

Deu elements de transformació (i control) de la identitat contemporània

POMPEU CASANOVAS

La Trobe University School of Law, Melbourne
Institut de Dret i Tecnologia, Universitat Autònoma de Barcelona
p.casanovasromeu@latrobe.edu.au
pompeu.casanovas@uab.cat
<https://orcid.org/0000-0002-0980-2371>

Resum: Aquesta contribució versa sobre el control de la identitat digital. Partint de sis exemples recents, mostra la natura canviant del poder i la necessitat de pensar altres formes de regulació i d'intervenció que vagin més enllà de la tradicional estructura normativa dels codis ètics i jurídics. La creació d'ecosistemes regulatius i la construcció del que denominem *mesonivell*, o aproximació teòrica de dins a fora (*middle-out*) a la relació entre humans i màquines, sembla més apropiada per preservar la protecció dels drets i, al mateix temps, garantir la seguretat col·lectiva.

Paraules clau: Internet, control de la identitat, poder a la xarxa, dades i metadades, mesonivell, perspectiva de dins a fora, ecosistemes regulatius.

Ten elements of transformation (and control) of contemporary identity

Abstract: This contribution is about the control of digital identity. Based on six recent examples, it shows the changing nature of power and the need to think about other forms of regulation and intervention that go beyond the traditional normative structure of ethical and legal codes. The creation of regulatory ecosystems and the construction of what we call meso-level, or the theoretical middle-out approach in the relationship between humans and machines, seems more appropriate to preserve the protection of rights and, at the same time, ensure collective security.

Keywords: Internet, identity control, power on the web, data and metadata, meso-level, middle-out approach, regulatory ecosystems.

1/ Introducció

Bon dia a tothom i moltes gràcies per convidar-me a ser avui amb tots vostès. Parlaré en la meua intervenció de la identitat, la identitat digital, la percepció i el control. Sintetitzaré alguns elements del canvi cultural que estem experimentant gairebé sense adonar-nos-en en el món contemporani. I mostraré que els models de regulació (entre ells, els de l'estat i el dret) també estan experimentant canvis i constitueixen avui un element de conflicte.

La identitat és un concepte ambigu, una síntesi d'una munió de processos cognitius, socials i polítics que configuren la forma de percebre, entendre, esquematitzar i transformar la nostra realitat quotidiana. La imatge de nosaltres mateixos que ens va llegar el racionalisme i la Il·lustració en els darrers tres segles (els humans com a éssers reflexius guiats per una racionalitat pràctica) ha implorat en dimensions i nivells diferents: micro, meso i macro. I si això és així, des del cos individual a la coordinació de les accions comunes i la construcció d'institucions, ja no podem assumir les pressuposicions habituals sobre les accions col·lectives que han estat la base de l'ètica i la filosofia política des del Renaixement. Breu, l'impacte de la transformació digital, les tecnologies del llenguatge i la informació, i la intel·ligència artificial està canviant què podem conèixer, què podem esperar i, en definitiva, què i qui som, o pensem que som.

I tanmateix, certa prudència és necessària. La base neurobiològica del nostre cervell no ha canviat. En puritat, és la mateixa que tenien els homes i dones del neolític i dels estats antics. És el coneixement i la cultura el que ha canviat, és la nostra capacitat tecnològica d'intervenció el que ha canviat. I aquesta capacitat s'aplica des dels nivells ínfims abans inabastables (la genètica i la nanotecnologia) a la genòmica de poblacions, la descripció física de l'univers i la generació, organització i gestió dels algorismes de les denominades *big data*. Però no s'aplica en el buit, sinó que es té en compte el que hi havia abans: les condicions socials, l'economia i tota l'estructura de les corporacions i dels estats-nació. Seguim naixent, vivint i morint seguint sistemes de reproducció i convivència que són coneguts. I seguim experimentant el desig, l'amor i l'odi tal com els grecs, els romans i els medievals els sentien també. Però, un altre cop, és la forma d'experimentar-los, la cultura i els seus elements estructurals, el que ha canviat. També la forma de generar-los, percebre'ls i gestionar-los.

Hi ha canvis que són de civilització. Som en un món de contrastos, on la divisió entre les persones i els països molt rics i els molt pobres no ha parat de créixer de forma accelerada des dels anys vuitanta del segle passat. Els fotògrafs de guerra i els fotoperiodistes aixequen testimonis molt feridors de les desigualtats i els conflictes.¹

1. Cf., per exemple, els treballs d'A. Fazzina i V. Rovira: <https://www.noorimages.com/alexandra-fazzina/> ; <https://www.telegraph.co.uk/culture/culturepicturegalleries/7999800/>

Hi ha canvis, altrament, que sí que depenen de la tecnologia i del coneixement aplicat. Però això pot ser objecte d'una, diguem-ne, excessiva atenció. Per exemple, afirmar que «Facebook defineix qui som, Amazon defineix què volem i Google defineix què pensem», com assevera Dyson (2012: 308), conté un element de veritat, però no és tota la veritat. Això afecta les condicions de producció i accés als béns, a la informació i al coneixement, però no esgota les variables que cal definir per entendre la producció d'ecosistemes de regulació i la forma com s'exerceix el poder en el segle XXI. Jo proposo que la visió sigui global i sistèmica: els nous algorismes de regulació certament compten, però també el canvi climàtic, els conflictes irresolts i la distribució desigual de la riquesa.

