Tema 9. TIC, societat, professió i ètica: una confluència necessària

Has de saltar sempre pel precipici i construir les ales en el camí de descens.

Ray Bradbury

Una vegada assentades les bases de l'ètica i deontologia informàtica anem un pas més lluny: la nostra societat, on vivim tots, canvia. I nosaltres no som aliens a aquests canvis, que patim per acció o omissió. Parlarem del fenomen hacker *i particularitzarem en el que s'ha anomenat* hacking ètic *i en fenomenologies amb una incidència cada vegada superior, com ara l'anomenada* ciberguerra *o les actuacions basades en l'enginyeria social. Després d'això, visitarem com raja fenòmens tan presents com són la intel·ligència artificial, la robòtica, la Internet de les Coses o el* Big Data *o dades massives i posarem l'accent en el nostre treball, tot això sense deixar de particularitzar les referències que ja vam veure sobre els codis ètics.*

Introducció

Hi ha unes quantes figures que brillen amb llum pròpia en el que s'ha anomenat el submón/submón informàtic. Una d'aquestes és la cada vegada més mediàtica de Kevin Mitnick. Doncs bé, una frase recollida en un dels seus llibres és la que sembla donar la clau del que a continuació tractarem de desenvolupar. Diu Mitnick que "des del meu punt de vista, al col·legi haurien d'ensenyar els infants els principis de l'ètica informàtica des de l'escola primària, quan s'inicien en l'ús d'ordinadors" (Mitnick & Simon, 2007).

Efectivament, l'ordinador ja no és tan sols un electrodomèstic més, és un estri que forma part de l'ADN de qualsevol societat d'avui, i no solament un utensili accessori, sinó un element central. I ja que a tots ens demanen que ens comportem i mantinguem unes bones formes, i fins i tot per a usar eines perilloses (com pot ser un cotxe), ens certifiquem per a poder usar-lo (seguint l'exemple, el permís de conduir), sembla lògic esperar que, des d'infants, siguem instruïts en les "bones formes".

Un dels problemes principals és on fixar el punt de vista ètic: aquests valors que se suposa que hem de compartir. Podem pensar que en l'ús comú, en el que és habitual, encara que a vegades és una cosa desencertada. Se sap que la interacció en línia precisament referma conductes no desitjables. Així, un pederasta que no tinga comunicació amb uns altres de la seua classe pot veure, finalment, que la seua actitud és reprovable. Però si té la retroalimentació positiva d'un grup de persones com ell, el grup pot fer-li sentir més fort i pensar que no és tan dolent això que fa. Aquesta motivació que apareix sempre no és dolenta: quan l'objectiu és bo, col·laborar a realitzar determinades pràctiques dona l'oportunitat de secundar accions considerades positives i el compromís. Dudley ací fica un tascó en plantejar que podem pensar que la participació en les activitats d'Al-Qaida, en línia o en la vida real, té poc de virtuós i, tanmateix, l'efecte aconseguit per la col·laboració en línia d'aquests terroristes o aprenents de terroristes és que es refermen els uns als altres que aquesta idea comuna és positiva (Dudley, Bramen, & Vincenti, 2012).

D'altra banda, atesa la figura del *hacker* (terme que per la claredat i la seua popularització emprarem sense cometes), és sabut que no tots són el que podríem catalogar com germanetes de la caritat. D'exemples, n'hi ha molts, però el més típic és el que ens dona Libicki: Els hackers també poden entrar en els sistemes empresarials i fer-se passar per usuaris legítims amb els drets i privilegis de qualsevol altre usuari (Libicki, 2009). D'altra banda, veurem en aquest mateix tema que el seu ús com a personal d'alta qualificació forma part ja del dia a dia dels estats moderns. Parlarem sobre com apareixen guerres de baixa intensitat, a partir de confrontacions polítiques entre estats o grups, amb un perfil d'hostilitat inferior a la guerra convencional, però que alhora supera la convivència pacífica entre nacions.

Les TIC afecten tota l'òrbita de l'ésser humà: família, oci o treball. Aquesta sociabilitat digital que influeix en la professionalitat de l'individu no és la menys important: la presència d'amics en el seu entorn de treball sol implicar que una persona treballe més o menys intensament que en cas d'estar sola; bé per no semblar un setciències, posa el fre, i així de pas evita que li consulten de continu, o, si és algú una miqueta lent, o directament gandul, pot intensificar-ne el quefer per a així evitar semblar un peresós. En qualsevol cas, les relacions humanes, que és el llibre sobre el qual s'escriu l'ètica, afecten la seua capacitat de treball. Sembla exagerat? Pensem que la manipulació sobre la base dels exemples externs i les influències que de fora venen, és el nostre pa de cada dia. Això es veu de forma gràfica amb un exemple: pensem en el món de l'espectacle, on cada any el nivell del que és acceptable o moral sembla canviar, en què ens venen el canvi com "llibertat". Aquests canvis procedeixen del que "el públic", aquesta massa anònima, aplaudeix amb les seues audiències o deixa de fer. Finalment l'individu, part de la massa, és manipulat per la massa en si mateixa, i acaba canviant-ne en molts casos els criteris (Hadnagy, 2011).

I, per descomptat, ens queda alguna cosa que sembla que és nova, però que no ho és tant: la intel·ligència artificial (IA), i la robòtica. Si preguntem si volem tenir un robot, la majoria diríem que sí, i es tracta d'una majoria que en realitat no sap que ja en té, fins i tot no diria ningú que ell mateix podria arribar a ser un robot per hibridació en el futur. Si preguntem si ens agradaria ser transportats en taxi sense conductor o compartir els nostres treballs amb un robot, probablement la majoria dirà que no si s'ho pensa una miqueta. Hi ha un rerefons ètic, però també jurídic. (Barrio Andrés, 2018). Això ens portarà a considerar la intersecció de les TIC amb els valors humans[1].

És un fet evident que les societats actuals han entrat en una dinàmica de canvi constant, cosa que, al seu torn, implica, com ens recorda (Colmenarejo Fernández, 2017) la necessitat urgent de desenvolupar una ètica adaptada als canvis que provoquen els avanços tecnològics sobre la qualitat i les formes de vida. I és que hi ha anys llum entre saber jugar als escacs i sentir el cor en un puny en escoltar una òpera de Verdi (Latorre Sentís, 2019). Però, i si parlem de

[1] : Els elements a considerar segons (Bynum & Rogerson, 2004) són:
1. Relacions humanes
2. Privacitat i anonimat
3. Propietat intel·lectual
4. Treball
5. Justícia social
6. Govern i democràcia

compondre-ho? Recordem sistemes com ara DeepBach[2]. Potser no estem tan lluny del futur com creiem, sinó ja dins d'aquest. I és que..., pensar el futur és el primer pas per a habitar-lo. (Latorre Sentís, 2019)

Un poc d'història

No podem deixar de donar unes pinzellades sobre les fites històriques en l'ètica de la informàtica. Hi seguim (Bynum & Rogerson, 2004) i ho exposem per a més simplicitat de forma lineal.

- 1940 a 1950. Norbert Wiener i la seua obra, en particular *The human use of Human Beings*.
- 1960. Donn Parker va examinar els usos il·legals i poc ètics dels professionals de la informàtica, se'l considera després de Norbert Wiener el segon pare de l'ètica informàtica.
- 1970. Joseph Weizenbaun crea ELIZA, programa informàtic dissenyat al MIT, va ser un dels primers programes a processar llenguatge natural. Va escriure *Computer Power and Human Reason* (1976) i es considera una persona clau en l'ètica informàtica. El terme *Computer ethics* el crea a meitat dels anys setanta Walter Maner i el defineix com el camp aplicat en les ètiques on els problemes poden ser agreujats, transformats o creats per la tecnologia dels ordinadors.
- 1980 a 1990. James Moore va publicar el seu article "What is computer ethics?" el 1985. També cal considerar l'obra de Sherry Turkle el 1984, *The Second Self*.

Definicions

Apuntarem una sèrie de termes que ens seran necessaris per al desenvolupament del tema actual. Comencem amb el més bàsic: l'ètica informàtica. Per a això ens farem ressò de l'evolució històrica del concepte, seguint l'estudi de (Bynum & Rogerson, 2004). S'emmarquen cinc etapes, que es poden veure en la taula següent.

---

[2] Vaig fer un experiment emprant composicions "a l'estil de" Vivaldi, Beethoven i Bach. Generades per una IA i, posades a prova amb humans, no advertits de l'origen, els dubtes es decanten entre si són peces poc conegudes dels compositors o de coetanis.

No fa molt se xifrava el vertader salt de la IA no a aconseguir màquines que venceren intel·lectualment els humans, fet que ja ha succeït fa temps, o que aconseguiren substituir-los en tasques intel·lectualment complexes (p. e. com a radiòlegs en hospitals, cosa que ja ha succeït també), sinó en el sentir, com diu Latorre, el cor en un puny en escoltar Verdi.

I pot ser que siga un error, ja que tots coneixem que una part important de la nostra societat que no s'emociona ni davant Verdi, ni davant Velázquez, ni davant absolutament res, siga la mort d'un xiquet, una tragèdia al Nepal o la mort de sa mare. Després d'aquest camí que hem recorregut com a societat, on els nostres dirigents no han sigut precisament innocents, crec que sí, d'ací a poc, la IA ens superarà. I em permet postil·lar: i a qui li importa? Algunes adreces que il·lustren això (no referenciades a manera de bibliografia, sinó com a exemple):

https://www.youtube.com/watch?v=cgg1hipaayu
https://www.youtube.com/watch?v=o7ztlw7s2dc
https://www.youtube.com/watch?v=2kuy3brmtfq
https://www.youtube.com/watch?v=qibm7-5ha6o

Taula 1. Evolució del concepte "ètica informàtica", segons Bynum & Rogers.

1	Maner va ser el primer a usar el terme de *computer ethics* a mitjan dècada de 1970 com a "problemes ètics agreujats, transformats o creats per la tecnologia informàtica".
2	En el seu llibre *Computer Ethics* (1985), Deborah Johnson el va definir com "estudi de noves actituds morals davant problemes i dilemes. Increment d'antics problemes i obligació de crear de forma ordinària normes morals inexplorades".
3	En el seu article "Què és l'ètica informàtica?" (1985), James Moor va proporcionar una definició d'ètica informàtica que és molt més àmplia i més extensa que les de Maner o Johnson. És independent de qualsevol teoria filosòfica específica i és compatible amb una extensa varietat d'enfocaments per a la resolució ètica de problemes. Des de 1985, la definició de Moor ha sigut la més influent. Va definir l'ètica informàtica com un camp relacionat amb "buits de polítiques" i "confusions conceptuals" respecte a l'ús ètic i social de la tecnologia de la informació. Un problema ètic sorgiria per no haver-hi polítiques sobre com cal usar un ordinador. Ens donen noves capacitats i això ens força a fer determinats girs a les accions que ja teníem consolidades. Juntament amb un buit de polítiques, sovint hi ha un buit conceptual.
4	El 1989, Terrell Ward Bynum, seguint un suggeriment de Moor, va usar una definició que es basava a identificar i analitzar impactes tecnològics en la part social i humana (salut, riquesa, treball, oportunitat, llibertat, democràcia, coneixement, intimitat, seguretat, realització personal, etc.).
5	En la dècada de 1990, Donald Gotterbarn va canviar el prisma. Per a ell l'ètica informàtica hauria de ser vista com una branca de l'ètica professional, preocupat abans de tot amb estàndards de bones pràctiques i codis de conducta per a informàtics professionals.

Uns altres termes que ens caldran, per a complementar els del tema anterior, són:

Cibernètica: del vocable grec *kybernetes*, que significa pilot o timoner. En Plató, *kybernetiké* expressa pròpiament l'art del pilotatge i, al seu torn, extensivament, l'art de governar els homes. Del terme grec *kyberneter-kybernetes* procedeix la veu llatina *gubernator*, que té aproximadament la mateixa significació grega. Les llengües neollatines recullen del llatí la veu i la significació: en valencià tenim, per exemple, d'una banda, *governall*, terme nàutic i, d'una altra, *govern*, *governador*, terme polític i administratiu. El 1834, el cèlebre científic André Marie Ampère en el seu conegut assaig sobre la filosofia de les ciències, empra la veu *cybernétique* per a indicar l'estudi dels mitjans de govern, en la política. (David, 1973). Amb tot això, entenem plenament la definició que el Diccionari Normatiu Valencià dona del terme: "Disciplina que estudia les diferències i les similituds entre els processos comunicatius humans i els de les màquines amb l'objectiu de construir aparells que imiten els sistemes de comunicació i de comportament humans" o la Real Academia espanyola: "Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas".

Intel·ligència artificial: Qualsevol tècnica de processament d'informació caracteritzada per fer càlculs sobre determinada informació en un espai dimensional virtual i construït mitjançant

operacions generalment no lineals dutes a terme dins del mateix algorisme per a aprofitar diverses propietats d'espais altament dimensionals. (Barrio Andrés, 2018)

Robot: és de sobres conegut el seu origen de la mà de l'autor de ciència-ficció Karel Čapek. El Diccionari Normatiu Valencià el defineix com "Màquina automàtica programable capaç de manipular objectes i d'executar operacions i moviments diversos abans reservats exclusivament a les persones." O la Real Academia espanyola: "Máquina o ingenio electrónico programable, capaz de manipular objetos y realizar operaciones antes reservadas solo a las personas". Però ens interessa més un terme derivat, la **roboètica**, que es defineix com "Part de l'ètica de la intel·ligència artificial que s'ocupa del comportament moral dels éssers humans en relació amb el disseny, la construcció, l'ús i el tractament de robots o de sistemes robòtics dotats d'intel·ligència artificial" o, en espanyol, "Parte aplicada de la ética cuyo objetivo es el desarrollo de herramientas técnico-científicas y culturales que promuevan la robótica como causa de avance de la sociedad humana y de sus individuos y que ayuden a prevenir un uso equivocado de ésta contra la propia especie humana". (Barrio Andrés, 2018)

Molt lligat a l'anterior apareix un terme cada vegada més freqüent, la **màquina ultraintel·ligent**: aquella que pot superar en totes les activitats intel·lectuals qualsevol humà, per llest que aquest siga. Atès que el disseny de màquines és una d'aquestes activitats, una màquina ultraintel·ligent podria dissenyar màquines encara millors. Inqüestionablement, hi hauria una explosió d'intel·ligència, i la intel·ligència humana quedaria totalment endarrerida. En conseqüència, la primera màquina ultraintel·ligent serà l'última invenció que els homes podran fer i assumiran que aquesta màquina siga prou dòcil per a permetre'n que mantinguem el control. (Latorre Sentís, 2019)

Ètica informàtica i professional informàtic

Ja hem vist que malgrat ser la informàtica una ciència recent, és una de les ciències centrals en l'actualitat, perquè és de les que més influència ha tingut al llarg del segle XX, com queda clar en una qüestió ja gastada: se'n sol comparar l'impacte amb la Revolució Industrial, perquè ha canviat la manera de pensar i actuar no solament de les persones sinó també dels grups socials. (Garriga Domínguez, 2012). Els treballadors d'aquesta disciplina tenen, doncs, una sèrie de responsabilitats que cada vegada es fan més importants per al conjunt de la societat. Encara que no sempre va ser així.

