Cap a un mètode d'avaluació d'impacte per a la protecció de dades: Donant sentit a les obligacions del RGPD

Kloza, Dariusz; Van Dijk, Niels; Casiraghi, Simone; Vazquez Maymir, Sergi; Roda, Sara; Tanas, Alessia; Konstantinou, Ioulia; Vazquez Maymir, Sergi

Published in:
d.pia.lab Policy Brief

Publication date:
2020

Document Version:
Final published version

Cap a un mètode d'avaluació d'impacte per a la protecció de dades: Donant sentit a les obligacions del RGPD

d.pia.lab Nota normativa No. 1/2019

Dariusz KLOZA, Niels VAN DIJK, Simone CASIRAGHI, Sergi VAZQUEZ MAYMIR,
Sara RODA, Alessia TANAS i Ioulia KONSTANTINOU
Laboratori d'Avaluació d'Impactes en Privacitat i Protecció de Dades de Brussel·les (d.pia.lab)

Aquesta nota normativa estableix els fonaments per a un mètode d'avaluació d'impactes en matèria de protecció de dades (AIPD) a la Unió Europea. En primer lloc i com a requisit previ, proposa un mètode genèric d'avaluació, que pretén ser utilitzat – en tant que adaptat al context particular – a diversos dominis, com ara la pràctica mediambiental, el desenvolupament tecnològic o el legislatiu (Secció 2ª). Tot seguit, en base a aquest mètode genèric i tenint en compte les obligacions establertes pel Reglament General de Protecció de Dades (RGPD), la nota estableix la base d'un mètode específic per a dur a terme un procediment d'AIPD a la UE adaptable a contextos concrets. La present nota normativa, té per objecte la clarificació de dos aspectes crucials d'aquest mètode que a dia d'avui han demostrat ser altament contenciosos. Per una banda, les tècniques de valoració (és a dir, l'avaluació de la necessitat i proporcionalitat i la valoració de riscs), i de l'altre, la implicació de les parts interessades (incloent-hi la participació de la societat) en la presa de decisions. La secció 4ª ofereix un resum de les conclusions fent una crida a una major orientació, clarificació i adaptació. Aquesta nota normativa, es dirigeix principalment als agents polítics responsables de desenvolupar mètodes d'avaluació d'impacte, als professionals que adapten aquests mètodes al context d'usos concrets i als assessors experts que duen a terme procediments d'avaluació d'acord amb aquests mètodes.

1 INTRODUCCIÓ

1.1 CONTEXT

El Reglament General de Protecció de Dades (RGDP o Reglament) suposa la clau de volta del reformat marc legal de protecció dades a la Unió Europea. El Reglament proporciona una plètora de solucions per a, *inter alia*, assegurar un "nivell coherent i elevat de protecció a les persones físiques" (Considerant 10) en aquells casos on hi hagi un tractament de dades personals. D'entre les seves novetats destaca l'obligació del responsable del tractament de realitzar una avaluació d'impactes en matèria de protecció de dades (AIPD), amb caràcter previ al inici del tractament de dades personals. Aquest procediment serà necessari sempre que els tractaments contemplats puguin, comportar un "alt risc per als drets i llibertats de les persones físiques" (Article 35(1)), i es durà a terme a fi "d'assegurar la protecció de les dades personals i per a demostrar el compliment amb la llei" (Article 35 (d)).

El AIPD representa una forma d'avaluació d'impactes (AI) i – a grans trets – suposa una variació de l'avaluació d'impacte de privacitat (AIP). En termes generals, un avaluació d'impactes és una tècnica d'avaluació utilitzada per analitzar les possibles conseqüències d'una iniciativa respecte d'un interès o interessos socials (e.g. assumpte o assumptes d'interès o importància). Quan una iniciativa pugui suposar un perill per a un interès o interessos, es realitzarà un AIPD per a facilitar una decisió informada respecte el seu desplegament, les seves condicions o si escau el seu rebuig. L'AIPD s'erigeix – primordialment – com una eina de protecció dels interessos socials que puguin resultar compromesos per una operació de tractament.