En aquesta intervenció, esmentaré breument deu elements que em semblen essencials per entendre el canvi cultural i polític profund que s'està produint en relació amb la forma com ens comportem i ens regulem. Són aquests: (i) la identitat digital, (ii) la web de les dades, (iii) l'internet de les coses, (iv) l'eclosió i anàlisi de grans dades, (v) els algorismes de gestió, (vi) els llenguatges semàntics de representació, (vii) l'ús de programes intel·ligents de decisió, (viii) els robots en les societats artificials, (ix) els models de coordinació col·lectiva (sistemes multiagents) i (x) la distribució desigual de la informació. Aquests elements es combinen per alterar, modificar o reconstruir els sistemes que fem servir per autoregular-nos o heteroregular-nos. I fan alguna cosa més: estructuren el mirall dels altres. Com si diguéssim, defineixen l'usuari a partir del que aquest és capaç de fer amb la tecnologia i els altres veuen que fa. I això crea patrons, models de conducta.

2/ Alguns exemples

2.1/ Cambridge Analytica

Posaré sis exemples dels problemes a què ens enfrontem. Cal notar que aquests exemples mostren que el que és tècnicament possible no sempre és socialment desitjable. La tecnologia és (o serà en un futur immediat) a punt. És la seva orientació i especialment la seva implementació el que cal calibrar acuradament. El cas de Cambridge Analytica és el més conegut: la identificació dels perfils dels votants, que rebien informació personalitzada sense haver-ne donat el consentiment. Si una empresa és capaç d'agregar totes les dades en xarxa sobre algú per efectuar-ne el perfil sense el seu consentiment, simplement l'empresa adquireix un poder inusitat no solament sobre les se-

ves dades, sinó sobre la persona mateixa, perquè és capaç de controlar els seus sentiments, desitjos i decisions.

Carole Cadwalladr, la periodista que va revelar les males pràctiques de Cambridge Analytica, ha assenyalat que la manca de control públic de les dades que es recullen i s'analitzen és una amenaça directa per a la democràcia. En una entrevista recent a *The Guardian*, va rebre la següent pregunta: «Què és el que la va dur a mantenir-se ferma en aquesta investigació fins a reunir tots els elements de la història?» Cadwalladr (2018) va donar una resposta directa i senzilla: «Que som impotents i vulnerables, i que continuem essent-ho, i que hi ha una classe de persones molt riques que s'aprofiten de les noves tecnologies per acumular poder i influència per a elles soles».

Les conclusions que treu de la seva investigació, en una *TED Talk* provocadora davant dels executius de Facebook el 19 d'abril d'enguany (2019), representen una acusació directa. Ve a dir: «La democràcia ha desaparegut perquè vostès l'han fet desaparèixer. És això el que volem?». És això el que realment volem?

2.2/ Registre d'identitat dels infractors (sistemes de crèdit d'informació personal)

El segon cas és menys conegut, però no menys real: les targetes d'identitat basades en les violacions de regulacions corporatives o legals que s'agreguen en una mena de carta traçable del nostre compliment, és a dir, el retrat de la nostra conformitat amb les normes. Són similars als carnets per punts dels codis de circulació o a les targetes de crèdit, però diguem que formen un retrat institucional de cada un dels usuaris d'un determinat servei públic. Escoltem l'advertiment que reben els passatgers del tren d'alta velocitat de Beijing a Xangai, enregistrat pel també periodista James O'Malley (2018):

Benvolguts passatgers, els passatgers que viatgin sense bitllet o es comportin de forma desordenada, o fumin en espais públics, seran castigats d'acord amb els reglaments, i el comportament serà enregistrat en un sistema de crèdit d'informació individual. Per evitar un expedient negatiu de crèdit personal, segueixin si us plau les regulacions pertinents i ajudin a complir les ordres en el tren i a l'estació.²

2. <https://twitter.com/i/status/1056811593177227264>. Enregistrat per J. O'Malley el 18 d'octubre del 2018, a les 12.24 h de la tarda. L'anglès original, amb sintaxi xinesa, sense preposicions, és aquest: «Dear passengers, people who travel without a ticket, or behave disorderly, or smoke in public areas, will be punished according to regulations, and the behaviour will be recorded in individual credit information system. To avoid a negative record of personal credit, please follow the relevant regulations and help with the orders on the train and at the station».

Aquest sistema forma part d'un pla del govern xinès per estandarditzar el 2020 un sistema unificat de reputació econòmica i social basat en tècniques d'agregació d'informació a gran escala per a cada ciutadà. És el que es coneix com a sistemes de vigilància massiva (*mass surveillance*) de la població (en pinyin: *shèhuì xìnyòng tíxi*).