Relacionar l'ètica dins de la professió informàtica és un tema que sorgeix de manera estructurada i amb entitat científica en la dècada dels noranta del segle passat. Tal com (Himma & Tavani, 2008) diuen i hem avançat en aquest tema, en aquests anys Donald Gotterbarn defensava que l'ètica informàtica havia de ser vista com l'ètica professional dedicada al desenvolupament i avanç de les normes de bones pràctiques i codis de conducta per als professionals de la informàtica. D'aquesta manera, i com un dels punts de partida, el 1991 publica l'article "Ètica de la computació: la responsabilitat recuperada", del qual destaquem el paràgraf següent: "Hi ha poca atenció al camp de l'ètica professional, als valors que guien en el dia a dia les activitats dels treballadors de la informàtica en el seu paper com a professionals. Per professional de la informàtica em referisc a qualsevol persona involucrada en el disseny i desenvolupament. Les decisions ètiques realitzades durant el desenvolupament tenen una relació directa amb molts dels temes tractats en el marc del més ampli concepte

d'ètica de la computació". Gotterbarn és una de les figures clau, ja que va treballar amb un comitè de l'ACM per a la creació del seu Codi d'Ètica i Conducta Professional i amb uns altres membres de l'ACM i de la Computer Society del IEEE, els codis ètics del qual referenciem en l'apartat pertinent.

Aquesta visió, molt lligada al desenvolupament, és compartida per altres autors. Així, (Bynum & Rogerson, 2004), dediquen el capítol 6 de la seua obra a l'ètica en la gestió d'un projecte programari, assumpte de summe interès que tractarem en aquest mateix apartat. Però potser pecaria de miopia una visió de l'ètica en la professió informàtica sense tractar altres aspectes, com els que ressenyem tot seguit.

D'una banda, tenim l'esfera de la relació del treballador amb la seua empresa. Edgar (Edgar, 2003) parla de la lleialtat que el treballador deu a l'empresa, excepte quan descobreix que l'empresa fa coses il·legals i immorals (el tan conegut *whistleblowing* o revelador d'informació). També Edgar parla dels errors en l'exercici de les seues funcions i la responsabilitat que es contrau amb ells. La catalogació de possibles errors és enorme (canvi d'identitats, errors de transcripció...) i variable segons el tipus de lloc i organització on s'exerceix. Hi ha llocs, com per exemple els relacionats amb la medicina, on aquests poden ser si no més greus, si més visibles socialment. Sobre aquest tema en concret es poden consultar casos (Khosrow-Pour, 2003) (revisat el 2007), (Barger, 2008), i reflexions diverses (Himma & Tavani, 2008). Tanmateix, uns altres, (Cotino, 2008) relacionen exclusivament aquest tema amb la llei i, com a molt, recomanacions de la UNESCO.

Un altre factor important, ressenyat per (De George , 2003), en el seu capítol 3, i per (Edgar, 2003) és el control de les comunicacions que el treballador té dins de l'empresa (i fins i tot a vegades, fora): correus que puga enviar o rebre, webs que visite, presència en xarxes socials i ús d'aquestes... i, sobretot, la importància que hi haja enregistraments o diaris (*logs*) d'això.

Seria absurd intentar abastar totes les facetes possibles, que són moltes i diverses, sobretot tenint en compte la transversalitat de la professió informàtica: podem trobar informàtics a hospitals, col·legis, forces i cossos de seguretat de l'Estat, bancs, empreses farmacèutiques..., cada lloc de treball tindrà uns quants aspectes comuns i d'altres propis i intransferibles. Però sí podem destacar una sèrie d'elements fonamentals en l'ètica de les TIC i els negocis. Això ho veurem amb detall en l'apartat corresponent, però podem començar amb un dels autors ja esmentats i comprovarem que, si no estan tots els elements d'interès, almenys sí són d'interès tots els elements citats: (De George , 2003). Així, esmenta com a principal per a un treballador del sector la privacitat, el risc que corre o pot fer córrer, les relacions dins de l'anomenat negoci electrònic (*e-business*) amb tot l'anterior, el perill que la flexibilitat en el món laboral que es produeix amb les TIC; això és, elements com ara teletreball, temps flexible, globalització, sistemes experts, es gire contra algú i finalment, la censura (que De George relaciona amb la pornografia, especialment la infantil).

No podem esperar tampoc que aparega sola. Lamentablement, l'ètica no sorgeix de manera natural en una organització, per la qual cosa cal emprendre una sèrie d'accions per a incorporar aquests comportaments. Reischl ens diu que "la tecnologia no és ni moral ni immoral, perquè no és ni bona ni dolenta". D'acord, però es pot dir el mateix de les persones que estan darrere de la tecnologia i la venen? En dir això, parla de Google, encara que podria

pujar a aquest carro un altre tipus d'empreses, com és Facebook, per exemple (Reischl, 2008) (una altra visió d'interès en (Ippolita, 2010)). I és que hi ha una doble moral que no es pot obviar. L'exemple el dona Suárez Sánchez-Ocaña en referir-se com Telecinco i la seua guerra contra YouTube, ja que mentre en alguns programes emetia vídeos de YouTube, denunciava la pujada de fragments dels seus programes en la plataforma (Suarez Sánchez-Ocaña, 2012).

L'ètica en els projectes informàtics

(Bynum & Rogerson, 2004) plantegen la qüestió mitjançant un parell de passos, partint del supòsit que es tracta d'una actuació correcta. Per a determinar això, ofereixen una bateria de preguntes que han de tenir un resultat monocolor. Si l'assumpte és pot afrontar, és quan s'estableix un pla: enumeren els principis bàsics en què un professional de les TIC s'ha de moure, amb qüestions que ens permeten saber si anem o no per bon camí i això es creua de forma matricial amb els passos d'un projecte informàtic. Veurem això punt a punt. Comencem amb les preguntes.

- L'acció final donarà com a fruit una cosa positiva? Per a obtenir resultat, es planteja la bateria de preguntes següent sobre l'acció a executar:
- És honorable? Hi ha algú de qui t'agradaria ocultar l'acció?
- És honesta? Viola algun acord, real o implícit, o d'una altra manera traeix un compromís?
- Evita la possibilitat de conflicte d'interessos? Hi ha altres consideracions que puguen esbiaixar el judici?
- Està dins de la seua àrea de competència? És possible que fins i tot amb el teu millor esforç el resultat no siga adequat?
- És just? És perjudicial per als interessos legítims dels altres?
- És considerat? Violarà la confidencialitat o privacitat o danyarà algú o alguna cosa?
- És de naturalesa conservadora? Es malgasta innecessàriament el temps o altres recursos valuosos?

Per a ser ètica segons (Bynum & Rogerson, 2004), una acció ha de provocar una resposta positiva a totes les preguntes anteriors aplicables i una resposta negativa a cada explicació.

Una vegada veiem que no hi ha problema, deixem de veure-ho de forma general i ho particularitzem. Per a això, s'estableix una relació de principis ètics per a professionals de la informàtica.

Taula 2. Principis ètics per a professionals de la informàtica, adaptat de Bynum i Rogerson.

Principi	**Pregunta relacionada**
Honor	L'acció es considera més enllà de tot retret?
Honestedat	L'acció viola cap acord explícit o implícit?
Biaix	Hi ha alguna consideració externa que pot esbiaixar l'acció a prendre?

Adequació professional	Està l'acció dins dels límits de la nostra capacitat?
Cura deguda	S'usen els millors estàndards de garantia de qualitat possibles?
Equitat	Es consideren tots els punts de vista dels implicats respecte a l'acció?
Consideració (Cost social)	S'accepta la responsabilitat i la responsabilitat que comporta aquesta acció?
Acció efectiva i eficient	És l'adequada atesos els objectius establits i s'usa la menor despesa de recursos?

Finalment, fets els passos de desenvolupament d'un projecte, es vincula a cadascun d'aquests passos una relació d'aquests principis.

Taula 3. Principis ètics dominants en cada pas de la gestió d'un projecte. Adaptació de Bynum i Ward.

Pas/principi	Honor	Honestedat	Biaix	Adequació	Cura	Equitat	Consideració	Acció
Visualitzar l'objectiu	X	X	X		X	X	X	
Llista dels treballs que deuen			X					X
Assegurar-se que hi haja un líder			X	X	X			X
Assignar persones als treballs	X	X	X	X				X
Gestionar les expectatives		X			X	X	X	
Estil de lideratge	X			X			X	X
Controlar què succeeix								X
Contar què succeeix	X	X	X		X	X		

Repetir els passos anteriors fins a realitzar l'objectiu					X			X
Realitzar l'objectiu del projecte	X		X				X	X

Amb la taula precedent podem saber on hem de marcar el focus en cadascun dels passos.

Deures del professional informàtic

Ja tenim el professional dins d'un projecte. Ens queda marcar aquestes delicades línies roges que no ha de traspassar. Per a això, seguim (Vázquez & Barroso, 1996) que ens donen la relació següent:

Secret professional

Naix d'un contracte tàcit o exprés entre aquell que exerceix la professió informàtica i aquell que va a la recerca del seu consell en virtut de la seua professió. La matèria del secret professional s'estén a tot allò que no pot, per la seua naturalesa, ser manifestat sense causar perjudici justificat i, a més, a tot quant ha sigut confiat sota promesa de guardar silenci. Per a informàtics s'estén no solament al que ha sigut confiat directament al professional, sinó a tot allò que ha arribat a coneixement del professional en virtut de l'exploració o dades que se li han donat directament. Per les nostres mans passen moltes dades que impliquen no solament la privacitat de les persones, sinó moltes vegades la seua vida. S'ha parlat molt del poder que dona la informàtica, fet que parteix del clàssic d'Orwell *1984*, amb el seu Gran Germà, i arriba als nostres actuals sistemes de prevenció de delicte amb algorismes precrim o a les mateixes dades massives (Big Data).

Caldria relacionar això amb la fidelitat a la institució o empresa i el revelador d'informació que ja anticipàvem.

La dicotomia

Es refereix a treballar amb diverses "caretes", a la divisió d'horaris, a la repartició indeguda o fraudulenta d'honoraris..., és una pràctica moralment il·lícita, es tracta de repartir els honoraris de la consulta, donar comissions, etc.

Suborn

Donar avantatges o regals de tota mena per a aconseguir determinades concessions o contractes en favor de terceres persones o entitats.

Relacions laborals

S'atempta contra la deontologia en les relacions laborals en incomplir un contracte laboral, per tema salarial, tant per ser excessivament baixos en les escales més modestes com per excessivament elevats per als alts directius, per abusar de treballadors eventuals, per augmentar els beneficis per procediments condemnables, quan es produeixen baixos rendiments que ocasionen costos, quan es donen fallides culpables i fraudulentes o escàndols financers o quan no s'adopten garanties efectives en treballs proclius al risc i, en general, tot el

tipus de treball que no siga adaptat a les actituds, forces i capacitats de la persona segons l'edat, sexe i salut.

Dins d'aquestes relacions laborals caldria considerar la prevenció del delicte. Sembla paradoxal després d'haver plantejat la discussió sobre els algorismes precrim com a massa intrusius, però és que parlem no d'inferir conductes sobre les persones, sinó en la prevenció pura. La veritat és que aprofitant una xarxa que gestionem, un empleat pot cometre delictes informàtics que no solament cauran sobre la nostra consciència, sinó sobre el nostre expedient: si un empleat usa les xarxes de l'empresa per a enviar correu brossa (*spam*), per a amenaçar algú, per a propagar continguts perillosos, ens assegurem almenys una visita de les forces i cossos de seguretat. Referent a això, cal recomanar la lectura d'un cas magníficament exposat per Jennings: "Employee and Technology Privacy: Is the Boss Spying?" (Jennings, 2009).

També les TIC semblen empènyer a continuar treballant a persones que haurien d'estar jugant o comunicant-se amb la seua família i amics. La frontera familiar, la invasió de la privacitat i l'oci, mantenir els límits: família, treball i diversió. D'igual manera que els jocs en línia o les xarxes socials capten cada vegada més persones, el teletreball pot afectar en el mateix sentit. Aquest és un altre aspecte que encaixaria dins de les anomenades relacions laborals.

A més del que deixen assentat (Vázquez & Barroso, 1996) ens permetem afegir un element d'interès addicional.

Vigilància tecnològica

Hi ha alguns aspectes de les TIC que preocupen la societat en general. Al marge d'elements com ara la bretxa digital, els analfabets digitals, que ja s'intenten combatre des de la nostra legislació, considerem facetes de profunda preocupació sobre la qual tot professional ha d'estar alerta.

En aquest sentit podríem parlar del fenomen del ciberassetjament (*cyberbullying*) o el porno venjatiu (*revenge porn*), de la seua prevenció, però com un fet que va més enllà d'impedir un delicte, sinó de posar tota barrera possible per a combatre'ls, parlem d'un nivell molt més elevat. Pensem que elements com són el porno venjatiu, o l'assetjament, pot portar les persones a casos extrems que fins i tot consideren el suïcidi. Posarem l'accent en dos elements molt sensibles: les notícies enganyoses (*fake news*) i la informació de menors.

Comencem amb les anomenades **notícies enganyoses**, que són una edició corregida i augmentada de les velles xafarderies i mentides de porteria, però que cobren una importància tremenda amb la xarxa de xarxes. Pensem en la facilitat que hi ha, usant rumors, per a decantar la balança política d'un país o afonar una empresa. El primer dubte és, doncs, per què ens ho empassem? I l'explicació ve quasi de la nostra pròpia evolució. L'ésser humà durant quasi tota la seua història, millor dit, la prehistòria, abans de cap registre escrit, va viure en comunitats, en tribus, molt reduïdes. Quan arribava una notícia de l'estil "el lleó ve corrents", li donàvem la credibilitat que necessitava la nostra vida per a ser salvada. Dividíem el missatge pel nombre de gent que podia donar-lo. Si en una tribu de vint individus, quatre ens avisaven de l'arribada del lleó, una probabilitat del 20% era molt alta: el lleó venia.

Ara ens arriba milers de vegades la notícia que el lleó ve, i a més és verd i amb fermalls violetes. Però continuem dividint pel nombre de gent coneguda, que és molta, però no és tot el globus. El missatge, si arriba moltes vegades, continua sent creïble. Com a més l'ésser humà té, com tots els antropoides, una innata tendència a imitar, es produeix immediatament el contagi en la xarxa: tots comencen a copiar. I provoca l'èxit de les teories conspiranoiques: si fa l'efecte que tothom parla d'un tema, això ha de ser cert.

En particular és de molt d'interès posar cura en **els infants**. Ens recorda (Livingstone, 2009) que cada vegada és més fàcil crear continguts, no solament per professionals, sinó pels mateixos xiquets, que moltes vegades no li donen per si mateixos el significat i les conseqüències de l'ús d'Internet. En aquest sentit, Livingstone ens ofereix una taula amb oportunitats i riscos de les activitats en línia per a menors. (Livingstone, 2009)

Taula 4. Oportunitats i riscos en línia, adaptat de Livingstone.

Oportunitats	**Riscos**
Accés global a la informació	Continguts il·legals
Recursos educatius	Pederastes
Xarxes socials entre amics	Violència extrema o sexual
Entreteniment, jocs i diversió	Un altre contingut ofensiu nociu
Aprendre a desenvolupar continguts	Material i activitats racistes
Participació cívica o política	Publicitat i màrqueting agressiu
Privacitat davant la pròpia identitat	Informació errònia o parcial
Participació en la comunitat / activisme	Robatori d'informació personal
Increment de coneixements tecnològics i alfabetització digital	Assetjament / assetjament cibernètic / *Cyber-bullying*
Millores per a futures ocupacions	Jocs d'atzar
Orientacions sobre salut / sexe	*Phishing*, estafes financeres
Fòrums especialistes	Autodany (suïcidi, anorèxia)
Fòrums de fans	Inducció a cometre activitats il·legals
Compartir experiències amb uns altres	

Els xiquets usen les oportunitats, és cert. Exploren espais privats en línia per a experimentar amb noves identitats, per a buscar anuncis confidencials, explorar gustos personals, inspeccionar la interacció dels altres o per a conèixer persones de llocs llunyans. A pesar que la xarrada en línia pot semblar vàcua per als observadors adults, per als infants és una activitat altament valorada socialment, que els converteix en la generació del contacte constant.

