Revista catalana de dret públic #64

www.rcdp.cat

LÍMITS DEL PRINCIPI DE PRIVADESA PEL DISSENY

Antoni Roig Batalla*

Resum

El principi de privadesa pel disseny, incorporat finalment al Reglament general de protecció de dades, forma part ara de les garanties jurídiques. Analitzem, en aquest treball, l'abast d'aquesta crida a la tecnologia garant. Concretament, ens interessa valorar els seus límits o problemes d'aplicació. Un aspecte que mereixerà especial atenció és la falta de coordinació entre les comunitats jurídiques i tècniques, i les seves conseqüències. Així, descriurem casos d'ús de tecnologies pretesament garants que a la pràctica no ho són; també veurem casos de tecnologia garant contrària a dret, i, finalment, mencionarem casos d'eines que no tenen en compte el concepte jurídic de privadesa a l'hora de dissenyar-ne la protecció. Dedicarem la part final del treball a suggerir possibles vies per redreçar la situació i treure tot el potencial corregulador de les eines tècniques garants.

Paraules clau: privadesa pel disseny; eines garants de la privadesa; corregulació; dret i tecnologia.

THE LIMITS OF PRIVACY BY DESIGN

Abstract

Privacy by design (PbD), an approach to systems engineering included in the European Union's General Data Protection Regulation, now forms part of the EU's legal safeguards. This article examines the scope of this reliance on privacy-enhancing technologies (PETs). More specifically, it assesses their limits and the problems with their real-world application. One aspect worthy of particular consideration is the lack of co-ordination between our legal and our technology communities: we shall be providing examples of supposedly privacy-enhancing technologies that are ineffective in practice, as well as those that are unlawful and, finally, those that do not take account of the legal concept of privacy in the design of the protection they afford. The article concludes by suggesting some possible ways of remedying this situation and of leveraging the full co-regulatory potential of privacy-enhancing technologies.

Keywords: privacy by design; PbD; privacy-enhancing technologies; PETs; co-regulation; law and technology.

* Antoni Roig Batalla, professor titular de Dret Constitucional al Departament de Ciència Política i Dret Públic de la Universitat Autònoma de Barcelona. Facultat de Dret, edifici B2, c. de la Vall Moronta, s/n, 08193 Bellaterra (Cerdanyola del Vallès). antoni.roig@uab.cat. 0000-0002-4760-9361.

Article rebut el 02.09.2021. Avaluació cega: 04.10.2021 i 06.10.2021. Data d'acceptació de la versió final: 06.10.2021.

Citació recomanada: Roig Batalla, Antoni. (2022). Límits del principi de privadesa pel disseny. *Revista Catalana de Dret Públic*, *64*, 174-186. https://doi.org/10.2436/rcdp.i64.2022.3717

Sumari

1 La crida a la tecnologia: el principi de privadesa pel disseny

Si mirem l'article 18.4 de la Constitució espanyola (CE), hi podem albirar el que ha estat la relació tradicional entre dret i tecnologia: "La llei limitarà l'ús de la informàtica per garantir l'honor, la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets."

Com es veu, la tecnologia és un nou supòsit de fet o factor de risc que requereix unes garanties jurídiques per evitar que afecti els drets fonamentals de les persones. La tecnologia incorpora, doncs, nous escenaris que cal protegir amb una regulació específica. El dret és la garantia, la tecnologia és el nou factor de risc.

La privadesa pel disseny, aparentment, sembla trencar l'entesa tradicional de la tecnologia:

– La tecnologia ja no és només un factor de risc.

– La tecnologia pot ser, fins i tot, part de la solució o garantia dels drets fonamentals.

– El dret crida la tecnologia a contribuir a la defensa dels drets fonamentals.

Aquesta crida jurídica a la col·laboració tècnica no és una autèntica corregulació. Si fos així, el dret estaria perdent el monopoli de la regulació en favor de la regulació tecnològica. Certament, els principis jurídics i el dret a la privadesa haurien de ser respectats per la regulació tecnològica, però seria possible un marge regulador complementari o executiu. S'estaria autoritzant així un àmbit autoregulador que respectés els principis jurídics i els drets fonamentals. No és el cas. El legislador ha fet aquest pas per motius més modestos: veu els límits de la regulació per principis i vol aprofitar la capacitat protectora que poden aportar les tecnologies garants de la privadesa (*privacy enhancing technologies*). No és, doncs, una aposta revolucionària, sinó més aviat una evolució cap a una major eficàcia de la regulació tradicional (Schartum, 2016). Més recentment, s'intenta aplicar el principi de privadesa pel disseny en àmbits tan nous i canviants com l'internet de les coses (Tamò-Larrieux, 2018).

Cal tenir present que aquest apropament a la tecnologia no ha suposat un apropament a la comunitat tècnica, que, des de finals dels anys noranta i més clarament des de principis del present segle, pretén donar un contingut ètic a la tecnologia, amb un disseny que afavoreixi la privadesa –es poden veure les seves aportacions a European Union Agency for Cybersecurity (ENISA, 2014, 2016, 2019 i 2021). L'apropament jurídic a les tecnologies garants de la privadesa és, així, anterior al Reglament general de protecció de dades –en endavant, RGPD–, com es veu, per exemple, a Schaar, 2010 i Rubinstein, 2012. Ara bé, és amb la previsió de l'article 25 de l'RGPD que el principi de privadesa pel disseny adquireix la seva importància actual.[1] D'aquesta manera, la privadesa pel disseny s'emmarca ara en una nova etapa de la protecció de dades, amb unes avaluacions de riscos i una responsabilitat proactiva (Bygrave, 2017, 2020). Malgrat aquesta previsió expressa en l'RGPD, això no s'ha traduït en un autèntic diàleg amb la comunitat tècnica. Com veurem, les conseqüències d'aquesta manca de coordinació entre la comunitat jurídica i la tècnica afecten l'eficàcia de les eines garants.

Ens proposem en aquest treball mostrar els límits d'aquesta interessant reforma reguladora i proposar el que creiem que en podrien ser algunes vies de millora (en la mateixa línia que Klitou, 2014). Els límits que analitzarem en els següents apartats seran:

– La falta de valoració sobre la necessitat o no de la tecnologia garant en un supòsit concret.

– L'ús de tecnologia garant poc eficaç.