L'historiador Yuval Noah Harari ha fet notar que la repressió digital és individualitzada, dirigida a tots i cada un dels grups «monitoritzats», per usar la paraula habitual en tecnologia. L'objecte és un mateix, la persona individual, que constitueix un objectiu granular, relacionat però independent a la pertinença a un grup determinat: «la democràcia en la seva forma actual no pot sobreviure a la fusió d'*infotech* i de *biotech*. O es reinventa amb èxit a si mateixa sota una forma radicalment nova o els humans acabaran vivint en “dictadures digitals”» (Harari 2018: 66).

Sense color, podem afegir, perquè això succeirà en tots els antics règims del segle xx, siguin liberals o comunistes. L'estat de vigilància permanent es pot considerar com un primer símptoma (Zuboff 2019). Vegem-ho.

2.3/ Reconeixement facial

El tercer exemple és de reconeixement facial, al Regne Unit, aquest cop: «El 2017, la Policia Metropolitana de Londres va provar un algorisme de reconeixement facial en un carnestoltes d'un milió de visitants per identificar persones a la seva llista de persones en cerca i captura. La tecnologia va marcar 35 “coincidències”. Els examinadors humans en van descartar 30. La policia va detenir els cinc restants. Només un va resultar ser la persona esperada. Per empitjorar les coses, la policia llavors es va adonar que la llista no era actualitzada i que ja no es buscava aquesta persona per cap delictes» (Margetts, Dorobantu 2019: 164).

També la BBC ha enregistrat evidències de les multes que reben els qui es resisteixen a mostrar el seu rostre als sis milions de càmeres que hi ha a Londres en aquests moments.³ Les condicions ètiques i jurídiques del reconeixement facial (com del biomètric) és un dels temes candents en la filosofia pràctica contemporània. És un tema que no té una solució simple, perquè apunta a l'equilibri entre la llibertat individual i els drets de la privadesa amb els drets a la seguretat col·lectiva.

2.4/ Equifax

Ens hem acostumat que els sistemes informàtics decideixin per nosaltres. Si demanem un crèdit, entrem en una entrevista de feina o pretenem accedir a beneficis públics o privats, podem estar segurs que la decisió serà presa després de creuar totes les dades disponibles per efectuar un perfil del candidat. La

3. Cf. <https://www.youtube.com/watch?v=0oJqJkfTdAg>.

pregunta lògica –Per què jo no he estat escollit?; o, per què no compleixo les condicions?– no té una resposta personal que assumeixi la responsabilitat del judici. Solen dir-nos: «Ah! No podem fer-hi res. El sistema ho ha decidit».

El quart exemple és el cas de violació de dades d'Equifax, als Estats Units.⁴ Les dades personals de 145 milions de persones (la meitat de la població adulta dels EUA) van estar exposades a la llum durant mesos (Berghel 2017). Els pirates informàtics van prendre noms, números de seguretat social, dates de naixement, adreces i informació dels carnets de conduir. Hi havia una vulnerabilitat coneguda al programari de servidor d'Apache Struts anunciada a principis de març de 2017. La companyia va rebre una notificació de la solució disponible el 8 de març. Pel que sembla, Equifax no va aplicar-la fins al cap de tres mesos, quan el seu portal de disputes en línia havia estat ja hackejat. Posteriorment, l'empresa va jubilar el seu director general i d'altres executius, amb una compensació força generosa.⁵

2.5/ Reidentificació de dades

El cinquè exemple és austral. El 2016, a Austràlia, el Departament Federal de Salut va infringir les lleis de privadesa revelant informació personal per a un propòsit diferent pel qual havien estat recollides. Va publicar en línia els registres mèdics identificats de 2,5 milions de persones (el 10% de la població australiana) per a «propòsits de recerca». Culnane, Rubinstein i Teague (2018), investigadors de la Universitat de Melbourne, van ser capaços de reidentificar-los en qüestió d'hores. Tal com ells mateixos expliquen: «Vam ser capaços de desxifrar els números d'identificadors del proveïdor de serveis a la mostra del 10% de l'agenda de beneficiaris de Medicare (MBS) publicada recentment al lloc web data.gov.au del Govern Federal».

No els va caler desxifrar els números d'identificació del pacient per fer-ho. El Departament de Salut va ser notificat el 12 de setembre de 2016 sobre el problema i va retirar immediatament el conjunt de dades del lloc web.

2.6/ Ciberseguretat

El sisè exemple també és austral i ha passat just quan estic escrivint aquestes línies (4 de juny 2019):

Em sap molt de greu haver d'informar-vos que hem estat víctimes d'una violació de dades que ha afectat les dades personals de la nostra comunitat. A finals de 2018, un hacker va accedir als nostres sistemes de forma il·legal.