(Livingstone, 2009). Però com que també hi ha riscos, cal prevenir-los. Livingstone matisa la relació anterior amb una classificació de riscos en línia per als xiquets.

Taula 5. Riscos en línia per als infants, adaptat de Livingstone.

	Enganys comercials	*Mal directe*	*Sexe*	*Falsos valors*
Contingut – infant com a recipient	Anuncis Contingut brossa (*spam*) Patrocinadors	Violència Contingut amb càrrega d'odi	Pornografia o continguts sexuals inesperats	Racisme Consells enganyosos (p. e. drogues)
Contacte – infant com a participant	Seguiment / recol·lecció d'informació personal	Ser intimidat, assetjat	Conèixer estranys, pederastes	Autolesió, xarrades incòmodes
Conducta - infant com a actor	Jocs d'atzar, descàrregues il·legals	Assetjar un altre	Crear i pujar pornografia	Facilitar addiccions o males conductes (p. e. suïcidi, postures proanorèxiques)

Dimensions morals

Com podríem classificar els elements principals entorn dels quals agrupar els dilemes que susciten els sistemes d'informació? Si revisem la literatura científica podem trobar una quantitat de classificacions tal que necessitaríem tot l'espai de les anotacions de l'assignatura per a simplement ressenyar-les. Anem simplement a deixar constància de les més clàssiques i després ens centrarem en la que, per la seua completesa, ens sembla més rellevant: les dimensions morals dels professors Laudon (Laudon & Laudon, 2016). De fet, queda com a proposta per al lector veure com totes les categories que van apareixent encaixen en una de les dimensions morals, que es veuen amb més detall.

Un text de referència present en tota relació que es preue és el de (Bynum & Rogerson, 2004), que al·ludeixen als aspectes de les relacions humanes que s'afecten per la intersecció d'ètica i informàtica. Així, parlen de temes com ara:

- El sexe virtual.
- La privacitat i l'anonimat. Relacionat amb el punt relatiu a la privacitat, es plantegen si els polítics i altres personatges públics han de gaudir d'una privacitat assimilable a la de la resta dels ciutadans.
- La propietat intel·lectual, de forma àmplia, des de la difusió de material multimèdia fins als múltiples fronts que s'obrin, dels quals convé destacar la dicotomia entre cultura i propietat.
- Relacions laborals, incloent-hi el teletreball i els seus problemes.

- Possibles problemes de justícia social. Aquest és un tema molt ampli, que va des de l'analfabetisme digital fins a la gent sense identitat digital que pot perdre qualsevol identitat.
- Govern i democràcia: del vot electrònic al contacte dels ciutadans amb els seus representants, un tema que les xarxes socials han tornat a posar al cim.

És una visió més pròxima a la que nosaltres busquem: crear categories per la seua interacció amb l'ésser humà i la societat en general. Uns altres autors, com ara (Edgar, 2003) el que fan és prendre la llei com a referència, cosa que si bé ha sigut presa com un eix vertebrador per molts, pensem que ens allunya del que és el nostre propòsit en parlar d'ètica, de deontologia: es tracta d'anar més enllà del que la llei exigeix. Així, part de la divisió de danys realitzats contra els ordinadors o usant ordinadors i relaciona:

- Estafa (un usuari que no existeix realitza una compra).
- Robatori de servei (serveis de telecomunicacions).
- Robatori d'informació (mitjançant *sniffers*, per exemple).
- Frau (lucrar-se mitjançant engany. Això és molt ampli, és clar. Bàsicament parlem de dues coses: presentar informació falsa per a obtenir benefici o, directament, malversar).
- Crim organitzat, on l'autor inclou el fenomen de la pederàstia.
- *Counterfeiting* o falsificació: robatori de comptes, suplantació de perfils...

Com hem anticipat, ens centrarem per al desenvolupament en el treball dels professors Laudon. Les seues dimensions morals dels sistemes d'informació són una proposta clàssica (la seua primera edició és de 1996) per a enfrontar-se a l'ètica dels sistemes d'informació. Són cinc categories en què encaixarien tots els dilemes a què un professional es pot enfrontar: (1) drets i obligacions d'informació, (2) drets i obligacions de propietat, (3) qualitat del sistema, (4) qualitat de vida i (5) rendició de comptes i control. Anirem desglossant-los.

Drets i obligacions d'informació

Quins drets d'informació posseeixen els individus i les organitzacions respecte a si mateixos? Què poden protegir? Podríem parlar de camps tan actuals com ara Big Data o la IoT (a través de la informació dels sensors).

Ja sabem que a Espanya, a la UE, això és un dret bàsic, recollit en la normativa sobre protecció de dades, on a més es parla de temes que entren de ple en el camp de l'ètica, els *codis tipus*. També ens incumbeixen en aquest sentit aspectes com és el control del correu electrònic en les organitzacions.

Els algorismes creuen dades i cerquen traure conclusions entre les persones i els seus comportaments i persones. Ací apareix el primer punt: És ètic crear programes que recopilen informació sobre el nostre comportament? Fins a quin nivell és lícit que l'aspecte humà siga supervisat, analitzat, escodrinyat en els detalls més íntims per legions de programes operats per interessos que desconeixem? (Latorre Sentís, 2019) Hem de considerar que en situacions límit per a la seguretat, fins i tot sense haver d'arribar a l'extrem d'una ciberguerra (Edgar: 425), es pot emprar una, anomenem-la, ètica alternativa (Edgar, 2003) (Himma & Tavani,

2008) (Clarke & Knake, 2010) que incloga l'ús de la informàtica per al control de ciutadans, pacífics o no[3].

Durant anys s'ha utilitzat el terme legal d'"Habeas Data" com un resum de tot dret sobre les nostres dades. Parlem del dret a conèixer l'existència i accedir als documents que ens concerneixen, incloent-hi dades genètiques, bancàries o qualsevol fitxer que conste en entitats públiques o privades, del qual podrem conèixer-ne l'ús, finalitat, origen i destinació a més de poder exercir el dret a l'actualització de les nostres dades, la rectificació, limitació o anul·lació. (Latorre Sentís, 2019)

Les organitzacions, les empreses, empren bé la majoria de les vegades la informació dels ciutadans, però a voltes es produeixen problemes. Els exemples possibles serien molts: des de qui trafica amb dades mèdiques que s'emmagatzemen als hospitals fins a activitats poc honrades per empreses que inclouen bombes lògiques en el seu programari, de manera que si el número de registre no s'ha introduït en una data determinada, el programari, i potser un poc més, s'esborra (Barger, 2008). Això, a cavall entre ètica i llei sovint es complica amb episodis de falsedat documental, com ara la venda de títols acadèmics en línia o un altre tipus de documentació falsificada. Un exemple real pot ser el que comenta (Girard, 2007): Un competidor pot fer milers de clics sobre els anuncis a Google dels seus competidors per a incrementar-ne les factures. Encara que segons Google no és sinó un fet aïllat ens permet reflexionar-hi.

Abans de deixar aquesta dimensió, anem a un cas extrem: les dades dels morts, considerades des del conegut dret a l'oblit. El professional hauria d'establir protocols per a esborrar la presència a Internet de gent que ha mort, evitar que estranys els insulten o se'n riguen. Però no tot es pot esborrar, si hi ha referències en diaris impresos queden les hemeroteques i, d'altra banda, és lògic que una part de la informació d'individus públics siga preservada. (Latorre Sentís, 2019).

Drets i obligacions de propietat

Com es protegiran els drets de propietat intel·lectual tradicionals en una societat digital en què és difícil rastrejar i retre comptes sobre la propietat, i és molt fàcil ignorar aquests drets de propietat? Ací podríem plantejar-nos dilemes sobre els secrets comercials, a més de les clàssiques regalies a la propietat intel·lectual, i la diferència entre *copyright* i patents. Això sí, considerem que, en aquest cas concret, hi ha diferències significatives: diferents països, diferents lleis (Barger, 2008).

Partim d'un exemple que ens permet veure que en aquest cas no hi ha blancs i negres, no hi ha veritats absolutes, ens movem sobre un paisatge gris. El 10 d'octubre de 2007 el grup Radiohead va oferir als seus seguidors l'opció de pagar el que volgueren per descarregar-se'n el nou àlbum *In rainbows*. Si volien ho podien descarregar gratis, o donar el que volgueren.

[3] Durant la legislatura de 1964 a 1968, el president dels Estats Units Lyndon B. Johnson va mantenir unes tibants relacions amb J. Edgar Hoover, director del FBI. Aquest no deixava de recórrer a escoltes telefòniques il·legals a fi d'obtenir informació valuosa d'altres dirigents polítics, susceptibles de ser emprades per a coaccionar-los i fer-los xantatge. El president tement que acabara per intervenir el seu telèfon va estar a punt de destituir-lo, però va desistir després de concloure amb mordacitat "És preferible tenir-lo dins de la botiga pixant cap a fora, que no pixant cap a dins".

Vora un milió de fans ho van fer el primer mes, dels quals 6 de cada 10 no van pagar res. Diversos milions més s'ho van descarregar per P2P en lloc de fer-ho de forma gratuïta des del web del grup. Va ser el disc que més diners li va donar, sense haver de compartir els diners amb cap segell discogràfic. Quatre mesos després va eixir a la venda una versió de més qualitat de l'àlbum i va arribar a ser el més venut de les llistes americanes i britàniques. A l'octubre de 2008 havia venut més de 3.000.000 de còpies, de les quals 100.000 en una capsa especial a un preu de 80 dòlars i sobrepassava les vendes dels seus dos àlbums anteriors. (Porter, 2011)

Podem pensar que Internet ho ha revolucionat tot en aquest camp, però, sense deixar de tenir bona part de certesa l'afirmació, no ho és de forma completa. Abans d'Internet, hi va haver la ràdio, i entre les dues, la televisió, que va ser el model de mitjà de comunicació gratuït per excel·lència. Un programa d'una hora implica normalment 48 minuts de programa i 12 minuts d'anuncis amb els quals es paga aquest. El 2009, per exemple, els anunciants van afirmar haver pagat uns 230.000 dòlars per un espot de 30 segons en la sèrie d'ABC *Desperate Housewives*. A aquell preu cadascuna de les 10,6 milions de llars que veia la sèrie tenia un valor per a la cadena de 79 centaus. I apareixen ací els gravadors de vídeo digitals com és el Tivo, que permeten als teleespectadors saltar-se els anuncis i, per tant, amenacen de privar-ne les cadenes dels diners en permetre que els seguidors d'una sèrie la vegen sense cost de diners ni de temps[4]. Els executius plantejaven que cada vegada que un televident se salta un anunci està robant la programació, però els teleespectadors no tenim obligació legal de veure res, per molt que s'assumisca un acord econòmic implícit amb el qual s'han sostingut les cadenes de televisió i que, si fracassa, els forçarà a trobar altres fonts de finançament[5]. (Porter, 2011)
Quan es vulnera de debò la propietat intel·lectual? És homologable compartir una pel·lícula en format DivX amb un amic, amb la clàssica còpia de vinil a casset que el legislador al seu moment va preveure? On traçar la barrera entre còpia de seguretat i còpia privada?

La vulneració de la propietat intel·lectual la va estudiar des del prisma ètic (De George , 2003), que va crear la classificació següent:

- Intercanvi de pel·lícules, cançons..., als països desenvolupats.
- Enginyeria inversa en determinats països, p. e., per a copiar vacunes, retrovirals..., l'autor cita com a exemple que la Xina ha signat tots els tractats internacionals sobre propietat intel·lectual, però dins les seues lleis semblen no tenir efecte, ja que es planteja: és dolent salvar vides usant un retroviral patentat, amb el formulisme i

[4] Quan el VCR va arribar als EUA, la indústria de la TV i el cinema clamaren a Déu, amb l'argument que el VCR violava les lleis de *copyright*. Els jutges van dir que els VCR tenien molts usos legítims, un dels quals enregistrar les emissions per a veure-les de forma privada més tard.
Es pot gravar un programa fins i tot si es ven comercialment per a veure'l en un altre moment, i també deixar-lo a un altre amic, que interessat a veure'l s'equivocara al seu torn en programar el vídeo. El principi per a Internet és, hauria de ser, igual (De George).

[5] Els problemes dels mitjans convencionals i els seus ingressos no es deuen a la difusió pels nous mitjans tant com per les tècniques emprades. En la premsa escrita, més antiga que la ràdio i la TV, els diners venen no solament de la venda. De fet, l'import de compra és minoritari en els ingressos de les empreses: els diners venen més de la publicitat que de la venda de diaris. Quan apareix la xarxa, es va pensar que s'incrementarien els ingressos publicitaris i es reduiria el cost d'edició, però això no va ocórrer. I no per cap pirateria, sinó per una falta d'adaptació als nous models de negoci possibles (Porter).

forma d'obtenció que s'ha *piratejat* dels ordinadors d'una poderosa multinacional farmacèutica?

- Comprar menys llicències que còpies instal·len d'un determinat programari.
- Vendre programari que en principi no tenia preu, per exemple, creats amb llicència Creative Commons. I no solament programari.
- Copiar programes per a ús personal: el cas d'un estadístic que es porta a sa casa per a ús i gaudi privat una còpia de l'última versió de SPSS disponible a la seua empresa. Sense pagar les llicències, evidentment.

Quant a nosaltres, fem una classificació molt elemental: contingut i continent. El contingut per a nosaltres són els elements que gràcies a la informàtica poden ser transferits fins i tot sense coneixement dels propietaris dels seus drets, i el continent, el programari.

En parlar de transferència de continguts el que va al capdavant de molts són les descàrregues directes i les xarxes P2P o d'igual a igual (*peer-to-peer*). Aquest tipus de protocol es va fer famós amb Napster: els usuaris de manera gratuïta descarregaven enregistraments en format mp3. De resultes d'això, alguns músics, productors, artistes i companyies van presentar demandes per infracció de drets d'autor contra Napster. Una anècdota poc coneguda és que a mesura que l'assumpte es complicava en els tribunals, Napster va començar a experimentar alguns problemes amb el seu logotip, que va aparèixer en samarretes a la venda. Napster va presentar una demanda contra els que utilitzen la marca sense autorització, que va demanar danys i perjudicis. Posteriorment, un tribunal federal va tancar Napster i BMG el va comprar. Unes altres plataformes van aparèixer, com ara Grokster, Kazaa o Morpheus, però també les portaren a plet. La Recording Industry Association of America (RIAA) va iniciar una agressiva política en presentar demandes fins i tot contra els usuaris que descarregaven cançons, i va intentar en els tribunals que els prestadors de serveis d'Internet revelaren els noms dels usuaris, a la qual cosa algunes es van resistir (Jennings, 2009).

(Lessig, 2001) planteja un escenari terrible: als EUA la indústria creà un estàndard per a facilitar el control en la distribució de música. El congrés dels EUA, al seu torn, crea una llei que considera delicte greu crear SW que eludira aquest control. I una empresa que fabrica reproductors anuncia plans per a complir aquests estàndards de control. El resultat és pervers: el control està codificat pel mercat, amb el suport de l'Estat.