L'obligació de dur a terme un AIPD cristal·litza la visió de risc envers a la protecció de dades personals que impera en el reformat marc legal de la EU, i que enforteix el principi de responsabilitat establert pel mateix marc (Article 5(2)). Elaborant sobre l'experiència de tècniques d'avaluació en altres dominis (e.g. mediambiental, tecnològic o avaluacions d'impacte reguladors), l'AIPD té per objecte esdevenir una eina potent per assegurar el compliment i l'aplicació de la llei de protecció de dades personals.

 | ISSN 2565-9936

El procediment d'AIPD està sent exportat progressivament a d'altres instruments de protecció de dades dins el marc de la EU. Més enllà del RGPD, a dia d'avui trobem l'obligació legalment vinculant de dur a terme un AIPD dins la Directiva 2016/680, sobre la protecció dades en assumptes penals (Article 27), al Reglament 2018/1725 de protecció de dades personals tractades per les institucions, òrgans i agències de la Unió (Article 39 i 89), i a la Directiva 2019/1024 sobre dades obertes i la re-utilització de la informació en el sector públic (Considerant 53). De ser adoptada en el seu redactat actual la proposta de Reglament sobre Privacitat i Comunicacions electròniques, també inclourà l'obligació de realitzar un AIPD en determinades situacions (Article 6). Anteriorment, la UE ja havia experimentat amb marcs voluntaris per a la realització d'un AIP i AIPD, en la identificació de radio freqüències (RFID) i les "xarxes intel·ligents d'electricitat". En la mateixa línia, el Conveni 108 del Consell d'Europa proporciona el mandat legal per a establir obligacions comparables (Article 10(2)). Fora d'Europa, diverses formes de AIP i AIPD han estat desenvolupats en països com Austràlia, Canada, Japó, Sud Àfrica, Corea del Sud, Estats Units i Nova Zelanda. Tanmateix, organitzacions internacionals com el Comitè Internacional de la Creu Roja, també preveuen procediments d'avaluació en els seus estatuts.

Aquesta obligació jurídica i vinculant de realitzar AIPD a la EU genera un nombre d'interrogants, degut, entre d'altres, a la introducció de conceptes clau sobre els que una AIPD es fonamenta (e.g. risc envers a drets i llibertats), la freqüent vaguetat terminològica de la normativa reguladora (e.g. "gran escala" o "de forma sistemàtica") o la quantia relativa de les sancions en cas d'inobservança i males pràctiques. La introducció de conceptes propis de l'AIPD tot i atorgar flexibilitat a l'instrument també afecten negativament la seva seguretat jurídica, fent necessària una interpretació i orientació normativa. En el moment de presentar-se la proposició de reforma del marc legal relatiu a la protecció de dades personals, la Comissió Europea va descriure la seva formulació com la d'un "trincatge jurídic", en tant que el legislador havia de procurar expressar el mínim d'aquells elements considerats essencials. Qualsevol altre especificació, de ser necessària, s'esperava provinent per exemple, de les industries o sectors públics rellevants. Únicament en cas que aquests esforços fossin insuficients o errats, el legislador hauria d'intervenir. En aquest sentit, l'any 2017, el llavors Grup de Treball de l'Article 29, va emetre les línies directrius a la EU sobre AIPD i la determinació de quan una operació de tractament de dades "podia comportar un alt risc". Les guies van clarificar alguns aspectes relatius tant al marc legal com al mètode (e.g. llindar d'anàlisi), tot i que van tractar altres aspectes de forma merament superficial (e.g. la necessitat i proporcionalitat de l'avaluació o les parts implicades). A dia d'avui, l'orientació acadèmica i professional no n'ha proporcionat tampoc molta claredat. Un dels aspectes que cal il·lustrar és el relatiu al mètode, és a dir, el conjunt d'etapes per a dur a terme una avaluació. Això és precisament el que el aquesta nota normativa pretén abordar.

1.2 ANTECEDENTS

L' "arquitectura" d'una avaluació d'impactes està conformada normalment per dos elements, el *marc* i el *mètode*. El *marc* constitueix l'estructura de suport essencial o arranjament organitzacional, que en aquest context, està relacionat amb la política d'avaluació d'impactes i que defineix i descriu, les condicions principals de la mateixa. D'altra banda, el *mètode*, és un "procediment particular per acomplir o assolir un fi", es refereix a la realització de l'avaluació d'impacte i defineix les etapes iteratives o consecutives que s'han de realitzar per a dur-lo a terme. El mètode correspon al marc i s'ha d'entendre com un reflex pràctic del mateix. Aquesta "arquitectura" sovint es troba suplementada per unes guies (o manuals) i formularis, que desenvolupen l'avaluació del procés i ajuden en l'estructuració del procediment i la redacció d'un informe documental.