4. Aquest escàndol va arribar a tots els mitjans; cf. SBS: <https://www.youtube.com/watch?v=X2mbhfrdBhg>.
5. El conseller delegat (CEO) va cobrar uns 90 milions de dòlars i altres tres executius d'Equifax van poder vendre 1,8 milions de dòlars en accions just abans del reconeixement públic per part de l'empresa de la violació de dades que s'havia produït (Berghel 2017: 72).

Hem detectat l'incompliment fa dues setmanes. Durant les últimes dues setmanes, el nostre personal ha estat treballant incansablement per enfortir encara més els nostres sistemes contra atacs secundaris o oportunistes. Puc donar ara els detalls de què va passar. Creiem que hi ha hagut un accés no autoritzat a quantitats significatives de dades del personal, dades d'estudiants i de visitants durant els darrers 19 anys.

És la carta del rector de l'Australian National University (ANU), la universitat més important del país, en què es disculpa per aquesta fallada de seguretat que podria haver afectat 200.000 persones, segons *The Guardian* (4 de juny 2019) durant els darrers 19 anys. Si es té en compte que els indicis assenyalen la Xina (sembla comprovat), ja tenim dibuixat un escenari de conflicte d'espionatge industrial, econòmic i polític amb conseqüències en l'escenari internacional.

3/ El poder, un altre cop

Tots els casos anteriors són diferents i responen a dinàmiques d'ús de les dades amb constriccions distintes. Tots són cridaners, però, i tenen un element en comú: *mostren la feblesa dels instruments tradicionals del dret, de la política i de la democràcia participativa clàssica per fer front a aquestes situacions*. Hem de comptar amb la manca, diguem-ne, de disponibilitat democràtica no ja dels *brokers* de Wall Street sinó dels emprenedors de Silicon Valley. Aquest mes d'abril la revista *Wired* els comparava amb el futuristes italians d'entreguerres: enamorats de la innovació tecnològica i completament aliens als seus efectes negatius, és a dir, a l'avantsala del feixisme.

«Amazon ha estat proporcionant programes de reconeixement facial a la policia nord-americana. Hewlett Packard Enterprise, Thomson Reuters, Microsoft i Motorola Solutions tenen contractes amb Immigration and Customs Enforcement ICE i estan aprofitant l'actual onada de deportacions i camps d'internament. Els científics i les empreses tecnològiques nord-americanes estan ajudant la Xina a fer un seguiment dels grups minoritaris. La Xina també espera que Google l'ajudi a suprimir qualsevol tipus d'informació sobre el tractament d'aquests grups minoritaris» (Eveleth 2019).

Es tracta també de la redefinició del tema del segle xx de la societat de masses (*the crowd*). Però del que estem parlant, primer de tot, és de la natura canviant del poder que la mou. Jeremy Heimans i Henry Timms han escrit un llibre sobre això, titulat precisament *New Power* (2018). Heimans és un activista digital, l'emprenedor que el 2005 va fundar la plataforma *GetUp*, que a Austràlia ha encapçalat i conduït força campanyes en pro de la ciutadania, contra la corrupció, contra el tracte que reben els aborígens, contra els abusos sexuals a nens. La gent només ha d'aixecar el dit amb un clic. És molt fàcil sumar-s'hi. L'èxit de la plataforma ha inspirat el llibre. Quina és la raó de l'èxit?

Heimans i Timms proposen redefinir l'exercici del nou poder en relació amb el vell. Han elaborat el que denominen *new power compass*, la brúixola del nou poder: flexible, connectat, inexigent, inarticulat, informal, traient profit de la manera com la gent es connecta, participa, comparteix, empatitza amb idees i sentiments, i fuig quan sent massa constriccions, se li imposen deures o senzillament sent que no li agrada el que veu a la pantalla del mòbil, la tauleta o l'ordinador. Els autors classifiquen el comportament i la comunicació de les organitzacions (ja siguin empreses, partits o estats) segons aquest model. Diuen que és com l'aigua o l'energia: s'ha de canalitzar i deixar-lo fluir. En canvi, el vell poder és autoritari, repressor, manaire, impositiu, burocràtic, i exigeix obediència. No serveix per triomfar a la xarxa.

La brúixola del nou poder l'organitza en dos eixos –models i valors– i quatre quadrants. La massa *crowd* és un nou model de poder amb nous valors (per exemple, Obama en campanya). El líder estimulador o animador (*cheerleader*) professa nous valors però està encara enganxat a les formes del vell poder (per exemple, *The Guardian*). Un castell (*castle*) és com un búnquer: tancat en banda a tota innovació de comportament (Apple o l'Enciclopèdia Britànica). Un cooptador o connector (*co-opter, connector*) representa un nou model de poder, però aplicat a vells valors (Uber o Facebook).

