de trànsit? Viatjarà sol un estudiant menor d'edat en transport públic cap a l'escola sense que abans hi hagi anat acompanyat, diverses vegades, per un adult? A quina edat i en quines circumstàncies permetrem que un menor es desplaci per la ciutat pel carril bici o amb un patinet elèctric?

Amb total seguretat, la realitat condicionarà la resposta d'aquestes preguntes i no serà única, ja que hi influirà en forma d'oportunitat o necessitat; de l'entorn familiar o educatiu; de dimensió de la ciutat o de regulació administrativa. De la mateixa manera passa a l'actualitat amb els processos de digitalització. Qui explica a la seva filla què és una *cookie* o com es gestionen les paraules de pas a les pàgines web? En quines condicions pot un menor tenir accés al telèfon mòbil? Podrà navegar per internet sense vigilància d'un tutor o sense un entorn segur de navegació? A quina edat permetrem que es registri en una o altra xarxa social?

Són molts els dubtes i els reptes educatiu que es plantegen davant aquest procés imparable de digitalització. Llancem el primer missatge: no hi ha una resposta única al repte digital educatiu, ja que els adults més propers no són sempre els millors assessors per als menors en educació en ambients tecnològics. La majoria de vegades per desconeixement; d'altres, per la visió esbiaixada que tenen d'un món analògic i simplista. La prohibició de l'ús dels telèfons mòbils a qualsevol edat i en qualsevol circums-

tància en l'àmbit educatiu és una d'aquestes mesures simplistes que obre un debat no resolt.

Un altre exemple ens remet, com no podia ser d'una altra manera, a la protecció de la privacitat dels menors en l'àmbit educatiu. Encara recordo xerrades amb directors d'escola sobre la necessitat del canvi del document de cessió de drets d'imatge. Els tutors legals estaven signant un document que establia una cessió categoritzada sobre el suport de la imatge, es parlava de CD!, quan el punt d'interès era el rang de difusió d'aquestes imatges, no hi havia condicionant a l'hora de pujar les imatges gravades a l'escola a YouTube o Facebook! Negar-se a signar la cessió de drets podia implicar que el nen no pogués participar en una obra de teatre, però l'alternativa no era gaire millor: indefectiblement, (gairebé) totes les gravacions acabaven visibles a les xarxes socials en format públic. Afortunadament, l'administració educativa va acabar entenent el problema associat a la imatge del menor com un problema de privacitat i no de comercialització.

La digitalització ha fet evident que l'educació és una cosa líquida, com la salut, una realitat que transcendeix les quatre parets del recinte escolar i s'estén a tots els àmbits socials del menor. Posem, per exemple, l'ús de sistemes de reconeixement facial en llocs públics. Es nota una gran preocupació social amb el fet del *Gran Germà*: «Ens estan vigilant amb les càmeres». No obstant això, cal entendre què vol dir *reconeixement* i quin n'ha de ser el límit. Un re-

coneixement implica associar una persona a un cert grup, com pot ser el grup de passatgers amb permís per accedir a un avió. Però, alerta!, *reconèixer* no vol dir identificar, que és el que, de manera abusiva, fan les empreses i el mateix govern. Jo voldria que el sistema d'accés amb reconeixement facial em donés accés a embarcar a l'avió, però no que m'identifiqui davant un tercer. «Si t'identifico, et puc reconèixer» no és una raó objectiva per permetre la identificació facial. Els exemples tecnològics com aquest, o l'anterior sobre drets d'imatge, són els que permeten introduir conceptes d'ètica, de drets civils, de necessitat de regulació en l'educació. Sense que hi hagi una resposta que sigui més apropiada que una altra. Ho justifica allò d'«aquí s'ensenya a pensar no què hem de pensar» i són conceptes extrapolables a qualsevol domini científic o social. L'exemple de l'embarcament a l'avió es pot fer extensible al reconeixement facial en el control d'assistència a un centre escolar.