Música, pel·lícules i... llibres. Amb la popularització dels llibres electrònics (*e-books*) es torna al cultura *vs* propietat intel·lectual. És un vell debat que porta a reflexionar sobre la infraestructura d'Internet i les eines digitals com a bé comú, no usar-les per a satisfer les necessitats d'un model propietari i –això és l'eix del debat– que els drets d'autor no poden imposar-se a costa d'altres drets fonamentals, i que només un procediment judicial pot establir sancions (Aigrain, 2012). En aquest sentit, recordem quan es va acusar Google de despietat per arrambar amb el seu Google books llibres que, fins i tot introbables a les botigues i també a les biblioteques públiques, tenien els seus drets intel·lectuals. (Brandt, 2009) recorda que l'adjectiu de despietat ja es va aplicar en una altra situació passada: quan la biblioteca d'Alexandria es va crear gràcies als saquejos dels pirates ptolemaics. I no fa falta recordar com es van nodrir els principals museus de Londres (potser gràcies a això pedres mil·liars de la nostra cultura s'han preservat fins avui).

Ens queda el nostre cavall principal de batalla. El programari. (Bynum & Rogerson, 2004) Posem una reflexió sobre les diferències entre patent, secret professional o *copyright*, però això fa curt. Per exemple (Barger, 2008) es pregunta: On encaixa ací, on està el programari obert? Així que ho ampliem amb una visita al text de Richard Stallman: "Per què el programari ha de ser lliure?" (Stallman, 2004)

Lliure no és gratis, encara que tendim a confondre-ho. D'altra banda, la gratuïtat no és exclusiva d'Internet. Pensem en els regals i el seu important paper en moltes societats, com ara el *potlatch* entre els nadius de l'Amèrica nord-occidental i el *kula* entre els melanesis de les illes Trobriand: cicles de regals virtuals que es donen entre les tribus veïnes (Porter, 2011).

Després de les exposicions anteriors, queda clar el posicionament que puguem mostrar a favor del programari lliure. I és que, amb Crespo, creiem que (Crespo Fajardo, 2012) el moviment del programari lliure fa especial èmfasi en els aspectes morals o ètics del programari, que veu l'excel·lència tècnica com un producte secundari i en prioritza el valor ètic. L'ús, la millora i la distribució d'eines lliures i gratuïtes permet revisar conceptes que fins fa poc semblaven inamovibles. L'economia de mercat es converteix així en desenvolupament sostenible i la comunitat dels desenvolupadors és el nucli d'una vertadera i autèntica societat oberta, on, a més, es dona per l'efecte col·laboratiu una qualitat més alta de les aplicacions (Ippolita, 2010).

És una idea que es pot traspassar, tant de bo fora així, a la resta de les creacions humanes: estem acostumats a una visió dogmàtica dels drets d'autor. És més, propugnar la idea de permetre a les persones que no són ni autors ni titulars de drets d'autor d'una obra d'art, o una peça de programari, per a compartir-la amb altres persones, equival a l'heretgia (Aigrain, 2012).

Rendició de comptes i control

Qui pot i es farà responsable, a més de rendir comptes pel mal fet a la informació individual i col·lectiva i als drets de propietat? Parlaríem d'elements com ara la rendició de comptes als individus i a les institucions. I elements d'interès com el plantejat ací: si una persona es lesiona a causa d'una màquina controlada per programari, qui n'ha de retre comptes? (Pensem sobre aquest tema en els cotxes autònoms, en un tauler d'anuncis d'ADIF o una pantalla en un centre comercial que transmeta apologia del terrorisme o una cosa ofensiva.) N'hi ha un responsable? O és el mateix que amb els proveïdors de comunicacions, com són els telèfons? Es podrien analitzar casos clàssics, com ara el robatori per hackers coreans de dades de la seguretat social dels EUA o la sostracció del fòrum sobre malalties "Patients like me".

Vegem aquest cas més a poc a poc: PatientsLikeMe, *pacients com jo* des del seu origen: és un espai que permet a una persona que pateix una malaltia greu i cerca a Internet tot tipus de formació i suport emocional, trobar un punt de reunió: un web, un fòrum, un espai en una xarxa social per a compartir idees, notícies o tractaments, o qualsevol altre tipus d'informació rellevant sobre la malaltia que pateix. Però el que no es va preveure va ser protegir la informació personal que apareix en aquest espai i aquesta acaba arribant a una base de dades que utilitza l'empresa que contracta... aquest pacient, a qui se li nega un possible ascens per informació rebuda. (Latorre Sentís, 2019)

Un altre exemple: l'hegemonia de les grans empreses sobre els nostres drets. Pensem que la Casa Real, diferents ministeris, accepten sense pensar les TOS de Twitter i altres xarxes, que fan oblidar el marc legal espanyol per a traslladar-nos a Silicon Valley. D'altra banda, ja és hora de sembrar de denúncies tota xarxa social que s'arrogue prerrogatives de jutge? Fins a on és lògic que es retalle la llibertat d'expressió? Els drets fonamentals els són, estigues on estigues: podria una xarxa social negar l'accés a gent segons la seua raça o tendència sexual? No competeixen les TOS, termes de servei, amb les lleis estatals? Això que diu Zuckerberg de "si (Facebook) fora un país, seria el país més gran del món", se suposa que li possibilita situar-se per damunt de lleis nacionals i internacionals? El més important: hi hauria un jutge que s'atrevira a limitar-ne els actes?

Qualitat del sistema

Quines normes sobre la qualitat de les dades i dels sistemes s'han de requerir per a protegir els drets individuals i la seguretat de la societat? El terme *qualitat* redunda sobre el primer principi: si mantenim una dada antiquada d'un client, o bé si encara tan sols mantenim la dada, quan aquest n'ha sol·licitat expressament el desig de ser donat de baixa en la nostra base de dades, vulnerem la llei.

Sembla estretament relacionada amb l'anterior, però n'és independent. Ací ens preguntem: Quin és un nivell factible i acceptable, des d'un sentit tecnològic, de qualitat d'un sistema? En quin punt s'ha de deixar de provar i llançar un programari, un maquinari? El marc legal pot deixar llacunes..., i si l'usuari manipula el nostre producte? Hauríem de blocar aquesta possibilitat? Podem veure la qüestió difusa de l'assumpte considerant un sistema en què hi ha errors només predictibles i corregibles amb un cost molt alt, tant que no es podria comercialitzar. I si no ho traiem? No arribaria fins a decaure la qualitat de vida col·lectiva? Referent a això, relacionem les tres principals fonts d'un mal acompliment del sistema: a) brossa (*bugs*) i errors de programari; b) fallades de maquinari o de les instal·lacions provocades per causes naturals o d'un altre tipus, i c) mala qualitat de les dades d'entrada.

Quan pensem en el cim de la tecnologia humana, a molts el primer que ens ve a la ment és l'arribada de l'home a la lluna (i d'això ja fa mig segle!). Aquesta proesa va ser possible gràcies a l'ús de la informàtica per la NASA. *A priori*, tot sembla indicar que, si algú ha d'usar sempre l'última tecnologia i estar pendent de qualsevol innovació, ha de ser l'agència espacial... Doncs no, lamente desil·lusionar-vos. Es va saber que l'any 2002 la NASA adquiria a eBay un gran nombre d'equips mèdics antics que contenien el microprocessador 8086 de la companyia Intel, el mateix que havia emprat IBM per al seu ordinador personal el 1981. Un processador un quants milions de vegades més lent i moltíssim menys eficaç que els ordinadors d'aquell moment. L'explicació és que el programari que havia de provar els motors principals de la llançadora s'havia escrit en origen en aquest processador, el 8086, i si no podien executar-lo s'acabaven els llançaments. I és que quan els informàtics elaboren, netegen defectes i errors (vaja, se submergeixen en una depuració [*debug*] infinita) i assagen amb un programari tan *import*, estan aterrits per la idea d'haver de modificar-lo. El clàssic: "Si funciona, no ho toques. Si funcionava, ho vas tocar i ja no funciona, fava!". Però no els faltava raó: aquests programes són tan complexos que no s'atreviria ningú a alterar-los i estar segur que funcionaran a la perfecció en un aparell nou. La prova que la renovació és tan costosa és perquè aquell mateix any la NASA va dir que invertiria 20.000.000 de dòlars per a actualitzar-lo.

Recapitulem: la major gesta tecnològica de l'ésser humà, que va suposar la conjunció de moltes ciències i tècniques, amb suport i impulsades per la capacitat de còmput, sí, havia avançat..., però amb un retard almenys de dues dècades.

Qualitat de vida

Quins valors s'han de preservar en una societat basada en la informació i el coneixement? Quines institucions hem de protegir per a evitar que se'n violen els drets? Quins valors i pràctiques culturals donen suport a la tecnologia de la informació? Les tecnologies de la informació poden arribar a destruir elements valuosos de la nostra cultura i societat, fins i tot encara que ens brinden beneficis. Si hi ha un balanç de bones i males conseqüències, a qui responsabilitzem per les males conseqüències?

Pensem en la bomba atòmica i la seua responsabilitat. No està en l'avió que amolla la bomba ni tampoc en la bomba, sinó en els científics que van concebre l'arma i en el coronel que va triar el moment per a soltar-la. La responsabilitat dels nostres actes no es transfereix als objectes inanimats. Si aquesta decisió la pren un algorisme, hem d'intentar transmetre la nostra ètica a les màquines (Latorre Sentís, 2019).

Hi hauria molts subtemes que encaixar ací, però destacarem un que cada vegada més implica un nombre superior dels nostres conciutadans: els jocs, en concret els jocs en línia.

Dia a dia, el nombre de persones que entren en la xarxa, no a la recerca d'uns minuts de xarrada, ni per cercar referències de pel·lícules, cançons o llibres, sinó per jugar, per fer ús de jocs en línia, creix. Hi ha aplicacions milionàries en usuaris, on aquests passen hores i hores.

No és terrible aquesta manera de perdre el temps? (Lessig, 2001) Mentre el comú de la població es dedica a treballar seixanta, setanta hores setmanals per a empreses que no els pertanyeran mai i creen futurs que no saben si arribaran a gaudir, aquestes persones es dediquen a dissenyar i fabricar cases i construir-se una vida allí, encara que siga virtual, mentre treballen a colp de ratolí, sense arada, plantant melons i cuidant porcs virtuals que els permeten comunicar-se amb un nou codi de relacions amb els seus ciberamics (Himma & Tavani, 2008) ens parla dels jocs, en concret dels jocs compartits, i de les relacions que es generen, així com de la informació que es comparteix, com també de la realitat virtual i la simulació. Sobre jocs de més calat econòmic i la prevenció de riscos, es pot veure en (Cotino, 2008) "Juegos: prevención de riesgos y casinos de juego en Internet".

Codis ètics en relació amb la informàtica

En el cas de la professió informàtica, al marge del que els col·legis redacten a Espanya, són ja clàssics els que procedeixen de les associacions professionals que prenen el testimoni i formulen els seus codis ètics. N'hi ha de concisos, com ara el del IEEE, o prolixos, com és el de l'ACM (Association of Computer Machinery).

Els codis del col·legi professional, d'ACM i de IEEE són molt fàcils de localitzar a Internet. Cerca'ls.

També les empreses informàtiques o associacions d'aquestes tenen els seus codis, i un estudi sobre la seua composició ens fa veure que en un elevat percentatge estan centrats en la problemàtica de la protecció de dades personals, que com vam veure encaixava en una de les

dimensions morals. Però n'hi ha més, com ara la particularització, referida per (Cotino, 2008), de codis de conducta en la contractació electrònica a Espanya o l'autoregulació per a comunicacions comercials electròniques.

Recordes la definició de codi tipus? Relaciona-la amb la protecció de dades. Pista: Ves al Reglament Europeu de Protecció de Dades i localitza referències (directes o indirectes) sobre aquest assumpte.

Mínims a cobrir en cada dimensió moral per un codi ètic d'una empresa o associació informàtica.

En aquest epígraf seguim de forma rigorosa els professors (Laudon & Laudon, 2016).

Normes ètiques mínimes a incloure per consideració als drets i obligacions de la informació:

- Privacitat del correu electrònic.
- Tractament de les dades de l'empresa respecte a les normes.
- Polítiques de transparència cap als clients.

Normes ètiques mínimes a incloure per consideració als drets de propietat:

- Ús adequat de les llicències de programari.
- Respecte a la propietat d'instal·lacions i dades de l'empresa.
- Gestió adequada de la propietat del programari creat per empleats de l'empresa.
- Evitar ambigüitats en les relacions contractuals amb tercers.

Responsabilitat i control:

- Designació d'un responsable únic i sota aquest, responsables de cada àrea (drets individuals, drets a la propietat, drets a qualitat de sistemes, drets a qualitat de vida).
- Definició de responsabilitats de control, auditories i administració.
- Detallar les responsabilitats legals de cada perfil laboral.

Qualitat dels sistemes informàtics:

- Descripció dels nivells generals de qualitat de les dades i el marge d'error tolerable, amb especificacions detallades per a projectes específics.
- Exigència que tots els sistemes informàtics tracten d'estimar la qualitat de les dades i les possibilitats d'error en els sistemes.

Qualitat de vida:

- Establir que el propòsit dels sistemes és millorar la qualitat de vida dels clients i els empleats a aconseguir alts nivells de qualitat en els productes, en el servei als clients, la satisfacció dels empleats, l'ergonomia dels llocs de treball i usabilitat d'aplicacions, en el flux de treball.
- Establir un desenvolupament adequat de la gestió de l'ús de recursos humans.
- Mantenir de forma clara els límits entre família, treball i oci.

Una figura polèmica. Hackers, hacking

No és possible parlar d'ètica informàtica i oblidar aquesta figura que no deixa indiferent ningú. Els mitjans de comunicació l'enalteixen i embruten; s'odia i s'estima. S'interpreta com un fet bo, i com un fet dolent, i això ve de lluny. De fet, en el clàssic de Stoll, *The Cuckoo's Egg* ("L'ou del cucut"), llibre que va donar el tret d'eixida a aquest tipus de qüestions, podem llegir un paràgraf que resulta clarificador en extrem (Stoll, 1990):

> *"Per a Dennis l'assumpte del hacker era un problema d'ètica social.*
>
> *—Sempre hi haurà alguns cretins ficant el nas en la nostra informació. Em preocupa que els hackers enverinen la confiança sobre la qual s'han construït les nostres xarxes. Després de molts anys intentant connectar un munt d'ordinadors entre si, un grapat d'imbècils poden tirar-ho tot a rodar."*

Des del principi, des que algú es va considerar hacker, van aparèixer els codis ètics propis. A vegades escrits de forma rigorosa, unes altres mers comentaris en grups de *news* o fòrums, però amb punts de partida que poden continuar vigents. Dudley els revisa des de 1984 i d'aquest prenem algunes claus (Dudley, Bramen, & Vincenti, 2012) com que tota informació ha de ser lliure i disponible per al públic, fins i tot el dret a accedir als documents confidencials del govern. Després de revisar la situació una dècada més tard, apareixen elements que ens són coneguts per formar part de qualsevol codi ètic informàtic d'avui, com ara protegir la privacitat o ajudar la seguretat, i altres elements que ens poden semblar d'una actualitat tremenda avui, com són la necessitat de compartir, i fins i tot procurar, que els recursos dels equips no es balafien. Apareix una sèrie d'activitats prohibides, que delimiten qui pot ser considerat un hacker i qui no: no s'ha d'emprar programari nociu, robar...

Lluny queden ja aquelles reunions de Black Hat, mogudes per gurus de la informàtica de l'època on, malgrat el nom, es tractava de reunions de "barret blanc", o "ètic", on els hackers participants eren persones que treballaven (quan no ho eren ells mateixos) per als directors d'informàtica i caps de seguretat informàtica de bancs i quasi tot tipus imaginable de gran empresa (i moltes de grandària mitjana). Les empreses de programari ja pensaven en aquestes com en reunions de xicons dolents, però encara que Bill Gates i Steve Jobs clamaren a Déu denunciant com a il·legal la cerca i exposició dels defectes dels seus productes, no era un crim. Ho seria si s'utilitzara el mètode desenvolupat (l'explotador o *exploit*) per a utilitzar el defecte que ha descobert en el programari (la "vulnerabilitat") i emprar-lo contra una xarxa corporativa o el govern ("el blanc") (Clarke & Knake, 2010).