Tampoc els cal citar els filòsofs. Ni Habermas, ni Foucault, ni Derrida hi són, ni se'ls espera. Formen part de la reflexió del passat, del vell poder. Els autors, en canvi, ordenen simplement la seva experiència per compartir-la. Parlen d'ells mateixos, de què han fet i què volen fer. Els interessa «com funciona el poder en el nostre món hiperconnectat i com fer que treballi per a tu», com diuen en el subtítol. La proposta és força instrumental i no es correspon amb divisions morals. El *Tea Party* o Trump poden estar al quadrant superior. El seu èxit ha estat saber construir discs, canals i ponts per a les masses, que han fet també Trump a la seva imatge, com elles volien.

Penso que els autors ofereixen una visió que és al mateix temps intuïtiva i certa en relació amb els fenòmens col·lectius en xarxa, però potser no tan acurada respecte a la xarxa i el teixit social. Trump no va ser escollit per haver-se dirigit als seus votants de forma personal, sinó perquè els va *identificar* i *perfilar* primer amb informació obtinguda de forma reprovable. És a dir, els va re-crear des de fora, com va voler, des del poder tradicional de les elits acostumades a configurar el marc de la regulació i a decidir què hi va a dins.

Heimans i Timms passen també per alt el fet que la majoria de la població mundial no és a la xarxa. Hi ha gent que mana i gent que obeeix. I els qui manen cada cop se separen més de la resta. Aquest és el segon tret dels exemples que hem posat abans: alimenten en nosaltres la idea que l'escàndol, les violacions de drets, es poden evitar i regular intensificant els controls ètics i jurídics tradicionals. I això és un *trompe l'oeil*, una il·lusió. L'experiència de les plataformes digitals i d'activistes com Heimans té sentit, però només si

s'accepta que els instruments generals del dret i la política tal com els hem conegut fins ara no seran iguals després de la revolució digital.

El que cal canviar no és el contingut de les regulacions, sinó la seva forma, el concepte mateix de regulació. El que és nou són els efectes de la coexistència d'una pluralitat de formes de poder lligades a la tecnologia que busquen, com sempre, l'optimització econòmica i política del seu benefici. Comparteix la visió de Nigel Shadbolt i Roger Hampson a *The Digital Ape* (2018). L'espècie avança conformant relacions socials que són alguna cosa més que tecnologia i, malauradament, «el problema no és que les màquines hagin pogut prendre el control a les elits. El problema és que la majoria de nosaltres mai no puguem prendre el control de les màquines a la gent que mana» (Shadbolt, Hampson 2018: 63).

Penso que, de fet, el que ha canviat és (i) la composició de les elits, (ii) la composició dels estats, (iii) el poder incremental de les corporacions i dels seus òrgans de govern, (l'osmosi entre el govern o administració digital i els models tradicionals de governança de les corporacions, COSO, COBIT i TOGAF, per exemple),⁶ i (iv) la traducció tècnica dels vells models del dret i de l'estat.⁷ I aquest és un procés que va començar als anys vuitanta i noranta, ben abans de la creació d'internet, del web semàntic i de l'internet de les coses.

Però ara els estats han començat a actuar com les corporacions: es defensen i tendeixen a acaparar els mitjans digitals en benefici propi. No ens cal acudir a exemples d'estats d'arrel totalitària com la Xina o la Rússia de Putin. A França l'article 33 de la nova Llei de Reforma de la Justícia⁸ acaba de prohibir l'estudi de les sentències judicials completes amb els noms dels magistrats que les emeten amb instruments digitals avançats, en nom de la privacitat i la protecció de dades (*protection de la vie privée*).⁹ Això és clàssic:

6. Committee of Sponsoring Organizations of the Treadway Commission (COSO), i Control Objectives for Information and Related Technologies (COSO), constitueixen models corporatius de regulació basats en estàndards, principis i bones pràctiques professionals. The Open Group Architecture Framework (TOGAF) és un model que proporciona una arquitectura corporativa pel disseny, implementació i governança de la tecnologia de la informació.
7. Vaig tenir ocasió d'analitzar aquests models normatius a Casanovas 2017.
8. *LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*. Cf. *Artificial Lawyer* (2019).
9. «Les données d'identité des magistrats et des membres du greffe ne peuvent faire l'objet d'une réutilisation ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées. La violation de cette interdiction est punie des peines prévues aux articles 226-18, 226-24 et 226-31 du code pénal, sans préjudice des mesures et sanctions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés». https://www.legifrance.gouv.fr/eli/loi/2019/3/23/2019-222/jo/article_33; ELI: https://www.legifrance.gouv.fr/eli/loi/2019/3/23/JUST1806695L/jo/article_33; Alias: https://www.legifrance.gouv.fr/eli/loi/2019/3/23/2019-222/jo/article_33

l'opacitat, la dificultat de l'accés a les dades pertinents. Sempre ha estat difícil per als investigadors accedir a dades internes, per exemple, de mediació o de jurats. El que és nou és la claredat amb què l'estat es protegeix d'aquells mateixos que l'haurien d'avaluar, això és, els ciutadans. Això vol dir que una construcció més limitada de l'espai públic acompanyarà a partir d'ara el desenvolupament de l'espai universal que és internet. La vida privada dels servidors públics ha estat posada per davant de la transparència amb què han de signar les sentències.