1 Art. 25 RGPD: Protecció de dades des del disseny i per defecte.

> 1. Tenint en compte l'estat de la tècnica, el cost de l'aplicació i la natura, l'àmbit, el context i les finalitats del tractament, així com els riscos de diversa probabilitat i gravetat que suposa el tractament per als drets i les llibertats de les persones físiques, el responsable del tractament aplicarà, tant en el moment de determinar els mitjans de tractament com en el moment del mateix tractament, mesures tècniques i organitzatives adequades, com la pseudonimització, concebudes per aplicar de forma efectiva els principis de protecció de dades, com la minimització de dades, i integrar les garanties necessàries en el tractament, a fi de complir els requisits del present Reglament i protegir els drets dels interessats. [Les traduccions al català són de l'autor].

– La falta de criteris de preferència entre diferents opcions tecnològiques garants.

– L'existència de solucions tècniques de garantia de la privadesa que són contràries a dret.

– L'ús d'un concepte no jurídic de privadesa per part de la tecnologia garant.

– L'absència d'una mètrica de la privadesa per poder avaluar si una suposada tecnologia garant ho és realment, i en quina mesura, i si ho segueix sent després d'un temps.

– La manca d'una plataforma institucional per garantir el diàleg i l'actualització de les garanties.

2 Cal sempre una tecnologia garant de la privadesa?

La privadesa pel disseny pot afegir garanties complementàries a la protecció jurídica tradicional. Ara bé, no sempre serà necessària. Imaginem que una regulació tradicional aporta un nivell de protecció adequat; en aquest cas, afegir-hi una garantia tecnològica no només no millora el nivell general de protecció, sinó que podria ser contraproduent. En efecte, tota tecnologia –també la tecnologia garant– pot suposar un element de risc en la protecció de la privadesa. Per aquesta raó, només té sentit incorporar una tecnologia garant quan els avantatges superen els inconvenients. I, si no cal una protecció complementària, llavors els inconvenients sempre superaran els avantatges.

Per aquesta raó, el primer que cal decidir abans de plantejar la necessitat de tecnologia garant és si és possible una protecció mitjançant una regulació tradicional, ja sigui amb principis o amb una regulació procedimental. No serà sempre el cas, però a vegades una estructura organitzativa garant podrà ser suficient. Mostrarem ara un exemple en el qual la regulació tradicional, amb principis, drets i procediments, no requereix, al nostre parer, una tecnologia garant complementària, o, si més no, només per a supòsits residuals. Es tracta del cas dels escàners corporals usats als aeroports per raons de seguretat.[2] La Unió Europea ha prohibit un tipus d'escàners, els basats en radiació ionitzant, per raons de salut.[3] La resta d'escàners no estan limitats per aquesta prohibició, tot i que han de seguir alguns principis i procediments garants que creiem que són suficients per preservar la privadesa, sense necessitat de tecnologia protectora complementària.

Així, es preveu, com a principi general, la possibilitat d'opció alternativa entre l'escàner o altres mètodes tradicionals: el passatger ha de tenir, doncs, la possibilitat real d'optar per un escorcoll personal alternatiu, amb la detecció d'explosius per gossos o sense.[4] En conseqüència, l'escàner no és obligatori, sinó opcional, i s'ha de poder optar per un altre mètode de control si així es demana, sense veure's perjudicat econòmicament ni patir dilacions que impedeixin fer ús de la possibilitat. Un altre principi, inspirat en la retenció de dades, consisteix a prohibir que es guardin o s'imprimeixin imatges més enllà del temps estrictament necessari per a l'anàlisi, i en cap cas un cop el passatger ha superat el control.[5] Per tant, aquí hi veiem una aplicació de principis de la regulació de protecció de dades, com la minimització de dades o la limitació de propòsit.[6]

2 Reglament d'Execució (UE) núm. 2015/1998 de la Comissió, de 5 de novembre de 2015, pel qual s'estableixen mesures detallades per a l'aplicació de les normes bàsiques comunes de seguretat aèria (DO L, núm. 299, de 14 de novembre de 2015), i les seves successives modificacions, la darrera mitjançant el Reglament d'Execució (UE) núm. 2021/255 de la Comissió, de 18 de febrer de 2021.

3 Art. 4.1.1.2, lletra *e*) del Reglament (UE) núm. 2015/1998, mencionat en la nota anterior.

4 Art. 4.1.1.10:

> Els passatgers es podran oposar a ser inspeccionats per un escàner de seguretat. En aquest cas, el passatger serà inspeccionat per un mètode d'inspecció alternatiu que inclourà, com a mínim, un registre manual [...]. Abans de ser inspeccionats per un escàner de seguretat, els passatgers seran informats de la tecnologia utilitzada, de les condicions lligades al seu ús i de la possibilitat d'oposar-se a aquesta inspecció.

5 Art. 4.1.1.10, lletra *a*):

> Els escàners de seguretat no emmagatzemaran, conservaran, copiaran, imprimiran ni extrauran imatges; no obstant això, tota imatge generada durant la inspecció es podrà conservar durant el temps necessari perquè l'examinador humà l'analitzi, i s'esborrarà així que s'autoritzi el pas al passatger; estan prohibits, i s'impediran, l'accés i l'ús no autoritzats de la imatge.

6 El principi de minimització de dades el tenim recollit a l'article 5 de l'RGPD: "1. Les dades personals seran: [...] *c*) adequades, pertinents i limitades a allò que sigui necessari amb les finalitats per a les quals són tractades ('minimització de dades')." El principi

També es plantegen mesures procedimentals que implementen eficaçment aquests i altres principis de la regulació de protecció de dades. Així, la persona que revisa la imatge hauria d'estar en un espai des del qual no tingués accés visual directe a l'espai on es troba el passatger.[7] Aquesta mesura pretén preservar la privadesa del passatger, de manera que l'agent controlador només obté la informació de la pantalla del seu monitor. D'aquesta manera es preserva tota informació sobre la persona que no ha de ser usada per raons de seguretat i s'eviten possibles discriminacions. En la mateixa línia, l'agent revisor tampoc hauria de poder vincular la imatge del passatger amb cap altra dada que l'identifiqui, com el seu nom, número de document d'identitat, etcètera.[8] Això reforça la idea que s'està duent a terme només un control de seguretat i que només s'accedeix a la informació estrictament necessària per garantir la seguretat del vol. D'altra banda, el principi de dignitat o d'intimitat corporal o personal també és aplicat per mesures procedimentals. Si el passatger ho demanés, la revisió hauria de ser feta per una persona de sexe masculí o femení, segons la seva elecció. Per tant, el passatger pot demanar que sigui examinat per una persona del mateix sexe, posem pel cas.[9]

Aquest exemple mostra que, a vegades, algunes mesures organitzatives poden fer possible una activitat respectuosa amb els drets fonamentals sense necessitat d'introduir tecnologia garant o, si més no, amb caràcter residual. Una possible entrada residual de la tecnologia garant podria consistir, en efecte, a permetre o exigir difuminar la cara del passatger per evitar ser identificat en el control. Cal tenir present, en definitiva, que fins i tot la tecnologia garant pot ser mal utilitzada, i requereix ser inclosa en una dinàmica organitzativa garant. Els procediments garants han de ser revisats periòdicament, a mesura que avancen tant la tecnologia en general com la tecnologia garant emprada en particular.