En aquest sentit convé portar unes línies d'un dels hackers més famosos de tots els temps, Mitnick (Mitnick & Simon, Ghost in the wires, 2011):

> *"Han passat onze anys des que vaig eixir de la presó. He organitzat una consultoria que em proporciona un flux constant de negoci. M'ha portat a cadascun dels Estats Units i a tots els continents excepte l'Antàrtida. El meu treball avui és, per a mi, si més no un miracle. Intente cercar alguna activitat il·legal que, efectuada amb permís, es puga dur a terme de forma legítima i beneficiar tothom. Només se'm va ocórrer una: el* hacking *ètic.*

> *Vaig estar a la presó pel* hacking*. Ara la gent em contracta per a fer les mateixes coses per les quals vaig anar a la presó, però d'una manera legal i beneficiosa. En els anys transcorreguts des del meu alliberament he sigut orador principal en incomptables esdeveniments de la indústria i les empreses, he escrit per a la* Harvard Business Review*, i he sigut professor a la Facultat de Dret de Harvard. Cada vegada que algun hacker apareix en les notícies, em demanen que comente la notícia en la Fox, CNN o uns altres mitjans de comunicació. He aparegut en* 60 Minutes*,* Good Morning America*, i molts, molts altres programes. Fins i tot he sigut contractat per agències governamentals, com ara la FAA, l'Administració de la Seguretat Social, i malgrat el meu historial penal, en una organització del FBI, InfraGard."*

Confirmant el paràgraf precedent, el mateix assumpte que es mesura com dolent dolentíssim apareix després com una cosa que atorga valor. O, com deia el Marqués de Campoamor: "Res és veritat, res és mentida. Depèn del color del vidre amb què es mira".

Aquesta mateixa doble moral la veiem en un altre fragment d'un altre llibre de Mitnick. (Mitnick & Simon, 2007) en què valora l'actuació d'un hacker que, després d'entrar en un sistema, avisa de les vulnerabilitats:

> *"En el cas d'Adrian, el fiscal va optar per no reparar en què les companyies van saber-ne la vulnerabilitat als atacs perquè el mateix Adrián els en va informar. En tots els casos, ha protegit les empreses en informar-les que els seus sistemes tenen fallades de seguretat i esperant que les hagen solucionades per a després permetre que les notícies de les intrusions es publicaren. No hi ha dubte que ha violat la llei, però ha actuat (almenys en el meu llibre) amb ètica".*

Tipologia

Establir una tipologia sempre és difícil. Potser el més efectiu, seguint Joyanes (Joyanes Aguilar, 2010), siga fer una classificació atenent-ne la motivació, que pot passar des d'una mira alta, com ara cercar un canvi social o polític, a metes més prosaiques, com és obtenir un benefici econòmic. L'ampli ventall, del polític o militar a satisfer el propi ego queden coberts. Una altra possibilitat és atendre'n l'objectiu: individus, empreses, governs, infraestructures, sistemes i dades de tecnologies de la informació; o el tipus d'aquestes últimes: públiques o privades. Per descomptat, cal ressenyar el mètode que empren: injecció de codi nociu, ús de virus, cucs, troians, etc.

Atenent-ne l'autoria podríem parlar de (Joyanes Aguilar, 2010):

- Atacs patrocinats per estats, incloent-hi casos d'espionatge industrial, o des dels mateixos estats, com els perpetrats pels serveis d'intel·ligència i contraespionatge.
- Efectuats per terroristes o extremistes politicoideològics.
- Realitzats per la delinqüència organitzada, la màfia.
- Els més comuns: atacs de perfil baix, realitzats per persones amb coneixements variables.

Quant a la tipologia d'amenaces, també segons Joyanes, trobem una àmplia bateria, de la qual destaca (Joyanes Aguilar, 2010):

- DDoS. (Distributed Denial of Service o atac de denegació de servei distribuït): Tot un clàssic, que cerquen fer caure serveis com ara el web. Poden realitzar-se utilitzant xarxes d'ordinadors prèviament infectats per virus (xarxa de zombis o *botnet*), que són còmplices involuntaris.
- Xarxes de zombis: xarxes d'ordinadors zombis, usats per a enviar correu brossa o *spam*, espiar dades bancàries... El nombre d'ordinadors zombis al nostre parc és, senzillament, alarmant.
- Zeus: Parlàvem dels virus de xarxa de zombis (troià). En concret aquest recopila informació de l'usuari, que la utilitza per a suplantar-ne la identitat. Des de novembre de 2010 se n'ha detectat l'arribada a dispositius mòbils, que inunden xarxes socials.
- Unes altres amenaces futures: Queden obertes dues àrees d'impacte, l'una, l'enginyeria social, serà visitada si més no breument en aquest mateix tema, i, l'altra, els atacs multivectorials, una lògica evolució basada en la combinació de diferents tipus de suport com a atac: correu electrònic, missatges en blogs, xarxes socials...
- Stuxnet: Està bé referenciar-lo, perquè ens serveix d'avís previ al que denominarem *ciberguerra*. Es tracta d'un troià que aprofita una vulnerabilitat dels sistemes operatius Windows CC, emprats en els sistemes SCADA (Supervisory Control and Data Acquisition) utilitzats en infraestructures crítiques, com ara el control d'oleoductes, plataformes petrolieres, centrals elèctriques, centrals nuclears i altres instal·lacions industrials amb l'objectiu de sabotar-les. Òbviament, no va orientat a ordinadors domèstics sinó que està pensat per a atacar infraestructures crítiques o fins i tot sabotatges industrials. Una mostra del que desgraciadament trobarem.

Hi afegim un factor. La informàtica avança molt de pressa. En els anys noranta un telèfon intel·ligent era un somni de ciència-ficció. No fa molt, el núvol, les dades massives o la intel·ligència artificial com la coneixem ni tan sols les haguera considerades la ciència-ficció (un incís: quan llegisc els clàssics de la ciència-ficció amb el meu lector electrònic o *e-reader*, cerque referències d'algú que anticipara que hom llegiria aquest text o uns altres amb aquest tipus de dispositiu..., sense èxit). I ja que hem esmentat el núvol..., pensem en una carpeta compartida en aquest, per deu usuaris. Si un d'ells col·loca una foto pederasta, tots els usuaris, en el moment que l'aplicació d'escriptori actue sincronitzant amb el disc local, estaran violant la llei. Aquest tipus d'innovacions disruptives, com les anomena Joyanes (Joyanes Aguilar, 2010), tenen un fort impacte en la seguretat. També acaba ressenyant com a elements de risc la realitat augmentada i la Internet de les coses.

Cal fer un recordatori en aquests moments: les figures i termes que en aquest tema s'empren tenen, és obvi, un prisma ètic i deontològic, però també un de marcadament legal, amb dues referències ineludibles: el Codi Penal i l'Esquema Nacional de Seguretat.

Per no deixar de portar a col·lació l'anomenat *hacking* ètic, i seguint Himanen (Himanen, 2004), podem considerar per damunt de l'ètica hacker que ho relaciona al treball i als diners a l'anomenada *nètica* o ètica de la xarxa. Amb aquesta expressió al·ludim a la relació que el hacker manté amb les xarxes de la nostra actual societat. Es tracta d'un terme a no confondre amb l'habitual de *netiqueta* (que inclou principis de conducta com ara "evitar expressions inadequades", "no usar majúscules", etc.). Aquesta relació del hacker amb les xarxes de comunicació de la nostra societat es remunta a l'origen de l'ètica hacker, en la dècada de 1960,

la nètica, però va rebre un fort impuls el 1990 quan es va reformular a través de l'Electronic Frontier Foundation, per Mitch Kapor (creador del full de càlcul Lotus) i John Perry Barlow, des d'on es va intentar potenciar els drets del ciberespai.

Elements d'interès

A manera de calaix de sastre, hi ha dos elements que no podem deixar de tractar ací: l'anomenada enginyeria social i l'últimament tan de moda ciberguerra.

Enginyeria social

Obrim l'epígraf amb una referència de Mitnick que ens servirà per a aprofundir no solament en la doble moral que sembla traslluir-se..., sinó en el dubte de si és millor o pitjor enganyar màquines o éssers humans: (Mitnick & Simon, 2007)

> *"Mentre Mudge únicament va utilitzar mètodes tècnics en l'atac que ens ha descrit, Dustin va usar també l'enginyeria social. Encara que ell no se sent molt còmode per això. No té cap objecció en els aspectes tècnics del treball i admet gaudir cada moment d'un projecte. Però quan ha d'enganyar la gent, cara a cara, se sent violent.*
>
> *He intentat analitzar per què és així. Per què un mètode em descompon i un altre no m'afecta en absolut? Potser ens han educat per a no mentir a la gent, però no ens han ensenyat ètica informàtica. Estic d'acord que, en general, tenim menys objeccions a enganyar una màquina que a enganyar una persona.*
>
> *Així i tot, malgrat els dubtes, normalment sent la càrrega d'adrenalina sempre que supera un episodi d'enginyeria social que discorre sense problemes".*

La idea bàsica que sustenta l'enginyeria social és la següent: en molts casos, és més fàcil i eficaç enganyar les víctimes perquè ens donen la informació que volem que robar-li. L'engany que es produeix és psicològic, més que tecnològic, que requereix habilitats en àrees com són la psicologia i la lingüística que combinen amb els seus coneixements d'informàtica (Kshetri, 2010). L'home és la baula més feble de la cadena que representen les tecnologies de la informació i, per tant, la més susceptible a trencar-se. L'enginyer social el pren de blanc i això provoca reaccions enfrontades. Des del camp de la psicologia, Mitnick (Mitnick & Simon, 2007) ens porta una cita del Dr. Brad Sagarin, psicòleg social, que diu: "L'enginyer social empra les mateixes tècniques de persuasió que utilitzem tots els altres diàriament. Adquirim normes. Intentem guanyar credibilitat. Exigim obligacions recíproques. Però l'enginyer social aplica aquestes tècniques d'una manera manipuladora, enganyosa i molt poc ètica, sovint amb efectes devastadors."

Hi ha múltiples maneres d'aconseguir aquestes finalitats. (Hadnagy, 2011) ens parla, per exemple, de la reciprocitat. Es tracta d'un fet inherent a l'expectativa que tots tenim a ser ben tractats quan som amables amb els altres. Això és més important del que sembla perquè sovint el favor es retorna inconscientment. Un altre factor important, també segons Hadnagy, serien els incentius ideològics. Cada persona té uns ideals i creences[6] diferents als dels altres, i

[6] Els somnis i les creences poden ser una qüestió tan arrelada en una persona que separar-ho d'aquesta persona pot ser quasi impossible. Quan s'escolta la frase: "Tinc un somni ", la ment ens porta a pensar en Martin Luther King, així com quan sentim "No tingueu por", pensem en Joan Pau II. Entorn d'aquests

aquests afecten aquesta definició. Si el somni de la teua vida és dirigir una empresa d'informàtica orientada a la gestió, llavors aquesta és la teua passió, que provocarà que treballes més hores i més intensament que qualsevol altre empleat, i possiblement ho fas per menys diners, ja que és la teua motivació, mentre que per als altres és només un treball del qual eixir com més prompte millor. Les hores extres mal cobrades et pesaran menys. Sabràs que t'exploten, però et doldrà menys.

Atès que la gent és, doncs, argila emmotllable, com hem vist, comprendrem que la tasca de l'enginyer social es pot fer més fàcil o més difícil. Fàcil, perquè pasta una argila ja ablanida, o difícil, si intenta remar a contra corrent.

Per a tancar l'apartat, cal destacar una activitat professional nova que sorgeix referent a l'existència de l'enginyeria social: l'auditoria d'enginyeria social. Es tractaria de la situació on un professional és contractat per a posar a prova les persones, les polítiques i el perímetre físic d'una empresa mitjançant la simulació dels mateixos atacs que un enginyer social maliciós usaria. Les dues principals diferències entre un enginyer social maliciós i un auditor professional són les següents: l'auditor professional sempre tractarà d'ajudar i no avergonyir, robar o danyar un client i aquesta és la que més ens interessa a nosaltres, on l'auditor professional seguirà les pautes morals i legals existents (Hadnagy, 2011) (Mitnick & Vamosi, 2018)

Ciberguerra

Parlem ara, encara que breument, d'un fenomen a mig camí entre el *hack* i la seguretat de l'estat: la ciberguerra. Des del Ministeri de Defensa d'Espanya, Joyanes recorda una cosa que nosaltres ja coneixem per Clarke: (Joyanes Aguilar, 2010) (Clarke & Knake, 2010): Richard Clarke preveu o s'imagina una fallada catastròfica "en qüestió" de quinze minuts. S'imagina que els errors dels ordinadors portaran a la caiguda dels sistemes de correu electrònic militar; les refineries i els oleoductes explotaran, els sistemes de control de trànsit aeri es col·lapsaran; els trens de passatgers i de càrrega i els metros descarrilaran; les xarxes elèctriques dels Estats

---

nous tòtems humans es configuren grups relativament pròxims en pensament, on es mouen persones amb tendències similars. La gent tendeix a ser atreta a altres persones amb somnis i objectius semblants, "Déu els cria i ells s'ajunten", que diu el refranyer, però també és un factor que els converteix fàcilment en manipulables. I a vegades no és necessari que hi haja aquest tòtem o nexe d'unió, perquè es pot fabricar. Així, el domini que la casta política posseeix dels mitjans de comunicació en un camí accelerat a la neollengua d'Orwell en el seu tristament profètic *1984*, converteixen la gran massa en un grup de persones amb pensament pla. Persones que tenen idees afins, la major part de les vegades generades a través d'una refinada rentada de cervell que s'executa de forma invisible, van fent més gran el factor d'iniciació a aquesta nova marea humana: l'espiral del silenci creix, de tal manera que quan algú sap en el seu fur intern que el que l'envolta està equivocat, no parla, per a no ser assenyalat com el dolent de la pel·lícula o, usant el vocabulari de nou encuny, el "terrorista" o "el feixista", i acaba sent un més confós en la massa. Unes poques consignes, o discursos emotius, podran enfervorir o fer vessar llàgrimes al conjunt de persones de manera que participen sense dolor i regalen part dels diners guanyats amb esforç. Els seus ideals han sigut canviats, manipulats, sense recórrer al que en altres moments històrics era l'eina comuna: la por. Encara que cal reconèixer que no són una novetat: en l'educació, per exemple, s'ha usat des de fa segles per a ensenyar als infants a través de contes i rondalles amb un significat ocult o moralitat: Hans Christian Andersen o els germans Grimm són excel·lents exemples. Avui podem veure picades d'ullet en la comercialització, on s'usen anuncis "afins als nostres ideals": recordem la campanya d'Ikea que, en un moment en què la monarquia tenia una taxa de popularitat baixa, va usar com a lema "La república independent de ma casa".

Units cauran; les òrbites dels satèl·lits quedaran fora de control. I el fet pitjor de tot: la identitat de l'atacant pot ser un misteri.

Aquesta situació que descriu Clarke, en un escenari catastròfic respecte als EUA i la Xina, no està tan desencaminada. Els serveis secrets dels EUA fa temps que van divulgar l'existència de manuals de *guerra il·limitada* que defineixen com havien d'actuar-ne els informàtics especialitzats sobre aquest tema.

Estem parlant d'atacs dirigits des de dalt, encara que no cal descomptar l'ajuda d'*espontanis*, com assenyala (Libicki, 2009) els atacs poden provenir de tercers, fet que generarà més confusió encara. Això sol ocórrer quan la tensió entre dos estats es deixa veure a la societat en general, com va passar, recordem, amb el succés de l'illa Perejil entre el Marroc i Espanya. Això legitimaria èticament els atacs dels hackers que se sentiren més o menys patriòticament insuflats pels vents de guerra.