Observem la nova manera de publicar la llei: mitjançant un identificador singular universal, anomenat ELI, *European Legislation Identifier*. Quan parlem d'identitat parlem de la identificació de les entitats digitals, és a dir, de la *representació de la identitat en algorismes i llenguatges semàntics*. És igual, a aquests efectes, si es tracta de persones, organitzacions o objectes. La ISO/IEC 24760-1 defineix la identitat com «un conjunt d'atributs relacionats amb una entitat», a *set of attributes related to an entity*.

La identitat és un punt essencial. Hi ha un famós acudit de Peter Steiner a *The New Yorker* que s'hi refereix: *A internet, ningú sap que ets un gos* (Juliol 5, 1993). L'Institut Nacional d'Estàndards i Tecnologia del departament nord-americà de Comerç també ho ha deixat clar: La identitat digital és la representació única d'un subjecte actuant en una transacció en línia. Una identitat digital és sempre única en el context d'un servei digital, però això no significa necessàriament que identifiqui el subjecte en tots els contextos de forma única. En altres paraules, accedir a un servei digital no significa que es conegui la identitat del subjecte en la vida real.¹⁰

El que voldria assenyalar és que les noves formes de poder impliquen el domini d'aquests llenguatges de representació i de les tècniques d'autenticació, encriptació i privadesa, perquè són ells els que estructuren la possible relació entre les entitats digitals i les reals. És a dir, gestionen la referència i coreferència dels mots i discursos que fins ara fluïen només a través de les llengües naturals.

Per dir-ho de forma simple: qui domina la relació entre dades i metadades dels elements d'un sistema és capaç de construir el seu poder d'implementació, és a dir, l'abast de l'ecosistema de la seva utilització. I aquesta és una relació asimètrica: els ciutadans, consumidors, usuaris, poden ser totalment identificats i els escenaris i contextos perfilats, però ells no poden accedir al coneixement general que el sistema i els administradors del sistema posseeixen.

10. «Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known» (Grassi et al. 2017).

4/ Ecosistemes ètics i jurídics, més que no pas models normatius

Aquesta és la raó que no puguem usar només sistemes de valors, principis o normes per regular aquest híbrid complex que formem amb les nostres dades i metadades. És igual si es tracta de sistemes ètics o jurídics. Hi ha: (i) aquest element intermedi dels llenguatges semiformals i formals que no podem obviar (si és que volem evitar o pal·liar si més no casos com els que hem descrit abans); (ii) el terreny intermedi de la construcció de l'espai públic i la coordinació col·lectiva de conductes a partir de les decisions i accions individuals.

L'ètica en intel·ligència artificial (IA) és un dels punts nous identificats per Gartner (2019) com a essencials en els propers cinc anys en el seu popular *hype cycle* o cicle d'expectatives tecnològiques per al desenvolupament industrial. Per primer cop l'ètica i la governança compten com a elements reguladors. Però com? Com incorporar principis ètics i proteccions jurídiques dins de sistemes de conducta (artificial i humana)?

L'estratègia tradicional duta a terme per fer-ho és elaborar una sèrie de principis generals, que poden ser desenvolupats a través de sistemes regulatius, això és, sistemes de normes que permetin el seu compliment. Entre molts altres exemples, Europa i Austràlia estan elaborant una sèrie de principis ètics per ser aplicats a la legislació d'IA.

No poso en dubte que la formulació de principis d'honestat o justícia (*fairness*), rendició de comptes o responsabilitat (*accountability*) i transparència (*transparency*) hagi de ser aclarida. Només assenyalo que la seva aplicació requereix alguna cosa més, perquè és la natura social i política d'aquests principis el que s'ha de concretar, i això només es pot fer des del nivell de les interrelacions i interfícies entre els éssers humans i les màquines.

El que hem denominat *mesonivell* (Poblet, Casanovas, Rodríguez-Doncel 2019) i *middle-out approach* (Pagallo, Casanovas, Madelin 2019) es refereix al conjunt de mitjans tècnics i humans que hem de posar en obra per construir una comunitat, un sistema sociotècnic o un grup humà que utilitzi tecnologia. També em sembla que és en allò que hauríem de centrar-nos si és que volem posar una mica d'ordre en l'aplicació de la intel·ligència artificial als sistemes regulatius ja existents.

La construcció d'ecosistemes no es pot donar per descomptada. Els juristes i filòsofs polítics dels segles XVIII, XIX i XX es van acostumar a lligar el concepte d'*autoritat* a l'estat o als representants del govern escollit pels ciutadans (Parlament). De fet, l'autoritat pot relacionar-se amb el mercat o amb la societat en el seu conjunt també. La idea que ens pot guiar és la de trobar un equilibri entre totes aquestes fonts d'autoritat, incloent-hi allò que l'individu pot decidir sobre si mateix (i això darrer és essencial). Per molt que es limiti, la capacitat d'autonomia dels sistemes d'agents i la dels individus s'incrementa a mesura que les seves capacitats i el seu poder cognitiu i operatiu creixen. Els científics cognitius solen parlar d'*affordances*, la capacitat dels objectes

de moure a certs tipus d'accions segons hagin estat dissenyats, en un entorn determinat. L'enriquiment d'aquest entorn és exponencial ara.