3 Tecnologia garant ineficaç

Un altre aspecte a tenir en compte és que no totes les tecnologies garants són igualment protectores. En efecte, algunes poden ser útils en situacions concretes o favorables, però, en canvi, tenen una capacitat protectora limitada en situacions més obertes, amb sensors i internet de les coses (IoT). Ser conscient dels límits d'ús de l'eina pot evitar confiar en una protecció inexistent o legitimar sense fonaments una pretesa protecció que no es produeix. Aprendre que no totes les tecnologies garants són igualment protectores i que algunes només serveixen en certs contextos és important. Però això és difícil per al jurista, que confia ara en les tecnologies de privadesa pel disseny.

Un exemple de tecnologies garants limitades són les que s'apliquen a les polítiques de privadesa. Existeixen tecnologies, en efecte, que permeten personalitzar la difusió de continguts d'una pantalla en funció de si el destinatari és una persona autoritzada o no a veure aquesta informació. Així, en presència d'una persona no autoritzada, es taparien o s'alterarien les dades de la pantalla considerades sensibles o mereixedores de protecció, com serien les persones, els rètols o les matrícules de vehicles (Aved i Hua, 2012). Imaginem la seva aplicació a videovigilància: s'aplicarien, en temps real, uns filtres de privadesa que garantirien que la imatge gravada només fos plenament disponible per a persones autoritzades d'acord amb les polítiques de privadesa (Shen et al., 2015). Una altra possibilitat consistiria a aturar la projecció d'un contingut en una pantalla quan una de les persones que acaba d'entrar a la sala no està autoritzada pel sistema a veure-la. Els aparells poden, així, disposar de controls parentals o estar personalitzats: pensem en una pantalla que permet als treballadors d'una empresa comprovar la seva agenda de reunions personal. Davant la presència d'una altra persona, la pantalla pot desplegar només les reunions conjuntes, però no les altres. En general, es poden establir controls d'accés vinculats a polítiques de privadesa (Werner et al., 2019). Aquestes proteccions es basen en automatitzacions de les polítiques de privadesa, del control d'accés, i a vegades utilitzen també serveis de web semàntica. Resulten interessants com a tecnologies garants, però sovint són limitades. Un

de limitació del propòsit o de la finalitat el tenim també a l'article 5 de l'RGPD: "1. Les dades seran: [...] *b*) recollides amb finalitats determinades, explícites i legítimes, i no seran tractades ulteriorment de manera incompatible amb aquestes finalitats."

7 Art. 4.1.1.10, lletra *b*): "L'examinador humà que analitzi la imatge es trobarà en un espai separat, de manera que no pugui veure el passatger inspeccionat."

8 Art. 4.1.1.10, lletra *d*): "La imatge no s'associarà amb cap altra dada sobre la persona inspeccionada, la identitat de la qual es mantindrà en l'anonimat."

9 Art. 4.1.1.10, lletra *e*): "El passatger podrà sol·licitar que la imatge del seu cos sigui analitzada per un examinador humà de sexe masculí o femení, segons la seva elecció."

atacant podria accedir als continguts de manera remota, sense estar present a la sala, i, per tant, burlant-se de l'accés personalitzat. Per evitar-ho, cal un nivell de protecció superior; per exemple, xifrant la informació de manera que el receptor no autoritzat no pugui fer-ne ús.

Per tant, la decisió sobre quina tecnologia garant és adequada en cada situació requereix coneixements tècnics. L'ús d'una tecnologia garant no sempre és sinònim de protecció efectiva de la privadesa. En definitiva, la crida a la privadesa pel disseny ho és a un nivell de protecció adequat o eficient, no a un ús de tecnologia, sigui quina sigui, que resulti finalment ineficaç.

En aquest apartat podem concloure que la crida jurídica a la tecnologia és qualitativa: tot i que no predetermina totalment l'actuació de la comunitat tecnològica, pressuposa que es tracta d'una tecnologia adequada i eficaç. Per tant, la tecnologia garant ha de poder justificar aquesta eficàcia; si no fos així, es donaria la situació paradoxal que la tecnologia garant afegiria situacions de risc a les persones i institucions que hi confiessin. El problema és que no s'ha previst cap mecanisme per poder acreditar aquesta eficàcia. Si ens prenem la privadesa pel disseny seriosament, estem obligats a establir mecanismes de certificació i auditories adients. Cal tenir present que l'RGPD estableix un nou principi de responsabilitat proactiva que obliga els responsables del tractament de les dades no només a complir amb les previsions del reglament, sinó també a poder demostrar que ho fan.[10] D'altra banda, es preveu també en els articles 42 i 43 de l'RGPD la possibilitat de certificacions. Doncs bé, caldrà aprofitar aquesta opció per certificar les tecnologies garants, en contextos concrets i de manera temporal. Com és fàcil d'entendre, la certificació de les tecnologies garants requerirà una revisió periòdica, a mesura que avancin les possibilitats tècniques dels agressors.

4 Quina tecnologia garant eficaç és millor?

L'enginyer disposa de coneixements adequats per determinar si una eina és eficaç o no en certes circumstàncies. No és casualitat que les millors monografies sobre tecnologies garants de la privadesa siguin fetes per enginyers o informàtics (per exemple, Torra, 2017). Potser per això els juristes han preferit no especificar la tecnologia concreta a utilitzar, cosa que permet la flexibilitat i l'actualització per part de l'expert. En aquest sentit, l'article 25 de l'RGPD obliga el responsable a aplicar "mesures tècniques i organitzatives apropiades" per tal de garantir els principis de protecció de dades. La normativa de protecció de dades ha concretat uns principis que poden servir de guia general. L'article 25 de l'RGPD destaca el principi de minimització de dades, que es pot posar en connexió amb l'article 25.2, és a dir, amb la protecció de dades per defecte. Així doncs, només s'haurien de tractar les dades estrictament necessàries per a la finalitat buscada. Un llistat més ampli dels principis relatius al tractament de les dades personals es troba a l'article 5 de l'RGPD. El principi de proporcionalitat aporta també tres criteris a l'hora de valorar les restriccions de drets fonamentals. El primer –ja l'hem comentat– sosté que l'eina ha de ser adequada pel risc a evitar; no serà una autèntica tecnologia garant la que no serveixi per protegir efectivament. El segon criteri és el test de necessitat, segons el qual s'haurien de preferir les eines menys invasores sobre els drets fonamentals. Aquest és un criteri jurídic molt més difícil de complir per part de les tecnologies garants, com veurem a continuació. Finalment, caldria valorar, en conjunt, si les mesures restrictives aporten més avantatges o perjudicis. Els principis tenen, però, una capacitat reguladora limitada en el context actual. No només són criteris vagues, cosa que és quasi inevitable, sinó que, a més, no són criteris "vius". Ens referim, amb aquesta expressió, al fet que no hi ha una actualització ni una concreció suficients d'aquests criteris, tot i els esforços de les autoritats de protecció de dades per publicar informes de gran vàlua. Destaquen, també, els òrgans tècnics consultius, com l'antic Grup de treball de l'article 29 de la Directiva de protecció de dades, el Comitè Europeu de Protecció de Dades o ENISA, entre d'altres.[11] El seguiment dels informes i treballs d'aquests grups és imprescindible per a qualsevol que vulgui estar al dia sobre eines garants.