Em serveix aquest exemple precedent, i el següent, per llançar el segon missatge, que penso que és important, sobre l'impacte de la digitalització en l'educació. Sí, la digitalització deixa víctimes, per omissió o deliberadament. Cal adonar-se'n, sense escarafalls, sense hiperventilar. Cal alertar, no alarmar d'aquests perills. Els cartells que llegim en espais comercials, al transport públic, a la via pública!, com ara «Somriu, t'estem gravant» associats a «és per la teva seguretat», suposen una invasió injustificada de la privacitat. Enregistrar les meves accions en un

entorn públic perquè les vegi qualsevol persona en qualsevol moment em fa estar més segur? Pot entendre's que aquest ús permetrà, en escasses i comptades ocasions, ajudar a la investigació d'un delicte que s'hagi comès. Tanmateix, el missatge educatiu que llança és devastador en la formació dels joves. Per defecte, les teves accions podran ser analitzades i escrutades per qui sigui en qualsevol moment. Així, la sensació de «llibertat» envers aquest atropellament a la privacitat només s'aconsegueix «escapant» de les càmeres. Només s'és lliure escapant del sistema, de la vigilància. I la vigilància va molt més enllà del docent.

Tal com es pot observar, la digitalització planteja reptes educatius en molts casos més enllà de les quatre parets de l'escola, però impacta directament en la institució escolar. Vol dir plantejar-se el què i el com, tal com es fa en l'experimentació científica. Sens dubte encara queden molt més desafiaments per anotar, des de la recol·lecció de dades i la vida útil que tenen, fins als biaixos en la definició de les solucions. La dualitat entre eines estandarditzades i monolítiques o la diversitat d'aproximacions, malgrat els problemes d'interoperabilitat. Sí, sembla una neollengua, però no ho és. Al cap i a la fi, parlem de quin sentit té i durant quant de temps una fitxa policial o un expedient sancionador; per què la meva simple presència, amb una actitud o una altra, o una vestimenta o una altra, provoca reaccions diferents; o per què s'han de defensar les llengües minoritàri-

es o s'hauria de potenciar l'ús de només una. Així doncs, no: la digitalització no planteja problemes nous, sinó que fa evidents, permet precisar, en una nova realitat, els que ja hi ha.

Digitalitzar és vigilar

Traslladar qualsevol activitat al món digital és convertir-la en dades, crear un registre, posar etiquetes i fer-la rastrejable, per això cal protegir espais de privadesa analògica

Carissa Véliz
El País, 3 de desembre de 2021

Les grans tecnològiques volen continuar creixent, perquè les empreses que no van de pujada van de baixada, i ningú no vol anar de baixada. Però han estat tan reeixides i són tan gegantines, que no és fàcil trobar cap lloc cap a on créixer. Com *Alícia al país de les meravelles,* atrapada a la casa del conill després d'haver crescut massa, les tecnològiques tenen els braços i les cames sortint-los per les finestres i la xemeneia de la casa de la democràcia.

Una possibilitat per créixer encara més és intentar atraure nous clients. Però com poden trobar un públic nou quan la gran majoria dels adults amb accés a internet a tot el món ja són els teus usuaris? Una opció, que Facebook està perseguint sense escrúpols, és concentrar-se en nens cada cop més petits.

El nou grup d'interès per a la tecnològica són nens de sis a nou anys. Si fos per l'empresa, tot nadó naixeria amb un compte de Facebook. Aquesta opció és limitada, perquè tard o d'hora es captarà tots els nens vulnerables per ser exposats a la seva tecnologia, i també té riscos. Hi ha diverses investigacions en marxa sobre Facebook i Instagram als Estats Units per haver causat danys a menors sabent-ho. I cap a on créixer, llavors?