Un matís intermedi és la ciberdissuasió (Libicki, 2009), que es tracta d'un estadi anterior, on amagar la mà sense arribar a tirar la pedra. Espantar. Amb la ciberguerra un estat podria atacar, patirà represàlies, i viurà per a atacar un altre dia, amb la dissuasió intentaríem que no arribara a atacar. També és simètrica, ja que es duu a terme entre iguals. Des d'un punt de vista moral, el que pren represàlies no està *a priori* a un nivell moral més alt que l'altre. No cal pensar que l'objectiu últim és guanyar (p. e. en un conflicte nuclear), sinó la mateixa dissuasió. Per a deixar clares les diferències entre ciberguerra i ciberdissuasió, veiem la taula següent, basada en (Libicki, 2009)

Taula 6. Diferència entre ciberguerra i ciberdissuasió. Adaptat de Libicki.

Pregunta	***Ciberdissuasió***	***Ciberguerra***
Qui ho va fer?	No es pot saber sobre qui exercir represàlies en contra seua.	L'objectiu ha sigut ja seleccionat per altres raons.
Ens posa en risc?	No se sap. L'efecte desitjat és impedir-ho.	És important saber-ho, però no crític, per a justificar i donar forma a un major esforç.
Es produeix diverses vegades?	No es pot saber si la represàlia és repetible.	Afectarà la intensitat de l'esforç a través del temps.
Intervenen tercers?	Poden interferir en els *avisos*.	Poden incrementar la gestió de l'escalada de tensió.
Fem arribar el missatge correcte?	La política de dissuasió pot crear un risc moral.	La càrrega moral ja s'ha acceptat.
Hi ha un llindar a no traspassar?	Pot interferir en el desenvolupament.	Els llindars més importants ja s'han traspassat.
Evitem la tensió?	Fent-ho reduïm la credibilitat de	La ciberguerra és ja més que la

	les represàlies.	intensificació de la tensió.
Val la pena "colpejar"?	La represàlia pot ser fútil.	Sí, si podem cobrir una sèrie d'objectius.

Trastorns i malalties derivades de les TIC

Les TIC no solament es poden estudiar des del prisma què succeeix amb els actes del treballador, i com aquests poden afectar-ne el treball o els altres, i no hem d'oblidar que pot tractar-se el cas invers: com el treball pot afectar el treballador, bé físicament o psíquicament (Edgar, 2003) mitjançant elements com són el tecnoestrès i les anomenades *tecnomalalties* (*technomalady*: problemes musculars, mal d'ulls, vòmits...).

Són de sobres coneguts els riscos per a la salut, tant per l'agreujament de problemes existents com per l'aparició de nous. Posem per exemple les lesions per esforç repetitiu (el tipus més comú relacionat amb l'ús d'ordinadors és la síndrome de túnel carpià) o la síndrome de visió de computadora (CVS): qualsevol condició de fatiga ocular relacionada amb l'ús de les pantalles.

De les desconegudes fins a l'aparició de les TIC en la vida quotidiana, destaquen el *tinnitus* o acufen (escoltar brunzits, sentir timbres fantasma de mòbil, notificacions que no existeixen), la nomofòbia (la por d'eixir al carrer sense telèfon) o el tecnoestrès (estrès induït per l'ús d'ordinadors), per exemple per arribar a esperar que les altres persones i institucions humanes es comporten com ordinadors, donen respostes instantànies, estiguen atents i demostren una falta d'emoció. Altres síndromes relacionades serien la ignorància (la informàtica és una caixa negra, se sap què es fa però no com es fa), el de la complexitat (és un món tan complicat que és impossible entrar a explicar-li'l i molt menys posar normes) o el de realitat virtual (com que el que hi ha a Internet no existeix, per quina raó preocupar-nos-en?).

La por del canvi no ha de ser menyspreada tampoc. Tenim una visió, potser més heretada de les pel·lícules que de la realitat, del gran inventor que de colp ho revoluciona tot i genera amb el seu portentós cervell invents dignes dels inquilins de l'Olimp. Sobre això s'ha discutit molt. Ja en "l'evolució de la tecnologia" George Basalla rebutjava aquesta visió i apostava, en canvi, per la concepció darwiniana del canvi gradual. Basalla documenta que l'aparició dels invents cèlebres (dels quals destacarem, entre d'altres, el transistor i la màquina de vapor) no són més que el resultat de nombrosos canvis successius menors o, millor, de la combinació de petits elements ja existents. Potser una pedagogia basada en aquests pressupostos seria suficient per a combatre aquesta resistència que es presenta en forma de por pel canvi.

Una altra categoria es podria enfocar entorn de les patologies sexuals. En aquest assumpte, seguim (Smoller, 2014) de forma íntegra. Jordan Smoller es planteja la idea que Internet ha provocat un augment de la pedofília, sobre si aquesta i unes altres parafílies són molt comunes. I es respon que realment no ho sabem. Si anem porta a porta preguntant si l'atrauen, diguem-ne, els infants de 8 anys, no ho reconeixerà ningú. De fet no ho diuen fins que són detinguts, i fins i tot després ho continuen negant. Smoller creu impossible realitzar un estudi epidemiològic sobre aquest tema, però on sí es manifesta és entorn d'una altra expressió sexual a Internet: el fetitxisme. Internet està plena de webs amb xarxes socials de

fetitxistes. Esmenta un estudi per a intentar esbrinar quin és el fetitxe més comú, i empra Yahoo per a rastrejar Internet a la recerca de grups de debat relacionats amb el fetitxisme, que va donar com a resultat 400 grups amb milers de membres cadascun, i després de classificar-los es va trobar un clar guanyador: els fetitxes relacionats amb els peus polvoritzen la competència i sumen un 47% dels fetitxes relacionats amb el cos, seguits per un 9% relatius als fluids corporals. En el cas dels objectes inanimats, quasi un terç d'aquests grups parlaven de sabates.

Smoller continua avançant amb una reflexió objectiva: en els últims anys del segle passat es va produir un fet que va conduir a un canvi sense precedents en l'experiència sexual humana: per primera vegada en la història milions de persones podien veure unes altres realitzant l'acte sexual. Havia arribat Internet. Però això no és un canvi radical, una aportació nova a la humanitat, perquè l'auge de la pornografia a Internet no és més que l'últim capítol de la història entrellaçada de la tecnologia i l'estímul sexual. Posa com a exemple l'anomenada *escatologia telefònica* (telefonades sexuals). Ací hi ha un trastorn psiquiàtric que només va ser possible amb la invenció del telèfon. Amb l'avanç de la tecnologia de la comunicació el telèfon ha quedat desfasat, i hi ha indicis que l'escatologia telefònica es va fent menys comuna, perquè hi ha uns altres mitjans per a ocupar-ne el lloc (els missatges eròtics, l'anomenat *sèxting*).

Com s'anticipava, no resulta un fet nou. Smoller insisteix que la història de l'evolució conjunta de la conducta sexual i la tecnologia es remunta a molt abans. La invenció de la impremta en el segle XV va permetre la difusió de llibres i fullets obscens. En el segle XIX va arribar la fotografia, que va inundar el món d'un nou tipus d'imatgeria sexual, i per descomptat en el segle XX el cinema, la televisió i el vídeo familiar van crear tota una indústria de la pornografia que entrà a les nostres cases. Encara que reconeix que pel seu descomunal abast, volum i varietat el web no té parangó com a mitjà de difusió de la pornografia.

De la robòtica a la intel·ligència artificial, un canvi d'ètica?

Dudley (Dudley, Bramen, & Vincenti, 2012) planteja que atesa la dificultat per als usuaris mitjans, l'home del carrer, a interpretar les lleis, s'obrin dues possibilitats per al legislador: l'una, crear lleis de fàcil lectura i sense ambigüitats perquè siguen fàcilment comprensibles per tots els usuaris del ciberespai i, l'altra, codificar la mateixa llei en els programes d'ordinador de manera que els usuaris queden protegits. Una deriva extrema que ja s'aplica, com prompte veurem, és que la justícia s'exercisca mitjançant màquines dotades d'intel·ligència artificial que puguen substituir el jutge.

La veritat és que els documents legals, per simples que siguen, poden no arribar a llegir-se mai. Pensem quants de nosaltres llegim unes simples condicions de servei, les TOS. Fet que ens porta a valorar la segona part: la informatització de les lleis. El principi fonamental seria evitar danys als usuaris, cosa que dins de l'ètica en general ens porta a l'ètica de la màquina en concret.

L'ètica de la màquina definiria, sempre segons Dudley, com s'han de comportar les màquines amb els usuaris humans i amb altres màquines, que posa l'èmfasi a evitar el mal i altres conseqüències negatives de les màquines autònomes o programes d'ordinador sense control. L'estudi d'aquesta part de l'ètica cada vegada té més ressò al si de la UE, com ho mostra la

Declaració sobre Intel·ligència artificial, robòtica i sistemes “autònoms” (Comissió Europea. Grup Europeu sobre Ètica de la Ciència i les Noves Tecnologies, 2018) i uns altres documents interessants fàcilment localitzables mitjançant EURLEX (EUR-Lex, 2019).

De base es parteix de la idea que per a construir màquines ètiques abans hem d'entendre com els éssers humans empren l'ètica en la presa de decisions, i després tractar de traspassar aquestes conductes a les màquines. Com tot, arrossega avantatges i inconvenients. Com a avantatges obvis, en tractar-se de màquines que no necessiten menjar o dormir, tindríem la disponibilitat permanent i, per descomptat, la seua *freda* impassibilitat. A més, la seua gran capacitat de treball ens proporcionaria, per al cas d'haver de valorar diferents supòsits en dilemes ètics, una gran capacitat per a simulacions i la no-existència de límits sobre el nombre de casos avaluats. Per contra, apareixen problemes, perquè crear nous conjunts de regles específiques, o adaptar les existents als casos que es presenten, genera un coll de botella que és molt conegut en els sistemes d'intel·ligència artificial. A més, és necessari determinar els punts claus de l'ètica i lleis que s'estan incorporant dins d'un sistema i, qui vigila el vigilant? (Dudley, Bramen, & Vincenti, 2012). Per aquest motiu, la UE busca la construcció d'un marc ètic i legal comunament i internacionalment reconegut per al disseny, producció, ús i governança de la intel·ligència artificial, la robòtica i els sistemes “autònoms”. (Comissió Europea. Grup Europeu sobre Ètica de la Ciència i les Noves Tecnologies, 2018)

Els elements que preocupen són molts i diversos, des dels automòbils que no necessiten un conductor, els drons autònoms, robots exploradors, bots financers i el diagnòstic mèdic assistit per aprenentatge profund (*Deep Learning*), així com la intel·ligència artificial (IA) en la forma d'aprenentatge automàtic (*Machine Learning*), la mecatrònica avançada (una combinació de IA, aprenentatge profund, ciència de dades, tecnologia de sensors, Internet de les coses i les enginyeries mecànica i elèctrica), l'increment de la interacció entre els humans i les màquines (com en el cas de les interfícies cervell-computadora i els ciborgs) i el Big Data o dades massives, entre d'altres. D'això deriva la preocupació de la UE (Comissió Europea. Grup Europeu sobre Ètica de la Ciència i les Noves Tecnologies, 2018), per les conseqüències com ara la redefinició del concepte de treball, la millora de les condicions de treball i la reducció de l'aportació i la interferència humana durant les operacions.

Professionals i IA

El test de Turing, de primer anomenat joc de la imitació, va ser publicat en *Computing Machinery and intelligence*, 1950 (Latorre Sentís, 2019). Durant dècades ha sigut l'element clau per a poder verificar si una IA era similar a la humana. Amb aquesta imatge tan gràfica al cap, tendim a oblidar que Turing, que els programadors, que els creadors de les IA, són humans, i no solament humans, sinó professionals de la informàtica i ciències relacionades.

Els programes que originen l'embrió estan escrits per programadors, amb un treball que no és senzill. Latorre subratlla que per a molts empresaris aquest treball no és rellevant, la qual cosa és un error greu. Que un sistema informàtic funcione, avui dia, depèn de la bona preparació de la persona que ho estableix i gestiona. Si anàrem a prendre un avió on sabérem que el pilot té tendències suïcides, ens ho pensaríem. De manera similar, respecte al programador n'hem de comprendre en tot el possible la manera de pensar i procedir. (Latorre Sentís, 2019)

Però detinguem-nos en aquest punt, i posem l'accent en alguna cosa que acabem de dir: els programes que originen l'embrió de la IA. Perquè, ara com ara, aquests sistemes ja es retroalimenten i milloren sols, que donen alhora més capacitat, però també més opacitat, en no saber exactament què fan les noves línies de codi. Sovint es deia: "no existirà mai una màquina que siga capaç de fer aquesta o aquella altra cosa"; "una màquina no sabrà mai més que el seu constructor"; "sempre serà necessari un home per a conduir, vigilar o reparar la màquina". De totes les proposicions, aquesta és la més falsa de totes. (David, 1973)

Referent a això, pensem en alguns exemples que ens dona la mateixa (Comissió Europea. Grup Europeu sobre Ètica de la Ciència i les Noves Tecnologies, 2018): Google Brain desenvolupa una IA que pel que sembla construeix unes altres de la seua mateixa naturalesa millor i més ràpidament que els humans. Pensem també en AlphaZero i els escacs o AlphaGo i el Go, que expliquen amb pocs elements què és això de l'aprenentatge profund i els anomenats "enfocaments de xarxes generatives antagòniques" (*generative adversarial networks*), màquines que *s'ensenyen* a si mateixes noves estratègies i adquireixen nous elements per a ser incorporats en les seues anàlisis. Això, com hem anticipat, i que resulta un fet que causa preocupació a la Comissió Europea, provoca que les accions d'aquestes màquines es tornen indesxifrables i escapen de l'escrutini humà, tant perquè és impossible esbrinar com es generen els resultats més enllà dels algorismes inicials, com perquè el rendiment d'aquestes màquines es basa en les dades utilitzades durant el procés d'aprenentatge i aquestes poden no estar disponibles o ser inaccessibles. Però encara hi ha més: si aquests sistemes usen dades amb biaixos i errors, és molt difícil tornar arrere.

Presa de decisions per la IA

Hi ha decisions que prenem els humans i que causen rebuig en general en considerar que puguen ser preses per les màquines. Per a portar-ho a l'esfera més alta, el govern de les nacions. Hem vist com es reparteixen els poders dins d'un estat: els parlaments legislen, els governs (poder executiu) executen les lleis i els jutges en supervisen el compliment. I si alguna d'aquestes coses ho fera una intel·ligència artificial? Apareixen veus que diuen que no solament podríem fer-ho, sinó que hauríem, per a obtenir els mateixos avantatges que ja es reben, o almenys s'albira per la seua proximitat, en l'assistència a operacions mèdiques, la conducció de vehicles o generació de noves medicines, amb un factor que en fa més desitjable l'aplicació: erradicar la corrupció i eliminar les influències no justificables de *lobbies*. (Latorre Sentís, 2019)[7]

En el cas dels jutges, els primers passos ja s'han donat. Als Estats Units s'empra IA per a ajudar a establir fiances o estimar el risc de certes decisions judicials. El programari emprat rep el nom de *Public Safety assessment*, avaluació de risc públic. És obvi que el sistema anglosaxó basat en la jurisprudència és un bon candidat a ser emprat de forma eficient per intel·ligències artificials. (Latorre Sentís, 2019)

[7] Hi ha una sèrie de consideracions sobre la condició inherentment política de la tecnologia que ens fa (Colmenarejo Fernández, 2017):

- Les innovacions tecnològiques, lluny de ser neutrals, sempre estan orientades a un fi polític.
- Les tecnologies es veuen afectades des del punt de vista social i per aquest i no com un factor independent.