10 Art. 5 RGPD: "[...] 2. El responsable del tractament serà responsable del compliment del previst en l'apartat 1" –els principis relatius al tractament– "i capaç de demostrar-ho ('responsabilitat proactiva')".

11 Sobre l'antic Grup de treball de l'article 29 de la Directiva de protecció de dades, es pot consultar aquesta pàgina web; sobre el Comitè Europeu de Protecció de Dades, vegeu el seu portal a Internet; sobre ENISA, podeu consultar la seva pàgina web; també poden resultar d'interès els treballs del grup d'experts d'alt nivell sobre IA. [Consultes: 20 de febrer de 2022].

L'RGPD, tot i no predeterminar quines tecnologies garants s'han de preferir, en menciona alguna, com la pseudonimització (art. 25.1 RGPD), evidentment sense pretensió de ser exhaustiu. Un altre recurs pràctic per a l'enginyer són les avaluacions d'impacte que determinen les situacions de risc, així com les possibles solucions per fer-hi front (art. 35 RGPD). La regulació basada en els riscos és més concreta que la regulació per principis, i, per tant, més fàcil d'aplicar. L'inconvenient de basar la regulació en la reducció de riscos és que difícilment incorpora valors i drets. Un exemple que pot il·lustrar aquest punt és la regulació de les nanotecnologies (Roig, 2018). Els requeriments de reducció de risc d'un producte concret han hagut de ser completats amb exigències de sostenibilitat per incorporar valors socials i col·lectius que no es prenien en consideració en la definició de material segur. La reducció de riscos és una metodologia que ha de formar part de la discussió reguladora, però no s'haurien de reduir tots els problemes socials a optimitzacions, ni se n'haurien d'excloure els interessos generals que només pot defensar el legislador.

Sigui com sigui, aquests continguts de l'RGPD no estan pensats per a una autèntica col·laboració entre les comunitats jurídiques i els tecnòlegs que treballen amb les eines garants. Per tant, existeix risc de tecnologies garants legals, però ineficaces –o que ho seran amb el temps per falta d'actualització–, com ja hem dit, i també hi ha risc de tecnologies garants eficaces, però desproporcionades, com veurem a continuació.

5 Tecnologia garant eficaç desproporcionada

Hem dit que l'eficàcia d'una eina garant només la pot certificar un tècnic. Ara bé, assegurant que la protecció és eficaç no se solucionen tots els problemes. En efecte, la temptació d'un expert en tecnologia garant és afegir nivells de protecció per complicar la tasca d'un hipotètic atacant. Això té tot el sentit si ens basem només en l'eficiència o en la dificultat per obtenir els continguts desitjats. Des del punt de vista jurídic, però, algunes proteccions màximes suposen un preu massa alt per als drets fonamentals. Un exemple per entendre això el tenim en les tecnologies garants per protegir la privadesa quan s'empren controls d'accessos a edificis o instal·lacions basats en dades biomètriques.

L'interès d'usar dades biomètriques per al control d'accessos és fàcil d'entendre si es pensa com un expert en seguretat: són dades molt més difícils de suplantar o de transferir que una simple targeta o un codi. Ara bé, els riscos per als usuaris són, paradoxalment, més greus que amb altres tecnologies menys eficaces. Imaginem, en efecte, que una clau d'accés es veu compromesa –és a dir, que ha caigut en mans d'una persona no autoritzada. En aquest cas, el canvi de clau d'accés pot ser una solució ràpida i eficaç. En canvi, si s'han usat dades biomètriques, potser no resultarà tan senzill copiar-les o suplantar-les, però si algú aconsegueix obtenir una còpia d'una empremta digital, posem per cas, la solució no és evident. No es podran canviar les dades biomètriques usades pel servei. A més, el risc s'estén a tots els altres serveis –bancaris, transports, etc.– en els quals hem usat la mateixa dada biomètrica que ara ha quedat compromesa. Per aquesta raó, a vegades s'ha considerat desproporcionat l'ús de dades biomètriques per al control d'accés de treballadors a l'empresa. Per exemple, la Comissió Nacional de la Informàtica i de les Llibertats francesa (CNIL) adverteix que el primer que cal fer és justificar la necessitat d'un dispositiu biomètric: si amb targetes d'accés convencionals n'hi ha prou o si els béns que cal protegir no són especialment sensibles, llavors no estarà justificat l'ús d'un sistema d'accés biomètric a una empresa.[12]

Doncs bé, suposem, per als nostres propòsits, que hi ha raons de seguretat que justifiquen en un cas concret l'ús de dades biomètriques protegides amb una tecnologia garant de la privadesa. L'enginyer pot haver optat per una mesura molt difícil de superar per un hipotètic atacant, com és la tecnologia biomètrica multimode (Anakath et al., 2019). Aquesta tecnologia, en comptes de demanar només una dada biomètrica, busca la seguretat resultant de dues o més dades biomètriques combinades: iris, empremta dactilar i batec del cor, per exemple. Amb això s'assoleix un nivell d'eficiència més alt: es dificulta molt l'ús no autoritzat (Purohit i Ajmera, 2021). Però, com hem dit, no tot acaba amb l'eficàcia. Des del punt de vista jurídic, es tracta d'una opció no desitjable, atès que no només es compromet una dada biomètrica, sinó fins i tot més d'una. En lloc d'això, és preferible una eina garant basada en el que es coneix com a "biomètrica no traçable o cancel·lable" –*untraceable or cancelable biometrics*– (Manisha, 2020). El funcionament d'aquesta tecnologia biomètrica respectuosa és el següent: l'eina no guarda cap dada biomètrica original per confrontar-la en el moment de