Una altra possibilitat és digitalitzar cada cop més aspectes del món. Tot i el ràpid avenç de les tecnologies digitals, la major part de la nostra realitat continua sent analògica, fins i tot després de la pandèmia del coronavirus. La majoria de les nostres compres encara no són per internet. La majoria dels lectors prefereixen llibres en paper. Són analògics molts dels espais urbans, les cases, la roba, moltes de les converses, les percepcions, els pensaments i els nostres éssers estimats.

Els gegants tecnològics comparteixen el desig de digitalitzar el món perquè és una manera fàcil de guanyar terreny, d'engrandir la casa. Tot el que és analògic és un recurs en potència: es pot convertir en dades per després comercialitzar-les. Per això Facebook ha tret unes noves ulleres amb Ray-Ban que tenen micròfons i càmera. Més captura de dades. Per això el nou sistema operatiu de l'iPhone pot digitalitzar text i números des d'una imatge, pot escanejar edificis perquè siguin reconeguts a l'aplicació de mapes, té algorismes que poden identificar objectes

en un vídeo en temps real, i fa possible convertir fotos en models tridimensionals per fer-se servir a la realitat virtual. Per això Microsoft està proposant una plataforma que crea avatars tridimensionals per tenir reunions més interactives. I per això Facebook —perdó, Meta— està insistint en el seu metavers.

Els titans tecnològics ens asseguren que les seves noves invencions respectaran la nostra privadesa, per descomptat. El que ometen és el que anomeno la *llei de ferro de la digitalització*: digitalitzar és vigilar. No hi ha tal cosa com una digitalització sense vigilància. L'acte mateix de convertir en dades allò que no ho era és una forma de vigilància. Digitalitzar implica crear un registre, posar etiquetes a les coses perquè sigui més fàcil trobar-les i seguir-les. Digitalitzar equival a fer rastrejable allò que no ho era. I què és rastrejar, sinó vigilar?

Fa unes setmanes vaig tenir una conversa amb un parell d'enginyers que no concebien que hi pogués haver un problema de privadesa per digitalitzar el món. Massa gent entusiasta de la tecnologia digital està sota la impressió, tan convenient com equivocada, que si les persones consenten la recol·lecció de dades, i si el processament de dades passa dins del nostre propi telèfon o ordinador, no hi ha cap problema de privadesa.

Primer: no hi ha consentiment informat a la recol·lecció de dades. El consentiment que donem ni és consentiment, perquè no és veritablement voluntari, ni és informat, perquè ningú no té ni idea d'on

poden acabar aquestes dades i quines inferències poden suggerir en el futur. Segon: la creació de dades és moralment problemàtica per si mateixa. Les dades no són fenòmens naturals, com bolets que anem trobant pel bosc. Les dades les creem, i aquest acte de creació comporta una responsabilitat moral i un deure de cura envers els subjectes de dades.

Quin problema de privadesa pot haver-hi si les dades són al telèfon de cada usuari?, em pregunta l'enginyer, assumint que els usuaris tenen control sobre els seus telèfons, i ignorant els molts exemples que mostren el contrari.

En el millor dels casos, els nostres telèfons tenen vida pròpia. Tenen habilitats autònomes, com la capacitat d'enviar dades a tercers sense que ens n'adonem, i la majoria de nosaltres tenen poca idea de com funcionen. A més, tot telèfon connectat a internet és *piratejable*. I què hi ha dels maltractadors que estan aprofitant les tecnologies per controlar les parelles i fills? Si un maltractador et força a compartir la teva contrasenya, aquestes dades que ha creat el teu telèfon sense que tu li ho demanis (on has estat, a qui has trucat, etcètera) poden jugar en contra teva. I què passa quan un agent de duanes et demana a la frontera dels Estats Units que desbloquegis el telèfon? O si t'ho demana la policia? I qui et pot garantir que una asseguradora no et demanarà accés a aquestes dades en el futur? Tan aviat com les dades personals han estat creades i guardades, hi ha un risc de privadesa per al subjecte de les dades.