Però ens queda plantejar la medul·la de la qüestió: més enllà de quina ètica programar... Qui la decideix? I encara més. Qui escriu aquestes subrutines?

Veurem la importància d'això amb un exemple. Imaginem dos treballadors d'un hospital que escriuen un programa perquè subministre dades a la intel·ligència artificial que analitza les imatges de la ressonància magnètica i determina la localització de determinats tipus de tumor. Pep i Paquita, que així es diuen els nostres subjectes d'estudi, tenen obert un litigi contra l'hospital per impagament d'hores extres, així que a Pep se li ocorre que pot amagar en el codi una subrutina que li permeta alterar les dades des de qualsevol terminal de consulta de l'hospital, mitjançant una pulsació determinada de tecles. Aquestes dades alterades forçarà un 15% de diagnòstics incorrectes, una quantitat prou baixa per a no ser detectada de seguida. L'hospital acaba enfrontant-se legalment amb ells i, després d'un judici que li és favorable, els acomiada. Pep posa en marxa el seu codi. En un any, deu pacients moren per un diagnòstic equivocat. Com era l'ètica de Pep? Realment d'un perfil molt baix, perquè va menysprear la vida humana. Però algú hauria d'haver supervisat el codi? Paquita va poder veure alguna cosa i callar? Tot responsable ha de ser identificable, així que la resposta a la primera pregunta és òbvia: sí. Tot codi ha de ser revisat i, en la mesura possible, els algorismes han d'operar amb un codi públic, visible. La idea del codi obert sembla xocar amb els interessos comercials, però cal trobar un equilibri. Almenys per a poder seguir la traçabilitat i, per descomptat, si parlem d'intel·ligències artificials que es corregeixen soles. (Barrio Andrés, 2018)

Però no fa falta pensar tan sols en decisions d'alt impacte. També afecta el nostre dia a dia. Hi ha múltiples evidències d'una inevitable emancipació de les màquines enfront de l'ésser humà, sense anar més lluny, l'ús de Google[8], Facebook o Spotify que s'han emancipat ja de la memòria humana, atès que la sotmeten i poden arribar a conformar la nostra pròpia identitat, d'acord amb paràmetres que no elegim nosaltres. Considerem algorismes que trien per nosaltres continguts de la nostra biografia i que semblen saber més de nosaltres que nosaltres mateixos, no solament en el nostre passat si no, i ací més probablement, dels nostres desitjos futurs. I no solament parlem de memòria: les màquines s'han emancipat ja de la intuïció humana. Pensem en la diferència que podem comprovar entre fer una passejada guiats per Google Maps o deixar tan sols que la ruta acabe tan lluny com els peus ens porten. Memòria, intuïció. Queda res per sotmetre? Doncs sí, els nostres sentits, que sucumbeixen davant l'encanteri de les ulleres de realitat virtual o videojocs amb realitat augmentada. (Colmenarejo Fernández, 2017)

Sistemes autònoms

Des d'una perspectiva ètica, és important tenir en compte que (Comissió Europea. Grup Europeu sobre Ètica de la Ciència i les Noves Tecnologies, 2018) l'autonomia només pot ser

[8] Sobre el botó d'apagada de Google, cal incloure una reflexió de Latorre, que és molt encertada: Tots els perills inventats en la ciència-ficció poden ser irrellevants. Per contra, no som capaços de comprendre quines terribles conseqüències tindria una irrupció abrupta de la intel·ligència artificial avançada. En aquest sentit, Google ja ha establit un botó d'apagada de tots els algorismes avançats que utilitza. Està a les mans d'aquesta empresa tallar l'enorme flux de processament d'informació que ens assisteix. Crec que fa tanta por el descontrol de la intel·ligència artificial com deixar de tenir-la. Viuríem en una gran ciutat sense aigua, sense electricitat, sense cotxes? Durant la gran apagada de 1977, la ciutat de Nova York es va convertir en un caos, on les més baixes passions humanes es van desfermar. Caldria evitar usar el botó d'apagada de la intel·ligència artificial avançada, pel nostre bé.

atribuïda als éssers humans, però l'ocupació extensiva del terme tant entre el públic en general com entre la comunitat científica en particular, per a fer referència al grau més alt d'automatització i d'independència dels éssers humans en termes d'*autonomia* operativa i de presa de decisions, provoca que tendim a oblidar aquesta única atribució possible. Però, per al nostre estudi, ja que un sistema intel·ligent no puga ser considerat *autònom* en el sentit ètic, ens indica que no pot ser considerat tampoc titular de la moralitat i dignitat humanes. Això, per part seua, implica que els humans hem de continuar mantenint el control en els àmbits que concerneixen els éssers humans i el seu entorn i així poder continuar decidint en (Comissió Europea. Grup Europeu sobre Ètica de la Ciència i les Noves Tecnologies, 2018) qüestions tan importants com són els valors que fonamenten la tecnologia, allò que ha de ser considerat moralment rellevant, i els objectius últims i els conceptes del que és bo.

Les preocupacions de la UE en aquest sentit se centren en tres elements principals.

1. Els sistemes d'armes *autònoms*.
2. El programari *autònom*, els bots. Avui ja manejats en el comerç i les finances, a més de per aquells sistemes intel·ligents actuals que mantenen diàlegs amb clients en centres d'atenció telefònica. La Comissió Europea planteja un tema més enllà de la privacitat, i és si volem saber si parlem amb un ésser humà o amb una IA[9].
3. De forma més àmplia en els espais d'opinió pública, apareixen els vehicles que no necessiten d'un conductor, encara que de moment el debat sembla centrar-se en casos excepcionals, normalment anomenats *dilemes del tramvia*[10]. Com indica la Comissió Europea, aquesta interpretació suscita un enfocament calculador, que

[9] Molt relacionat, i també estudiat per Dudley, està l'ètica del joc. El joc ací considerat element lúdic on s'aposta un poc de valor, amb consciència del risc i esperança de guanyar, sobre el resultat d'un concurs, o un esdeveniment incert el resultat del qual pot ser determinat per atzar. Pensem que molts dels jocs d'atzar avui es desenvolupen a Internet, i no amb un crupier humà, sinó amb un bot: una màquina, a la qual hauríem d'aplicar l'ètica de què estem parlant. Les apostes per Internet, a diferència de molts altres tipus d'activitat de joc, són una activitat solitària, la qual cosa les fa encara més perilloses: la gent pot jugar sense interrupcions i sense ser detectats per períodes il·limitats de temps. D'altra banda, posseeixen la capacitat per a adoptar múltiples identitats falses en el ciberespai, que implica que el blocatge de comptes d'usuari serà ineficaç. És poc probable, doncs, que l'autocontrol servisca per a res. I ja que l'usuari no té control sobre si mateix, ha de ser el sistema, la màquina, en definitiva, qui ho faça (Dudley, 85).

[10] Per exemple, pensem que som els gestors del tramvia en una ciutat. Una màquina es descontrola, descarrilarà i el nombre de morts pot ser el major fins avui en els accidents d'aquest estil. Tenim una alternativa, que és desviar manualment el vagó, però sabem que en fer-ho irremissiblement matarem una persona, que es troba atrapada a la cambra de màquines a què va accedir per a fer una reparació. El desviem? Aquesta pregunta la vaig fer a un grup d'alumnes i massivament van dir "sí". Ara introduïm una variació: per a desviar el tramvia fa falta que espentem una dona que porta un carret de la compra sobre la via. La resposta canvia a un "no" sense fissures.
En tots dos casos mor un innocent. Quan demane que m'expliquen el perquè del canvi no apareixen explicacions racionals. Alguns diuen que són situacions totalment diferents. Uns pocs aconsegueixen justificar-ho, però després d'un període llarg de reflexió, superior al que la immediatesa per a salvar els passatgers del tramvia requerien.
La resposta va dins del nostre cervell de *sapiens*, predisposat a evitar la violència innecessària, a no fer mal de forma directa i intencionada, si no suposen una amenaça directa per a nosaltres. És un fre intern i, diguem-ho, un meravellós fre. És una cosa que ens fa prendre camins seguidament davant de dilemes ètics que se'ns presenten diàriament. Alguns gravats en els nostres gens, uns altres apresos i que conformen el dia a dia de les nostres societats.

generalment aplica paràmetres excessivament simplistes a les realitats humanes, la qual cosa, d'altra banda, provoca que ignorem preguntes de més calat com ara "quines decisions relatives al disseny es van prendre en el passat que conduïren a aquest dilema moral?", "quins valors han de contribuir al disseny?", "com s'han de sospesar aquests valors en cas de conflicte i qui ha de sospesar-los?", "què indiquen les abundants dades empíriques que s'estan acumulant sobre la forma en què les persones decideixen en els casos del dilema del tramvia i com es tradueixen aquests resultats a les configuracions automàtiques per a vehicles?" (Comissió Europea. Grup Europeu sobre Ètica de la Ciència i les Noves Tecnologies, 2018). En un termini breu o mitjà, hi poden haver pocs o molts accidents de cotxes autònoms, però serà un fet que els cotxes seran controlats per màquines. No importa tampoc si hi estem d'acord o no, o si creiem que és més o menys viable econòmicament. Al principi del segle XX, quan els vehicles, de primer elèctrics i després amb motor d'explosió, van començar a recórrer les nostres ciutats, es va generar un moviment de protesta, que al·legava que haurien molts morts. I és cert, en un sol dia els morts per accidents de trànsit superen els morts durant dècades per accidents amb cavalls o carretes de bous, però... Quants cavalls o carretes de bous circulen avui per les nostres ciutats? El futur és imparable. El mateix s'aplica a l'ús de màquines per a la fabricació o a l'ús de la telefonia mòbil. No hi ha opció de retorn. Podem definir límits, però no detenir el canvi. (Latorre Sentís, 2019). La pregunta del milió és: com codifiquem això en un algorisme?

Al gener de 2017, convocats per la conferència Beneficial Artificial Intelligence 2017, organitzada per Future of Life Institute, es van reunir investigadors, científics i líders de la indústria relacionats amb el desenvolupament de la intel·ligència artificial a Asilomar, Califòrnia, Estats Units, que analitzaren, debateren i redactaren posteriorment els Asilomar IA Principles coneguts en valencià com els principis d'Asilomar per a la intel·ligència artificial.

S'han inclòs en la regulació de l'estat de Califòrnia i hi donen suport investigadors principals en intel·ligència artificial a Google, Facebook, Apple i més de 3.800 experts en intel·ligència artificial.

Podeu veure'n un resum en l'annex.

Robots

El desenvolupament de la intel·ligència artificial genera progrés en la seua aplicació, però l'adopció pot plantejar-ne certs problemes de caràcter moral i ètic molt rellevant, i el problema sembla agitar-se si li donem forma antropoide o no a aquestes IA: si els donem forma de robots. No fa falta recórrer a la ciència-ficció, sinó als telenotícies, per a poder veure que els robots seran més ràpids i intel·ligents que nosaltres, i que de fet ja ho són en alguns aspectes, així que hem d'esperar conflictes relatius a la integració entre humans i robots. Una aproximació al problema és desenvolupar un conjunt de regles i normatives de seguretat industrial relatives al desplegament de robots industrials en entorns de treballs compartits amb humans. (Barrio Andrés, 2018)

Fem un poc d'història, per a contextualitzar la robòtica, segons (Barrio Andrés, 2018). A la fi del s. XVIII i principi del XIX, la Revolució Industrial va proporcionar les bases per a la construcció d'autòmats que pogueren ajudar a millorar l'eficiència de producció en la indústria tèxtil. Els

primers autòmats programables apareixen, i amb aquests l'important concepte de programa. En les primeres dècades del XX apareixen mecanismes més o menys autònoms que resulten útils en diferents indústries. I també el nom *robot* de la mà de Karel Čapek i, sense abandonar els escriptors de ciència-ficció, és entre aquest moment i la següent revolució quan Isaac Asimov publica les seues tres lleis de la robòtica[11], a la qual després n'afegirà una quarta. És el moment de màxima popularitat. Durant les dècades de 1950 i 1960 apareixen les primeres descripcions de robots en revistes populars i després industrials, robots de producció o industrials que encara avui funcionen. Són robots telemanipuladors que necessiten un control continu d'un operador humà. El pas següent es desenvolupa com una subdisciplina de la robòtica: la teoria de control (1970), que va de la mà de l'avanç de la informàtica, que converteix els robots en cada vegada més autònoms i més intel·ligents. (Barrio Andrés, 2018). La polèmica apareix i comença a ser un element d'interès[12].

Barrio proposa tres possibles classificacions dels robots: (Barrio Andrés, 2018)

1. Considerant-ne la complexitat: control manual, manipulador, automàtic, programable, capaç d'adquirir dades de l'entorn.
2. Quant als components: electromecànic, nanobot, *softbot*.
3. Quant a l'aplicació: ambiental, cirurgia, militar, educació, etc.

Els robots són molt mediàtics i no solen deixar indiferents. Latorre recorda la polèmica suscitada a l'Aràbia Saudita per l'obtenció de la ciutadania per la robot Sophia. (Latorre Sentís, 2019)

Una pregunta sol suscitar-se: Podem adoptar esquemes clàssics de l'ètica en la robòtica? Pensem en l'imperatiu categòric. Resumim de forma precipitada que Kant ens diu que hi ha dues maneres de dictar accions, dites imperatius. El primer imperatiu és molt freqüent: per a traure un pot de la màquina, fica una moneda. Però si no tinc set i no vull traure un pot, l'imperatiu perd sentit. La majoria dels imperatius depenen d'una condició, que s'anomenen imperatius hipotètics. Si la condició no es compleix, l'imperatiu perd tot el sentit. Però hi ha un altre tipus d'imperatius: l'imperatiu categòric. Un exemple elemental: no mentisques si no vols que et mentisquen. Veiem que és una expressió autosuficient, independent de les nostres creences i aplicable sempre. Pensem ara sobre la possibilitat de programar les màquines intel·ligents utilitzant com a guia l'imperatiu categòric. Un robot gestionat per una intel·ligència artificial es retroalimenta de dades, dades del mateix funcionament i dades de l'exterior que pot comparar i analitzar. No sembla senzill incloure imperatius categòrics en aquesta programació, però almenys sí hi pot haver un bon debat ètic sobre els seus criteris d'actuació.

[11] La primera: un robot no farà mal a un ésser humà ni permetrà amb la seua inacció que patisca mal, que ja ha sigut clarament violada per l'ús de robots de guerra: els drons.

[12] Es recomana cercar i revisar les trobades / documents següents:

1. Simposi Internacional sobre robòtica (San Remo, Itàlia, 2004)
2. Programa d'ètica de la ciència i la tecnologia per l'ONU i l'Organització de les Nacions Unides per a l'Educació, la Ciència i la Cultura (UNESCO)
3. Projecte *ethicbots* (Espanya, finançat pel 6è Programa Marc de la Comissió Europea)
4. Proposta del Parlament Europeu sobre robòtica i dret civil (2017)

Deixem ara aparcat Kant i anem amb l'utilitarisme, en un ràpid viatge al segle XVIII de la mà de Jeremy Bentham, que conclou que estem dominats per dues forces: plaer i dolor. L'utilitarisme trenca amb Kant, perquè les accions no són bones o dolentes per si mateixes. Això dependrà de les conseqüències que comporte. Podem intentar programar una presa de decisions sobre conseqüències futures? Inspirant-nos en fets passats que esperem que es repetisquen? Inspirant-nos en una experiència col·lectiva del passat? (Latorre Sentís, 2019)

IoT

Entenem per IoT o IdC, Internet of Things o Internet de les Coses, la interconnexió digital d'objectes quotidians amb Internet. Sense adonar-nos pràcticament, van introduint canvis en les nostres vides (López i Seuba, 2019), com nous hàbits que poden anar de l'ús de la domòtica a com veiem la televisió (mirem sèries de televisió amb Netflix, HBO, moltes vegades amb suggeriments presos dels nostres hàbits), apareixen nous productes (roba intel·ligent) i òbviament noves conseqüències (medi ambient) i noves possibilitats. Per exemple, ja que parlem del medi ambient[13], pensem en sensors tèrmics, sensors de CO2, llums que es poden apagar sols..., fins i tot edificis intel·ligents.