12 Vegeu la pàgina web de la Commission Nationale de l'Informatique et des Libertés. [Consulta: 20 de febrer de 2022].

la decisió d'accés. En comptes d'això, es guarda una dada biomètrica alterada o encriptada per un programa, de tal manera que es permet realitzar la tasca encarregada al sistema –per exemple, donar accés a la persona autoritzada– sense riscos. Si un atacant aconsegueix entrar en el sistema, no trobarà cap dada biomètrica original, sinó només aquesta dada derivada. Així com la dada biomètrica modificada permet la identificació a l'efecte de permetre l'accés, és en canvi totalment ineficaç per permetre reproduir la dada original. D'aquesta manera, la tecnologia garant permet els avantatges de les dades biomètriques sense els riscos associats a aquestes dades.[13]

Dit això, com pot l'enginyer saber que ha de preferir la tecnologia garant de dades biomètriques basada en la no traçabilitat abans que la multimodal? La major eficiència l'hauria de portar cap a la biomètrica multimodal. L'única opció és que treballi en un equip interdisciplinari format també per juristes. En tot cas, no trobarà cap norma que li ho indiqui: no hi ha cap llista de preferències jurídiques sobre les tecnologies garants de dades biomètriques. Això és un resultat que només es troba en alguns treballs doctrinals –mentre que en d'altres no es preveu– i que s'ha d'anar actualitzant a mesura que apareixen noves tecnologies. Com ja hem dit en alguna ocasió, la desconnexió entre les dues comunitats no ajuda a resoldre aquests problemes. Més encara, fins i tot quan les dues comunitats volen protegir la "privadesa", a vegades entenen que és una cosa diferent, com veurem a continuació.

6 Tecnologia garant d'una "privadesa" no jurídica

Pot resultar sorprenent pensar que la crida a les tecnologies garants pugui derivar en eines de protecció que es basen en un concepte de privadesa que, curiosament, no és el jurídic. I, en canvi, els enginyers sovint creen eines que protegeixen una "privadesa" que no es correspon totalment amb la dels juristes. Per tal de veure-ho clarament, agafarem l'exemple de les tecnologies garants de la privadesa en les xarxes socials. Com és sabut, la protecció jurídica de la privadesa parteix d'un dret individual a protegir un espai que l'individu considera propi i que vol preservar del coneixement dels altres. Tot i que pugui semblar un dret liberal clàssic, la seva configuració moderna es va produir fa poc més d'un segle, als Estats Units, en un moment en què els diaris d'abast federal podien suposar un risc molt important per a la dignitat i la reputació d'una persona. No era suficient canviar d'un estat a un altre per garantir que la reputació personal i professional renaixessin. El risc era general i calia una resposta jurídica: el dret a ser deixat en pau (*to be let alone*). Doncs bé, la protecció de la privadesa que tenen en compte els enginyers en les xarxes socials té poc a veure amb això.

La protecció de la privadesa dels usuaris de les xarxes socials, certament, pretén evitar que un atacant pugui accedir a continguts que es consideren privats o que es volen oferir només a persones conegudes o a contactes. Però ben aviat els analistes de xarxes han entès que, si volen protegir la privadesa d'un usuari en una xarxa social, han de tenir una perspectiva col·lectiva: cal protegir la xarxa (*graph*) de tots els contactes de l'usuari. En efecte, si un dels contactes tingués una política de privadesa oberta, la protecció individual d'un sol usuari seria ineficaç i els seus continguts podrien ser públics. De fet, amb una anàlisi estadística és possible fins i tot inferir continguts no oberts en una xarxa d'usuaris o identificar usuaris a partir del conjunt dels seus contactes.

Per tant, no n'hi ha prou amb l'aplicació de les eines garants a un sol usuari: no és suficient l'anonimització d'un usuari, com podríem pensar els juristes. Cal anonimitzar tota la xarxa o el graf de la connexió entre individus (per exemple, Gao et al., 2019). D'aquesta manera, es produeix un canvi en el concepte de privadesa que, tot i ser pretesament individual, resulta, per raons tècniques, col·lectiu. Aquesta protecció col·lectiva és la que s'intenta protegir en l'àmbit de les xarxes socials, no la protecció individual. Una eina d'encriptació individual o de gestió de les polítiques de privadesa sempre pot servir, però no protegeix realment davant certs atacs estadístics.

Les opcions de protecció col·lectiva són variades. Així, trobem referències a la *k*-anonimització o anonimat de grup (per exemple, Rajabzadeh et al., 2020). Es tracta d'una protecció que impedeix a l'atacant individualitzar la informació; com a màxim, obté un grup de *k*-unitats –posem per cas, 1.000 persones– que tenen unes característiques definides. No pot saber, però, si una persona concreta es troba en aquest grup o no. Per tant, no pot arribar a trobar un usuari concret, només grups de *k*-persones. Com més alta sigui la *k* –10.000 persones

13 Val a dir que comencen a aparèixer també sistemes biomètrics multimodals cancel·lables, que busquen el millor d'ambdues aproximacions (Gupta et al., 2021).

en comptes de 1.000 persones, posem per cas–, més protecció. Llavors es pot definir la privadesa segons aquesta tècnica com la garantia que mai ningú podrà individualitzar un perfil; només haurà obtingut grups de *k*-persones anònimes amb el mateix perfil.

Una altra tècnica de protecció col·lectiva és la *differential privacy* (Dwork, 2006; Yang et al., 2021). Aquí el punt de partida és que l'atacant coneix la informació d'un dels usuaris, i, a partir d'aquesta informació, intenta inferir la dels seus contactes. Així doncs, es vol protegir un usuari fins i tot quan un altre usuari es veu compromès. Per tant, no estem pendents només d'una persona concreta, sinó de totes, en el supòsit d'un usuari de qui es coneix tota la informació. Una altra protecció col·lectiva prové de la teoria de jocs o de diverses tècniques de cooperació entre usuaris. S'ha confirmat que resulta més eficaç per a la seguretat de tots els usuaris una actitud col·laboradora amb els altres que no pas una posició individualista. La complexitat de les tècniques de protecció col·lectiva va en augment, perquè es busca ara ja partir l'estructura de la xarxa social en diferents segments per tal de guanyar precisió. Es vol, així, fer front a atacs més intel·ligents que es basen no només en l'estadística, sinó també en la informació semàntica o els significats (Gu et al., 2019). En aquest sentit, la precisió permet anar més enllà de tècniques com la *differential privacy*, que tenen quinze anys i semblen ja clàssiques (per exemple, Yiping et al., 2019).