Per descomptat, demanar a les empreses tecnològiques que no digitalitzin el món és com demanar als constructors que facin el favor de no pavimentar els espais naturals. Llevat que la societat posi límits legals, ningú no en fa cas. Per això, els governs estableixen àrees protegides quan es tracta de construir.

Necessitem àrees protegides similars quan es tracta de la vigilància. És en la naturalesa de les empreses tecnològiques convertir allò analògic en digital. Però convertir-ho tot en un espia potencial, com passa amb la Internet de les coses, és una amenaça per a la llibertat i la democràcia. La vigilància condueix a societats de control, cosa que alhora porta a la disminució de la llibertat. Quan sabem que ens vigilen, ens autocensurem, i quan altres saben massa sobre nosaltres, poden predir, influir i manipular el nostre comportament.

Hi ha algunes dades que és millor no crear. Hi ha dades que és millor no tenir. Hi ha algunes experiències de les quals mai no hauria de quedar registre.

M'agradaria tenir un telèfon que no creés dades sense que l'hi demani, o que les esborrés al cap de poc d'haver-les creat. Vull un telèfon sense reconeixement facial, en què la càmera i els micròfons es puguin desactivar mecànicament, per exemple.

Fa poc més duna dècada, gaudir de la tecnologia digital era un luxe. Cada cop més, el luxe és poder gaudir d'espai i temps lluny de la tecnologia digital. Per això les elits de Silicon Valley crien els seus fills sense pantalles. Cal defensar el món analògic. Si dei-

xem que la realitat virtual proliferi sense límits, la vigilància serà igualment il·limitada. Només rastrejant la teva mirada, les empreses podrien reconèixer la teva identitat, l'etnicitat, les emocions, aspectes de la teva salut mental i física, i més. Si volem mantenir les nostres democràcies i llibertat a l'era digital, més val posar límits a allò que es digitalitza.

La digitalització com a bé universal

Tot progrés comporta uns riscos de què cal alertar i uns grups que queden enrere i no s'han d'oblidar

Cecilio Angulo

No ens cansem de sentir que les dades són el nou petroli del segle xxi. El nou or, si es pretén incidir en el valor que es pot crear a partir de les dades. No obstant això, no servirien de res sense els processos associats d'extracció, neteja, refinat, transformació, distribució, compartició o venda. En tots aquests procediments, la intel·ligència artificial hi fa un paper, no únic, però sí essencial, el la creació de valor a partir de les dades inicials en cru. La digitalització, en conjunt, com a nou sistema de riquesa i d'estil de vida associat a les tecnologies de la informació i la comunicació, suposa un salt enorme, potser un xoc, social i cultural.

Els primers temps de la industrialització, Rockefeller va monopolitzar mitjançant *Standard Oil*,

la indústria petroliera i va portar el concepte de *riquesa personal* a un altre nivell. Henry Ford i la seva cadena de muntatge van crear l'anomenada *classe mitjana* als Estats Units, obrers de baixa i mitjana qualificació que venien la seva força de treball per accedir a la compra de béns de consum. A l'era de la digitalització, els nous magnats actuen de manera semblant. Ja sigui monopolitzant l'extracció de dades, com Google o Facebook mitjançant aplicacions amb alta demanda social, o bé creant nous *blue-collars* a partir d'empreses com Amazon.

Ningú posa en dubte els beneficis que ha comportat, a mitjà i llarg termini, la industrialització per a la humanitat, però no hem d'oblidar que la seva consecució es va fer a costa d'un sacrifici enorme en èpoques primerenques, amb conseqüències mediambientals que encara avui continuem pagant. De la mateixa manera, la digitalització, en conjunt, és una transformació positiva per a la humanitat, però això no ha d'impedir que s'alerti la societat dels perills que comporta. En especial, per als col·lectius més vulnerables, com ara els nens, joves i gent gran.