Els elements de la Internet de les coses serien: (López i Seuba, 2019)

1. Objectes o coses connectats a Internet i entre ells.
2. Dades generades pels objectes.
3. Processos conjunts de fases a què es posa alguna cosa per a transformar-lo.
4. Persones.

Òbviament aquesta interconnexió és susceptible de presentar diversos problemes. Aquests els resumeix (López i Seuba, 2019) en la relació següent:

1. Seguretat física. És un dels factors més importants per als governs. No es tracta de pensar en recuperacions davant problemes amb el clàssic apaga i torna a engegar. De l'Administració pública depèn la nostra vida quotidiana: trànsit, hospitals, escoles...
2. Privacitat.
3. Altres qüestions.

L'ètica aplicada a la IdC es pot considerar una ètica d'àmbit professional en la mesura que s'ocupa essencialment de la responsabilitat de determinats grups d'experts, però també tindria una part d'ètica empresarial mentre aquests experts treballen en corporacions d'àmbit privat o públic que han de desenvolupar una determinada cultura ètica que permeta prendre decisions orientades cap a l'interès general de la societat o bé comú. (Colmenarejo Fernández, 2017)

[13] Escenaris concrets en parlar de medi ambient i IoT, on tots tenen en comú l'ús de la tecnologia de la sensorització per a obtenir dades i realitzar accions correctores (López i Seuba, 2019)

1. Conservació de la biodiversitat.
2. Caça furtiva i trànsit d'espècies.
3. Extinció de la fauna salvatge.
4. Restauració ecològica.

Big Data

En aquest apartat seguirem i tractarem de resumir l'estupend treball de (Colmenarejo Fernández, 2017) sobre aquest tema. L'assumpte es va esbossar en el tema relatiu a protecció de dades, així que és possible que es trobe alguna redundància en el present.

La gestió massiva de dades té una sèrie de conflictes a vegades ètics, a vegades legals, que ens han de fer repensar uns quants aspectes. Per exemple. Qui és el subjecte moral? Quins aspectes de l'exercici professional tenen dificultats per a estar regulats legalment? Els usuaris no han arribat a comprendre com afecta les violacions de privacitat tant a ells, com a individus, com, en general, com a societat. Hi ha una sèrie de problemes que, units, generen un vertader perill. Sumem la falta de transparència en les polítiques de privacitat de les empreses, l'habitual falta d'informació respecte a les anàlisis predictives que es realitzen, l'ús de dades falses que resulten d'anàlisis imperfectes i que poden ser compartides en centres de dades, amb la dificultat òbvia que resulta d'exercir el dret a corregir errors o falsedats i, no solament de dades falses ve el problema, sinó dels perfectes resultats d'anàlisis predictives que determinen amb exactitud atributs sensibles, com són l'orientació sexual, origen ètnic, creences religioses, ideologia política i fins i tot les probabilitats de cometre delictes, mitjançant les tècniques avançades de vigilància precrim. (Colmenarejo Fernández, 2017)

Així, podem resumir en dos els problemes ètics fonamentals que afecten la gestió de les dades massives, sempre segons (Colmenarejo Fernández, 2017)[14]:

1. Identitat: la diferència entre identitat en línia i identitat fora de línia, i fins i tot l'adopció d'altres identitats (com els consumidors proactius o *prosumers*, p. e., aquests consumidors d'una marca que no es conformen amb ser clients, sinó que semblen fondre la seua identitat amb aquesta i hi col·laboren).
2. Vulnerabilitats visibles i invisibles en la privacitat. Pensem en l'oxímoron "vigilar per a alliberar". De pas, això ens ajudarà a comprendre els retards en la publicació del Reglament General de Protecció de Dades després de l'ona d'atemptats gihadistes a Europa. Pensem en aquestes aplicacions ja conegudes que permeten reconèixer cares entre multituds en passos fronterers, basades en la mineria de dades (*data mining*), estadística i aprenentatge automàtic (*machine learning*) alhora.

Per a poder dur a terme una gestió correcta en l'ètica del Big Data (Colmenarejo Fernández, 2017) indica una sèrie de punts a considerar:

1. Cal identificar els *stakeholders*.
2. Cal identificar les implicacions en la presa de decisions ètiques.
3. Cal crear un marc per a la presa de decisions, una sèrie de punts de decisió ètica. Per a això proposa un seguit de termes:
    a. Conèixer la intenció: les intencions finals d'aquells que tenen accés a les dades.
    b. Verificar la seguretat: mitjans que l'organització té per a complir els requisits de seguretat establits per la llei o per la seua exigència.

[14] Bàsicament juguem amb cinc factors per a tractar de donar llum a tot això. Són les 5V: volum, velocitat, varietat, veracitat i valor. (Colmenarejo Fernández, 2017)

c. Estudiar la probabilitat: la probabilitat que hi ha que de l'accés a dades específiques resulte un benefici o un mal.
d. Estudiar possibles agregacions: l'organització ha d'establir i fer-se responsable de la combinació de possibilitats derivades de la correlació de les dades disponibles.
e. Definir responsabilitats: els diferents graus d'obligació que sorgeixen en cada punt de la cadena de dades respecte a la consideració de les conseqüències de l'acció.
f. Localització d'identitat: les col·leccions de dades correlacionades i interrelacionades que permeten que un subjecte siga caracteritzat individualment.
g. Estudiar els drets de propietat: qui té els drets en cada punt de la cadena de dades.
h. Quantificar el benefici: contribució específica positiva de les dades disponibles a l'organització i a l'usuari
i. Quantificar el mal: tipus de mal, sobre la identitat, la privacitat, la intimitat o la reputació que es podria derivar de l'accés a dades específiques.

Ens queda només tractar de dos aspectes, també estudiats per (Colmenarejo Fernández, 2017): el quan i el com. El quan es refereix als moments del procés on cal estar atents. Això és el que es relaciona com la taxonomia de la vulneració de la privacitat. Respecte al com, ens referim als principis que un professional ha de considerar. Vegem aquestes dues relacions.

Taxonomia de la vulnerabilitat de la privacitat (Colmenarejo Fernández, 2017):

1. Recol·lecció
2. Procés: inclou recopilació, identificació, seguretat, usos secundaris i exclusió
3. Difusió: violacions de confidencialitat, revelació, exposició indeguda...
4. Interferència en la presa de decisions i intrusió

Principis professionals en protecció de dades (Colmenarejo Fernández, 2017)

1. Prevenció del mal.
2. Desigualtat informativa: p. e. quan es col·loca persones en desavantatge per a negociar contractes, per exemple.
3. Injustícia informativa i discriminació: informació personal proporcionada en un determinat context, p. e. en atenció mèdica, que pot canviar de significat en un altre context, p. e. en transaccions comercials.
4. Instruccions d'autonomia moral: es pot exposar els individus a forces externes que influeixen en les eleccions del professional.

Solucions proposades per la Comissió Europea

Algunes de les iniciatives més destacades que cerquen la formulació de principis ètics per a la IA i els sistemes *autònoms* provenen de la indústria i dels professionals i les seues respectives associacions. (Comissió Europea. Grup Europeu sobre Ètica de la Ciència i les Noves Tecnologies, 2018)

Entre aquestes iniciatives és important destacar:

- El tractat “Disseny Èticament Alineat” del IEEE (Institut d'Enginyers Elèctrics i Electrònics)

- La cimera global IA per al bé, de la IUT (Unió Internacional de Telecomunicacions)

- La conferència AAAI/ACM “IA, Ètica i Societat” (2018).

- “Principis d'Asilomar per a la IA” (Future of Life Institute) (resum en annex)

La comissió presenta el que denomina una sèrie de principis ètics i prerequisits democràtics necessaris per a l'establiment d'un marc ètic en l'àmbit de la intel·ligència artificial. Un resum d’aquests es pot veure en l'annex.

Conclusions

Els sistemes d'informació, els ordinadors, Internet... són eines. Com un ganivet de cuina, bons o dolents segons en quines mans es manegen. No hi ha cap ètica en aquests, sinó en els humans que els manegen, manipulen o perjudiquen.

Pujant un esglaó més i parlant d'intel·ligència artificial, coincidim amb (Barrio Andrés, 2018) en dir-ne el mateix. Tota robòtica que contribuïsca en mitjans i finalitats a la felicitat i a la justícia dels éssers humans és bona i positiva. A això, afegeix una coda de molt d'interès: tota robòtica que escapa del control humà, si estiguera dotada de vertadera intel·ligència, estaria abocada a reproduir les nostres mateixes imperfeccions.

És possible, doncs, enfocar una ètica cap a màquines que pensen soles? (Latorre Sentís, 2019) ens recorda que no creia ningú que l'home volaria o que arribaria la lluna; que els humans descobriríem el codi genètic, manipularíem espècies o que crearíem màquines portentoses. La incapacitat de preveure el futur amb lucidesa és una constant en la història de la humanitat. És, per tant, no solament possible sinó necessari. Fins i tot, si volem endinsar-nos com sembla fer la UE (Parlament Europeu, 2017) en la ciència-ficció, sobre les pròpies màquines (recordem aquesta frase d'Arthur Clarke el 2010, Odissea 2: “Estar construït sobre carboni o sobre silici no constitueix una diferència fonamental; tots dos hauríem de ser tractats amb el respecte degut”)

La història ens ha donat suficients proves d'incapacitat de predicció tecnològica (n’hi ha prou amb recordar què va dir Thomas Watson, president d'IBM en els anys cinquanta: “crec que en el món hi ha mercat per a unes cinc computadores”, o un quart de segle després Ken Olson, quan estava al capdavant de la DEC, Digital Equipment Corporation, el 1977 “quin motiu hi pot haver perquè algú vulga una computadora a sa casa?). Això ens hauria de bastar per a poder obrir bé els ulls i anticipar de forma generosa què pot venir.

La millor manera d'acabar aquest tema és amb una idea de (Barrio Andrés, 2018): Prometeu va robar per a nosaltres el foc dels déus. Com a mortals no l’utilitzem per a convertir-nos en déus. Els déus no es van enutjar amb nosaltres per voler ser semblants a ells. No hi ha grans relats, el mite o la fe en la ciència han de cedir davant la necessitat vital i realista del discerniment: “amb nosaltres, amb les màquines, o les màquines o nosaltres. I això en cada situació concreta”.

Bibliografia

Aigrain, P. (2012). *Sharing. Culture and the Economy in the Internet Age.* Holanda: University Press.

Barger, R. N. (2008). *Computer ethics: a case-based approach.* NY, EUA: Cambridge University Press.

Barrio Andrés, M. (2018). *Derecho de los robots.* Madrid: Wolters Kluwer.

Brandt, R. L. (2009). *Las dos caras de Google.* Barcelona: Viceversa.

Bynum, T. W., & Rogerson, S. (2004). *Computer ethics and professional responsibility.* Cornwall: Blackwell.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* Ottawa, Canadà: HarperCollins.

Colmenarejo Fernández, R. (2017). *Una ética para Big Data.* Barcelona: UOC.

Comissió Europea. Grup Europeu sobre Ètica de la Ciència i les Noves Tecnologies. (2018). *Declaració sobre Intel·ligència artificial, robòtica i sistemes "autònoms".* Luxemburg: Oficina de Publicacions de la Unió Europea.

Cotino, L. (2008). *Consumidores y usuarios ante las nuevas tecnologías.* València: Tirant Lo Blanch.

Crespo Fajardo, J. L. (2012). *Arte y cultura digital.* Màlaga: Eumed.

David, A. (1973). *La cibernética y lo humano.* Barcelona: Labor.

De George , R. (2003). *The ethics of information technology and business.* Cornwall: Blackwell.

Dudley, A., Braman, J., & Vincenti, G. (2012). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices.* EUA: IGI Global.

Edgar, S. L. (2003). *Morality and Machines. Perspectives on Computer Ethics.* Boston, EUA: State University of New York, Genese. Jones and Bartlett Publishers, Inc.

EUR-Lex. (1 de juny de 2019). *El acceso al Derecho de la Unión Europea*. Obtingut de https://eur-lex.europa.eu/homepage.html

Garriga Domínguez, A. (2012). *Fundamentos éticos y jurídicos de las TIC.* Pamplona: Aranzadi.

Girard, B. (2007). *El modelo Google.* Barcelona: Granica.

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking.* EUA: Wiley.

Himanen, P. (2004). *La ética del hacker y el espíritu de la era de la información.* Barcelona: Destino.

Himma, K., & Tavani, H. T. (2008). *EINAR, K. y TAVANI, H. The handbook of information and computer Ethics.* Hoboken, Nova Jersey, EUA: John Wiley & Sons.

Ippolita, C. (2010). *El lado oscuro de Google. Historia y futuro de la industria de los metadatos.* Barcelona: Virus.

Jennings, M. M. (2009). *Business ethics.* EUA: South-Western.

Joyanes Aguilar, L. (2010). *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Madrid: Ministeri de Defensa.

Khosrow-Pour, M. (2003). *KHOSROW-POUR, M. Annals of Cases on Information Technology. Information Resources Management Association.* Londres, Regne Unit: Idea Group Publishing.

Kshetri, N. (2010). *The Global Cybercrime Industry.* N. Y., EUA: Springer.

Latorre Sentís, J. (2019). *Ética para máquinas.* Barcelona: Ariel.

Laudon, J. P., & Laudon, K. C. (2016). *Sistemas de Información Gerencial.* Madrid: Pearson.

Lessig, L. (2001). *El código y otras leyes del ciberespacio.* Madrid: Taurus.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* N. Y., EUA: RAND.

Livingstone, S. (2009). *Children and the internet.* Cambridge: Polity Press .

López i Seuba, M. (2019). *Internet de las cosas. La transformación digital de la sociedad.* Madrid: Ra-Ma.

Mitnick, K. D., & Simon, W. L. (2007). *El arte de la intrusión.* Madrid: RA-MA.

Mitnick, K., & Simon, W. (2011). *Ghost in the wires.* EUA: Little, Brown and Company.

Mitnick, K., & Vamosi, R. (2018). *El arte de la invisibilidad.* Madrid: Anaya.

Parlament Europeu. (2017). *Normas de Derecho civil sobre robótica.* Estrasburg: Parlament Europeu.

Porter, E. (2011). *Todo tiene un precio: Descubre que el valor de las cosas afecta al modo en que nos enamoramos, trabaja.* Madrid: Aguilar.

Reischl, G. (2008). *El engaño Google.* Madrid: Medialive.

Smoller, J. (2014). *La otra cara de lo normal.* Barcelona: RBA.

Stallman, R. M. (2004). *Software libre para una sociedad libre.* Madrid: Traficantes de Sueños .

Stoll, C. (1990). *El huevo del cuco.* Barcelona: Planeta.

Suarez Sánchez-Ocaña, A. (2012). *Desnudando a Google.* Madrid: Deusto.

Vázquez, J. M., & Barroso, P. (1996). *Deontología de la informática (esquemas).* Madrid: Instituto de Sociología Aplicada.

Contingut