En definitiva, aquesta protecció col·lectiva de la privadesa és nova en dret: si es vol protegir la privadesa individual d'un usuari, cal protegir la xarxa de relacions entre usuaris. Si apliquem tècniques de protecció individual de la privadesa d'un usuari com l'anonimització, no serem eficaços. Com és possible que les dues comunitats parlin de privadesa en termes tan diferents? Doncs perquè no hi ha una mètrica de la privadesa que mostri als juristes que la protecció individual, fins i tot l'anonimització, no és suficient en les xarxes socials, cosa que la comunitat tècnica ja té clar des de fa temps, com a mínim des del treball de Cynthia Dwork sobre *differential privacy*, de 2006. El concepte de privadesa en les xarxes socials incorpora un requisit *sine qua non* de protecció col·lectiva que encara desconeixem en la comunitat jurídica. I cal recordar que, sense protecció efectiva, no hi ha dret de privadesa. Sovint els juristes pensem que anonimitzant ja complim amb la privadesa pel disseny. Doncs bé, anonimitzant les dades d'un sol usuari no oferim protecció a la seva privadesa. Sense protecció col·lectiva, no hi ha dret de privadesa en les xarxes socials. La privadesa individual neix de la protecció de la mateixa xarxa.

Ens agradaria acabar aquest apartat amb una reflexió més àmplia. Potser el lector deu pensar que s'està defensant aquí la tecnoregulació, és a dir, la protecció de la privadesa sempre amb eines garants. Doncs bé, les xarxes socials ens ensenyen també el límit de la protecció tecnològica. Com a màxim, la protecció de la xarxa social pot protegir la privadesa individual dels usuaris que es troben en la mitjana estadística: és a dir, que interactuen amb els altres de manera habitual. Aquests usuaris estan protegits si s'implementen garanties col·lectives com les indicades. En canvi, els que interactuen més que la mitjana –per exemple, penjant més informació o tenint més contactes del que és habitual– no es troben protegits per la tecnologia garant. Simplement, són massa fàcils d'individualitzar estadísticament. Per tant, la darrera protecció és l'educació i la informació: cal saber que, si tenim un comportament no habitual, llavors no hi ha protecció tecnològica eficaç que hi valgui. Això caldria explicar-ho en els sistemes educatius, i fins i tot divulgar informació estadística general de la xarxa per poder camuflar el comportament propi amb el de la majoria dels altres usuaris.

7 Com saber si la tecnologia garant és eficaç?

La comunitat jurídica no sembla haver prestat més atenció a la comunitat tecnològica després de la crida a la tecnologia garant. En el cas de les tecnologies garants de la privadesa, com hem dit, no s'ha indicat als tecnòlegs que havien d'optar per la biomètrica no traçable i no, en canvi, per la biomètrica multimode. Tampoc els tecnòlegs han avisat els juristes que usaven un concepte de privadesa amb protecció col·lectiva en les xarxes socials. De fet, els juristes no hem mostrat gaire interès a saber si les tecnologies, suposadament garants, ho eren en realitat.

L'absència de preocupació en la comunitat jurídica mostra el profund desconeixement sobre la capacitat reguladora de la tecnologia. Segons el dret, la tecnologia garant només hauria d'aplicar els principis jurídics, cosa que l'hauria de fer útil *per se* a la protecció de la privadesa. Totes les opcions de l'enginyer són amagades en una caixa negra, de la qual surt una eina que desenvolupa els principis legals. La tecnologia és vista com

una eina d'aplicació del dret, no com una opció correguladora. Per això la ineficàcia o fins i tot la protecció d'altres conceptes de privadesa no provoca una reacció. La regulació, que s'entén únicament com jurídica, no se'n veuria afectada. Doncs bé, creiem que no és així.

La comunitat tècnica té clar que ha de validar l'eficàcia de les seves solucions, i ho fa al marge del dret –i sense el reconeixement jurídic que es mereix. Algunes mètriques són simples avaluacions de riscos, que fixen uns objectius a assolir i classifiquen segons els nivells assolits (Alsubaei et al., 2019). Aquests treballs haurien de poder ser fàcilment admesos en el camp jurídic després que l'RGPD incorporés les avaluacions d'impacte. Altres mètriques són sectorials, com, per exemple, les que se centren en les xarxes socials o l'anonimització de grafs (Casas, 2019, 2020; Zhang et al., 2019). Altres, en canvi, prenen una aproximació més general –i més interessant– i pretenen avaluar la garantia de privadesa en funció de les expectatives d'obtenir la informació per part de l'atacant (Rebollo et al., 2013). Aquí la privadesa tècnica s'apropia de la privadesa jurídica: l'expectativa de privadesa d'un usuari ve a ser la possibilitat que un atacant pugui accedir a les seves dades. La majoria de propostes, en canvi, semblen centrar-se en l'equilibri entre la precisió de l'eina i les garanties per a la privadesa (Sheikhalishahi et al., 2021). Per tant, només intenten evitar que es perdi precisió quan es vol protegir la privadesa de l'usuari.

En definitiva, la privadesa és un dret fonamental individual, definit, i que cal preservar en la seva integritat. En canvi, els enginyers conceben les tecnologies garants de la privadesa com una cursa d'armaments (*arms race*), talment com si es tractés d'un tema de criptografia o seguretat. Sembla cada cop més clar que no es podrà mai tenir la tecnologia definitiva que asseguri del tot la privadesa. Només es pot pretendre, en el millor dels casos, contrarestar i dificultar al màxim i temporalment els atacs. La privadesa és un àmbit de victòries temporals –o de derrotes temporals, depèn de com es miri–, un esforç tan necessari com limitat. Ni més, ni menys.

8 La necessària institucionalització de la crida a la tecnologia

Amb una mètrica de la privadesa podrem començar a valorar el nivell de protecció de les eines garants. Es podrà llavors descartar una eina per inadequada –primer criteri en el test de proporcionalitat– i també es podrà establir una prelació entre eines eficaces, preferint les menys invasores sobre els drets. Això permetrà realment aplicar el control de necessitat –segon criteri del test de proporcionalitat. També constituirà una informació rellevant per poder valorar finalment si la mesura aporta més beneficis o perjudicis –tercer aspecte del test de proporcionalitat. Tot i aquests avantatges, aquesta informació no serà realment útil si no descansa en una plataforma institucional que garanteixi, d'una banda, la presència del legislador, i, de l'altra, dels actors i usuaris afectats.