La universalització de la informació mitjançant internet comporta que joves en zones menys afavorides tinguin accés a continguts educatius que els porten a coneixements, i a opcions de creixement personal i laboral, que d'una altra manera no haurien pogut desenvolupar mai. Mai abans com fins ara joves de l'est mitjà americà tenen accés a universitats de referència americanes (les de la denominada *the*

ivy league). Però aquesta mateixa universalització, per exemple, també permet l'accés lliure a continguts de pornografia que està modificant la conducta sexual dels nostres adolescents cap a formes de relació tòxiques i perjudicials.

O, posem per cas, la tornada a les classes universitàries presencials després de la pandèmia. S'ha evidenciat que l'ús d'eines digitals remotes ha suposat una solució satisfactòria en la transmissió de coneixements, però el comportament social de l'alumnat s'ha vist alterat de manera significativa, a causa del llarg temps d'aïllament i a l'anonimització del seu comportament en remot.

La globalització que comporta la digitalització permet que puguis escoltar la teva emissora de ràdio local en qualsevol part del món, o tenir el despatx allà on t'ho permeti el portàtil o el telèfon mòbil. Deixa, tanmateix, en zona d'exclusió tant persones amb dificultats d'aprenentatge —en especial, persones grans i amb índexs baixos d'alfabetització—, com també àmplies zones territorials sense cobertura de telefonia o dades. Tot plegat amb el beneplàcit de les administracions i els seus poders polítics i mediàtics. Ja vam parlar de la complaença mediàtica en la creació de notícies falses o de la permissivitat administrativa en la conversió digital de serveis bàsics com els bancaris. L'època postpandèmica ha animat que la manera regular de comunicació amb l'administració sigui digital, però no ha facilitat ni ha educat la població sobre aquesta forma d'interacció.

Ens hauríem de poder imaginar el grau d'indefensió d'una persona de més de setanta anys en una àrea rural amb cobertura nul·la havent de gestionar la sol·licitud d'una recepta del mèdica electrònica o simplement lliurant la declaració de la renda. Són els nous immigrants i desplaçats digitals.

Tot progrés comporta uns riscos de què s'ha d'alertar i uns grups que queden enrere, la majoria de vegades sense que sigui per voluntat pròpia, que s'han d'allistar per no oblidar-los i encara menys abandonar-los. El progrés cap a la digitalització no s'ha d'aturar, però sí que ha de ser reflexiu i tenir tothom en consideració. Permeteu-me la llicència, tal com es diria en llenguatge de ciència de dades i intel·ligència artificial: l'algorisme de la digitalització no hauria de compilar en entrades amb valors NaN (*not a number*), tothom hi ha de tenir accés universal.

A més, totes les dades són vàlides, tothom és vàlid, no hi ha *outliers* (valors aïllats) socials que es puguin eliminar com si fossin soroll o un error en el sensor.

L'entrada de la intel·ligència artificial a múltiples facetes de les nostres vides, des del diagnòstic mèdic o l'educació, fins a la seguretat ciutadana o el control epidemiològic planteja seriosos dilemes ètics i morals. Carissa Véliz i Cecilio Angulo han esmolat la ploma per desentranyar, de manera amena i divulgativa, els conflictes que suscita la irrupció de la intel·ligència artificial en els aspectes més recòndits de la nostra quotidianitat.

La tecnoètica ha emergit recentment com a part de l'ètica encarregada de tractar la relació que hi ha entre l'ésser humà i els artefactes tecnològics. Després de definir alguns conceptes bàsics, Angulo i Véliz estableixen un diàleg humanista que despertarà la reflexió, sembrarà el dubte, i no deixarà indiferent el lector. S'abordaran, entre d'altres, els conflictes relacionats amb la privadesa, la digitalització, la vigilància i els riscos que el progrés tecnològic cec pot comportar a la societat. Què hem de fer i com cal actuar davant la irremeiable i ubiqua presència de la intel·ligència artificial?

9 788419 184047

UPCArtsDiàlegs

iniciativa digital politècnica
Publicacions Acadèmiques de la UPC

UPC ARTS