En un món hiperconnectat, els objectes fan de canal de transmissió de la informació. Cada un dels objectes quotidians que ens envolten transmetran en un futur gens llunyà informació sobre els seus usuaris: cotxes, neveres o torradors del pa. Com ens enfrontarem a això i al món de la nanotecnologia (microprocessadors) que els acompanyarà? Literalment, no ho podem saber ara.

Els límits han de venir no de restriccions sinó de les decisions conscients sobre com integrar-se en els diversos escenaris i contextos socials. Un altre cop la identitat: preservar-la s'ha convertit en una prioritat. I això significa poder definir (fins al punt on sigui possible) les relacions entre les entitats, els atributs i els valors dels atributs que configuren la nostra identitat digital i personal. No és senzill, perquè els múltiples punts de suport amb les xarxes personals i socials ja formen un *continuum* del qual és difícil desfer-se. La idea seria integrar tots aquests escenaris de forma controlable per a tots i cada un dels individus que els experimenten. Això és: trobar punts policèntrics per a la pluralitat d'ecosistemes que formaran la nostra vida i consensuar els ecosistemes de regulació.

5/ Democràcia enllaçada: un model de democràcia possible

És el que he denominat *meta-rule of law*. No té traducció al català, perquè la nostra cultura jurídica és continental, de dret civil i administratiu francès, i per tant traduir *metaestat de dret* no és acurat. Jo he fet servir aquesta expressió a contracor. Seria millor denominar-la *estructura ètica* o *metaestat de drets*, perquè es tracta de centrar-se en els drets, és a dir, en les expectatives de conducta que els nostres interlocutors, veïns i contraprestadors tenen de nosaltres i nosaltres d'ells (Casanovas 2017). Hi ha un mínim de protecció possible, que defineix l'àmbit d'allò que els sistemes regulatius abasten.

L'objectiu és estendre i encabir en l'estructura del web de les dades (dades/metadades i serveis web) les proteccions i garanties dels drets per mitjà d'instruments semàntics i els algorismes d'IA que puguem aplicar-hi (aprenentatge automàtic, *machine learning*, privadesa, etc.). Fixem-nos que els drets i obligacions no són creats pels llenguatges formals, sinó per les interrelacions (individuals i col·lectives) entre els membres de comunitats socials, els mercats i la societat civil. La cadena de transmissió s'inicia amb els identificadors. Operen en la interfície entre humans i màquines que hem definit recentment com la dimensió de governança jurídica de la intel·ligència artificial (Pagallo, Casanovas, Madelin 2019).

Definim mínimament els termes: (1) La web de les dades està formada per qualsevol dada disponible, en brut, semiestructurada o estructurada en un llenguatge formal, via API o fluxos d'informació de l'internet de les coses.

(II) *linked data*, dades enllaçades o vinculades, és un subconjunt del primer per publicar i compartir dades en xarxa, seguint les regles clàssiques proposades per Tim Berners-Lee i desenvolupades per la comunitat tecnològica del W3C (World Wide Web). La web de les dades no hauria de confondre's amb internet. La primera és semàntica, composta per fluxos d'informació que s'han de regular. El segon és el seu suport físic, un conjunt de tecnologies de la comunicació.

La democràcia deliberativa es defineix des dels anys noranta com «un conjunt de processos d'avaluació, i de formació i transformació de preferències a través d'un diàleg informat, respectuós i competent» (Dryzek, Niemeyer 2009). No vol limitar-se, doncs, al procés formal del vot. La democràcia epistèmica segueix aquest camí, i ha estat defensada per autors com Jeremy Waldron o Josiah Ober. Assumeix que existeix un procés de decisió col·lectiva que pot produir resultats epistèmicament vàlids (vertaders) o decisions raonables, fonamentades o adequades en major mesura a partir de la participació d'un major nombre de persones. Els processos polítics de *crowdfunding* i *crowdsourcing* es basen en aquest pressupòsit, i també els mètodes d'assemblees populars (mini-públics). La democràcia enllaçada: (I) estableix i estudia les condicions contextuais de la democràcia deliberativa i epistèmica, (II) se situa en el mesonivell intermedi d'implementació tal com l'hem definit, (III) requereix la interfície d'humans i màquines i (IV) adreça el nivell institucional que el pot regular i donar forma.