La Unió Europea concep eines de millor legislació (*better regulation*) i de corregulació.[14] Doncs bé, una comunitat conjunta de juristes experts en privadesa i de tecnòlegs especialitzats en eines garants seria una molt bona manera de millorar la regulació. Com ja hem dit, la decisió sobre les diferents tecnologies garants requereix un treball simultani, no una interpretació *a posteriori* d'uns principis o criteris. La Comissió Europea, en el marc del seu programa Better Regulation, ja aplicat des del principi de la passada dècada, ha vinculat cada cop més les avaluacions d'impacte amb una avaluació prèvia dels resultats de la legislació anterior. Existeix, en aquest sentit, un comitè de control reglamentari, encarregat d'assessorar el legislador.

De totes maneres, la Unió Europea no ha fet encara el pas cap a una institucionalització de la corregulació en plataformes digitals amb participació del legislador i que adoptin una dinàmica cíclica. Ens referim, amb l'expressió "dinàmica cíclica", a estratègies reguladores que difuminin la tradicional successió de regulació-aplicació per crear cicles permanents de regulació-aplicació-regulació. Creiem que les avaluacions d'impacte *ex ante* combinades amb les avaluacions d'impacte *ex post* podrien servir a aquest efecte. Sigui com sigui, Plataforma REFIT i Fit for Future Platform són eines més limitades, de simplificació, de participació i d'eficiència de la tècnica legislativa tradicional.[15] Resta per veure el seu potencial transformador davant la regulació de les noves tecnologies.

14 Vegeu, sobre aquesta qüestió, la comunicació *Better Regulation. Joining forces to make better laws*.

15 Decisió de la Comissió d'11 de maig de 2020, que estableix la Fit for Future Platform (C(2020) 2977 final). Decisió de la

La governança de la intel·ligència artificial o governança algorítmica sembla un altre bon exemple per veure aparèixer plataformes correguladores (Roig, 2020). En aquests casos, l'autoritat pública especialitzada hauria d'assumir un rol actiu en la dinamització de les plataformes.[16] S'obre, per tant, una oportunitat de dinamisme regulador en el marc de les noves tecnologies.

De moment, però, sembla que aniran apareixent, en el millor dels casos, plataformes informals de programes de recerca europeus, amb tasques parcialment colegislatives (Roig, 2018). Aquest és el cas en nanotecnologia, on han aparegut plataformes informals al voltant de projectes europeus, els resultats de les quals han estat adoptats posteriorment pel legislador. El problema d'aquesta dinàmica informal o no institucionalitzada és la manca de participació del legislador. És a dir, ningú ha defensat l'interès general. Una autèntica corregulació no pot prescindir del legislador. La distància entre regulació i aplicació s'està reduint, i sembla que veurem aparèixer progressivament cada cop més formes cícliques, de manera més o menys institucionalitzada.

9 Conclusions

La crida a la tecnologia garant no és un moment de ruptura en l'actual paradigma de monopoli regulador jurídic. Es tracta només d'incorporar una eina d'aplicació dels principis i drets previstos en el dret. Si més no, aquesta semblava la idea inicial. Hem intentat descriure, en aquest treball, les limitacions que, al nostre parer, suposa aquesta perspectiva originària de les tecnologies garants.

La primera, sovint no prevista pels juristes, és la conveniència o no de recórrer a les tecnologies garants. Tot i que pugui semblar paradoxal, l'eina garant pot incorporar nous riscos, i caldrà sotmetre la decisió d'usar aquesta tecnologia a un judici d'oportunitat, a una valoració sobre si els avantatges superen els riscos.

També esdevé cada cop més necessari valorar l'eficàcia de les tecnologies garants. Una eina ineficaç no només pot incorporar riscos, com dèiem, sinó que, a més, pot donar una falsa sensació de protecció o ser usada per legitimar una mesura reguladora.

Una bona part del problema rau en la manca de col·laboració entre les comunitats jurídiques i tècniques. No serà possible gestionar la corregulació de les tecnologies garants sense una recepció i validació per part d'alguna institució jurídica de les preferències d'algunes eines garants sobre d'altres, tenint en compte la seva afectació sobre drets i principis generals.

Això hauria de permetre, si més no de manera dialèctica i amb constants actualitzacions i revisions, evitar que s'utilitzin de manera generalitzada tècniques suposadament garants que, de fet, poden arribar a comprometre drets fonamentals.

La col·laboració entre les comunitats hauria de posar en evidència l'ús de conceptes no jurídics per part dels enginyers de les eines garants. D'aquest diàleg en poden sortir aspectes molt interessants per a la comunitat jurídica, com la defensa col·lectiva per tal de garantir drets individuals. És possible defensar el dret a la privadesa sense tecnologies garants? Si fos el cas, els juristes llavors hauríem de fer l'esforç de renovar la capacitat protectora del dret, si no volem ser còmplices, per acció o omissió, de la seva irrellevància pràctica com a garantia.

Sembla clar que la tecnologia no esborrarà la necessitat de regulació –potser fins i tot l'accentuarà. Però el que sí que pot passar és que hi hagi diverses "regulacions" simultànies: algunes reconegudes, però ineficaces, i d'altres emprades, tot i que informals o amb dinàmiques completament distanciades dels principis del dret i dels seus valors i drets fonamentals. No és un escenari desitjable, ni tampoc inevitable.

Comissió de 19 de maig de 2015, que estableix la Plataforma REFIT (C(2015) 3261 final).

16 El 21 d'abril de 2021, la Comissió Europea va presentar la Proposta de Reglament del Parlament i del Consell pel qual s'estableixen normes harmonitzadores en matèria d'intel·ligència artificial (Llei d'intel·ligència artificial) i es modifiquen certs actes legislatius de la Unió [SEC(2021) 167 final], [SWD(2021) 84 final], [SWD(2021) 85 final]. Els articles 56 a 58 d'aquesta proposta preveuen i regulen el Comitè Europeu d'Intel·ligència Artificial, que podria ser un actor important a l'hora de vertebrar espais de corregulació. Caldrà veure'n el text definitiu i el seu desenvolupament pràctic en els propers anys. També es parla que podria haver-hi el 2023 una Agència Estatal d'Avaluació d'Algoritmes. Junt amb la certificació, es podria pensar també, en aquest cas, en una funció dinamitzadora, amb plataformes de coregulació.

Ha arribat el moment d'institucionalitzar la col·laboració entre comunitats. Hi ha alguns exemples de corregulació incipient –com en nanotecnologia–, però no s'hi preserven els interessos generals, els drets ni els principis. La governança de la intel·ligència artificial pot ser una altra oportunitat a seguir. Caldrà estar-hi atents per veure si es pot, de retruc, vertebrar una plataforma per a les eines garants.

Referències

Alsubaei, Faisal, Abuhussein, Abdullah, i Shiva, Sajjan. (2019). A framework for ranking IoMT solutions based on measuring security and privacy. Dins Kohei Arai et al. (ed.), *Proceedings of the Future Technologies Conference (FTC) 2018* (p. 205-224).

Anakath, Arasan, Rajakumar, S., i Ambika, S. (2019). Privacy preserving multi factor authentication using trust management. *Cluster Computing*, *22*.

Aved, Alexander J., i Hua, Kien A. (2012). A general framework for managing and processing live video data with privacy protection. *Multimedia Systems*, *18*, 123-143.

Bygrave, Lee A. (2017). Data protection by design and by default: Deciphering the EU's legislative requirements. *Oslo Law Review*, *4*(2), 105.

Bygrave, Lee A. (2020). Article 25. Data protection by design and by default. Dins Christopher Küner, Lee A. Bygrave i Christopher Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary* (p. 571-581). Oxford University Press.

Casas Roma, Jordi. (2019, 15 de juny). An evaluation of vertex and edge modification techniques for privacy-preserving on graphs. *Journal of Ambient Intelligence and Humanized Computing*.

Casas Roma, Jordi. (2020). DUEF-GA: Data utility and privacy evaluation framework for graph anonymization. *International Journal of Information Security*, *19*, 465-478.

Cavoukian, Ann. (2011 [2009]). *Privacy by Design: The 7 Foundational Principles*.

Dwork, Cynthia. (2006). Differential privacy. Dins Michele Bugliesi, Bart Preneel, Vladimiro Sassone i Ingo Wegener (ed.), Automata, Languages and Programming. ICALP 2006. *Lecture Notes in Computer Science* (vol. 4052). Springer. https://doi.org/10.1007/11787006_1

European Union Agency for Network and Information Security (ENISA). (2014). *Privacy and data protection by design. From Policy to Engineering*.

European Union Agency for Network and Information Security (ENISA). (2016). *Privacy enhancing technologies: Evolution and state of the art. A community approach to PETs Maturity Assessment*.

European Union Agency for Cybersecurity (ENISA). (2019). *Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions*.

European Union Agency for Cybersecurity (ENISA). (2021). *Data pseudonymisation: Advanced techniques & use cases. Technical analysis of cybersecurity measures in data protection and privacy*.

Gao, Jianliang, Wang, Jianxin, He, Jianbiao, i Yan, Fengxia. (2019). Against signed graph deanonymization attacks on social networks. *International Journal of Parallel Programming*, *47*, 725-739.

Gu, Qiuyang, Ni, Qilian, Meng, Xiangzhao, i Yang, Zhijiao. (2019). Dynamic social privacy protection based on graph mode partition in complex social network. *Personal and Ubiquitous Computing*, *23*, 511-519.

Gupta, Keshav, Walia, Gurjit Singh, i Sharma, Kapil. (2021). Novel approach for multimodal feature fusion to generate cancelable biometric. *The Visual Computer*, *37*, 1401-1413.

Klitou, Demetrius. (2014). A solution but not a panacea for defending privacy: The challenges, criticism and limitations of privacy by design. Dins Bart Preneel i Demosthenes Ikonomou (ed.), *Privacy Technologies and Policy* (p. 86-110). First Annual Privacy Forum, APF 2012. Springer.

Manisha Kumar, Nitin. (2020). Cancelable biometrics: a comprehensive survey. *Artificial Intelligence Review*, *53*, 3403-3446.

Purohit, Himanshu, i Ajmera, Pawan K. (2021). Optimal feature level fusion for secured human authentication in multimodal biometric System. *Machine Vision and Applications*, *32*(24).

Rajabzadeh, Sara, Shahsaf, Pedram, i Khoramnejadi, Mostafa. (2020). A graph modification approach for k-anonymity in social networks using the genetic algorithm. *Social Network Analysis and Mining*, *10*(38).

Rebollo, David, Parra, Javier, Díaz, Claudia, i Forné, Jordi. (2013). On the measurement of privacy as an attacker's estimation error. *International Journal of Information Security*, *12*, 129-149.

Roig, Antoni. (2018). Nanotechnology governance: From risk regulation to informal platforms. *NanoEthics*, *12*(2), 115-121.

Roig, Antoni. (2020). *Las garantías frente a las decisiones automatizadas. Del reglamento general de protección de datos a la gobernanza algorítmica*. Bosch Editor.

Rubinstein, Ira S. (2012). Regulating privacy by design. *Berkeley Technology Law Journal*, *26* (3), 1409-1456.

Schaar, Peter. (2010). Privacy by design. *Identity in the Information Society*, *3*(2), 267-274.

Schartum, Dag Wiese. (2016). Making privacy by design operative. *International Journal of Law & Information Technology*, *24*(2), 151-175.

Sheikhalishahi, Mina, Saracino, Andrea, Martinelli, Fabio, i La Marra, Antonio. (2021). Privacy preserving data sharing and analysis for edge-based architectures. *International Journal of Information Security*.

Shen, Jie, Cai, Ying-Jue, i Luo, Lei. (2015). A context-aware mobile web middleware for service of surveillance video with privacy. *Multimedia Tools and Applications*, *74*, 8025-8051.

Tamò-Larrieux, Aurelia. (2018). *Designing for privacy and its legal framework: Data protection by design and default for the Internet of Things*. Springer.

Torra, Vicenç. (2017). *Data privacy: foundations, new developments and the big data challenge*. Springer.

Werner, Jorge, Westphall, Carla Merkle, Azevedo Vargas, Andre, i Westphall, Carlos Becker. (2019). *Privacy Policies Model in Access Control*. IEEE International Systems Conference. Orlando, Florida, EUA.

Yang, Liu, Yong, Zeng, Zhihong, Liu, i Jianfeng, Ma. (2021). Spectrum privacy preserving for social networks: A Personalized Differential privacy approach. Dins Yongdong Wu i Moti Yung (ed.), *Inscrypt 2020, Lecture Notes in Computer Science*, 12612 (p. 277-287).

Yiping, Yin, Qing, Liao, Yang, Liu, i Ruifeng, Xu (2019). Structural-based graph publishing under differential privacy. Dins Ruifeng Xu et al. (ed.), *Cognitive Computing – ICCC 2019. Third International Conference* (p. 67-78). (Lecture Notes in Computer Science, 11518).

Zhang, Cheng, Jiang, Honglu, Cheng, Xiuzhen, Zhao, Feng, Cai, Zhipeng, i Tian, Zhi. (2019). *Utility analysis on privacy-preservation algorithms for online social networks: an empirical study*. Springer.