El que estem proposant és anar una mica més enllà dels conceptes de *democràcia deliberativa* o de *democràcia epistèmica*. *Linked democracy*, democràcia enllaçada, és el concepte amb què ens referim a la interrelació entre un grup de gent, la tecnologia i les dades per tal de crear ecosistemes de participació on el coneixement és agregat, compartit i alineat per prendre decisions i crear línies d'actuació política i social (Poblet, Casanovas, Rodríguez-Doncel 2019). Els ecosistemes democràtics són contextuais, referits als sistemes d'interacció (mesonivell) en xarxa. I poden interrelacionar-se al seu torn per produir coneixement i decisions polítiques socialment rellevants. Aquesta concepció és similar a la de la democràcia epistèmica, però està més basada en innovacions socials que poden dur a una participació centrada en l'ús compartit de les tecnologies per resoldre problemes comuns. La preservació dels drets dels individus en aquest procés és el que denominem *estat de drets*.

Agraïments

Aquest article exposa alguns dels resultats de *Meta-Rule of Law* (DER2016-78108-P). I, parcialment, *Compliance through Design*, Data to Decisions Cooperative Research Centre (D2D CRC, Australia); *Meta-Rule of Law* (DER2016-78108-P), i EU Project LYNX. *Building the Legal Knowledge Graph for Smart Compliance Services in Multilingual Europe* (Grant agreement No 780602).

Bibliografia

- Artificial Lawyer*. «France Bans Judge Analytics, 5 Years in Prison for Rule Breakers», 4 de juny 2019. [<https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison-for-rule-breakers>]
- Australian University. «Message from the Vice-Chancellor». 19 de juny 2019. [<https://www.anu.edu.au/news/all-news/message-from-the-vice-chancellor>]
- BERGHEL, H. (2017) «Equifax and the latest round of identity theft roulette». *Computer* 50/12: 72-76.
- CADWALLADR, C. (2018) «Exposing Cambridge Analytica: “It’s been exhausting, exhilarating, and slightly terrifying”». *The Guardian* 28 de setembre. [<https://www.theguardian.com/membership/2018/sep/29/cambridge-analytica-cadwalladr-observer-facebook-zuckerberg-wylie>]
- CADWALLADR, C. (2019) «Facebook’s role in Brexit, and the threat to democracy». *Ted Talk* 19 d’abril. [https://www.ted.com/talks/carole_cadwalladr_facebook_role_in_brexit_and_the_threat_to_democracy?language=en]
- CASANOVAS, P. (2017) *Sub lege pugnamus. De la gran guerra a les grans dades*. Barcelona: Publicacions de la Universitat de Barcelona.
- CULNANE, C.; RUBINSTEIN B.; TEAGUE, V. (2018) «Understanding the maths is crucial for protecting privacy». Melbourne: University of Melbourne. [<https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy>]
- DRYZEK, J. S.; NIEMEYER, N. (2019) «Deliberative Turns», dins J. Dryzek (ed.), *Foundations and Frontiers of Deliberative Governance*. Oxford: Oxford Scholarship Online, 3-17.
- DYSON, G. (2012) *Turing’s Cathedral: The Origins of the Digital Universe*. New York, NY: Pantheon Books.
- EVELETH, R. (2019) «Ideas. When Futurism let to Fascism –and why it could happen again». *Wired*, 18 d’abril. [<https://www.wired.com/story/italy-futurist-movement-techno-utopians>]
- GARTNER (2019) «Hype Cycle for Artificial Intelligence 2019». 25 de juliol. ID: G00369840.
- GRASSI, P. A.; GARCIA, M. E.; FENTON, J. L (2017) *Digital Identity Guidelines*. NIST Special Publication 800-63-3. [<https://doi.org/10.6028/NIST.SP.800-63-3>]
- HARARI, Y. N. (2018) *21 Lessons for the 21st Century*. Londres: Jonathan Cape.
- MARGETTS, H.; DOROBANTU, C. (2019) «Rethink government with AI». *Nature* 568: 163-165.
- O’NEIL, C. (2016) *Weapons of math destruction: how big data increases inequality and threatens democracy* (First edit). Nova York: Crown.
- PACK, J. (2018) «How does China’s social credit system work?» *Market Place*, 13 de febrer. [<https://www.marketplace.org/2018/02/13/world/qa-china-s-social-credit-system>]
- POBLET, M.; CASANOVAS, P.; RODRÍGUEZ-DONCEL, V. (2019) *Linked Democracy. Foundations, methodologies, applications*. Cham: Springer Nature. [<https://www.springer.com/gp/book/9783030133627>]
- PAGALLO, U.; CASANOVAS, P.; MADELIN, R. (2019) «The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data». *The Theory and Practice of Legislation* 7/1: 1-25. [<https://www.tandfonline.com/doi/full/10.1080/20508840.2019.1664543>]

- SHADBOLT, N.; HAMPSON, R. (2018) *The Digital Ape: How to Live (in Peace) with Smart Machines*. Sydney: Pan Macmillan.
- The Guardian* (2019) «Australian National University hit by huge data breach», 4 de juny. [<https://www.anu.edu.au/news/all-news/message-from-the-vice-chancellor>]
- ZUBOFF, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.