Són nombrosos els marcs i mètodes d'avaluació d'impactes existents en diversos dominis pràctics, amb aplicabilitat i qualitat diversa. La necessitat constant de nous marcs i mètodes, és una de les conseqüències del principi de receptivitat de l'avaluació d'impactes. El principi de receptivitat comporta que marcs i mètodes hagin de ser refinats contínuament per a que l'avaluació pugui assolir millor els seus objectius (a través de les lliçons apreses d'experiències pròpies o les experiències d'altres), pugui respondre millor a canvi socials, i resulti aplicable a nous àmbits pràctics que requereixin d'una avaluació d'impacte concreta (tals com per exemple, la recentment proposat avaluació d'impacte algorítmica).

1.3 ESTRUCTURA

En aquesta nota normativa, el d.pia.lab, estableix els fonaments d'un mètode específic per a la realització d'un AIPD a la Unió Europea. Com a condició preliminar, es proposa un mètode genèric per a realitzar avaluacions d'impactes de cara a que, d'acord amb el context particular (e.g. indústria, sector administratiu), es pugui fer servir en múltiples dominis, com ara el mediambiental, el de desenvolupament tecnològic, o el legislatiu (Secció 2).

El mètode genèric reflecteix un marc de 16 principis per a l'avaluació d'impactes en diversos àmbits pràctics, i que va ser desenvolupat pel d.pia.lab en la seva nota normativa prèvia (2017). El segon mètode és específic per

al domini de la protecció de dades personals i, més concretament, fa referència al procediment de l'AIPD a la UE. El mètode específic està dissenyat tenint en compte allò establert pel RGPD i d'acord amb el mètode genèric (Secció 3). Aquest mètode específic també haurà de ser ajustat al context d'ús concret. Per a la seva elaboració, el d.pia.lab s'ha centrat particularment en els aspectes més contenciosos, com sónla participació de les parts interessades (inclosa la participació de la societat) en la presa de decisions, la necessitat i proporcionalitat de l'avaluació i l'avaluació dels riscs envers als drets i llibertats de les persones. Ambdós mètodes estan construïts mitjançant un pensament crític i a través de l'anàlisi comparatiu de marcs ja existents, en particular els relatius a la privacitat, la protecció de dades, el desenvolupament tecnològic, l'àmbit mediambiental, l'àmbit regulador i el dels drets humans.

Aquesta nota normativa té dos destinataris principals. En primer lloc els responsables polítics, particularment les autoritats de protecció de dades (APD) tant a nivell de la EU com dels Estats Membres, que necessitin desenvolupar mètodes d'AIPD ajustats al seu context nacional. En segon lloc a aquelles parts que estiguin interessades en adaptar aquests mètode d'AIPD a un context d'ús particular i eventualment als responsables de tractament que hagin de realitzar avaluacions. Tanmateix, confiem que el mètode genèric pugui ser utilitzat en tot aquells dominis on es duen a terme avaluacions d'impacte.

2 UN MÈTODE GENÈRIC PER A L'AVALUACIÓ D'IMPACTES

El mètode genèric proposat, es basa en un anàlisi comparatiu i en una crítica a les etapes que es troben habitualment a d'altres dominis i que han estat emprats i enriquits d'acord amb l'experiència del d.pia.lab. Paral·lelament, el mètode genèric reflecteix el marc de 16 principis proposat pel d.pialab a la seva nota normativa de 2017.

El mètode genèric proporciona els fonaments per a desenvolupar mètodes d'avaluació d'impacte específics a múltiples dominis. Es troba estructurat en deu etapes (sis de consecutives, tres de continuades durant tot el procés i una etapa que ha de ser realitzada posteriorment), agrupades en cinc fases. Alguna d'aquestes etapes segueixen una seqüencia lògica, mentre que d'altres són resultat dels principis que encarna el propi marc. Les etapes són les següents:

Fase I: Preparació del procediment d'avaluació

1) *Exploració o mapatge (anàlisi del llindar).* Aquesta etapa determina si una iniciativa o altres iniciatives similars, han de dur a terme o no una avaluació d'impacte donat un context concret. L'exploració està basada en una descripció inicial encara que suficientment detallada de la iniciativa tant a nivell tècnic com de context. La decisió es prendrà d'acord a un llindar, que serà tant intern (e.g. les pròpies polítiques de l'organització), extern (e.g. requeriments per llei o per altres reglaments), o *ad hoc*, com per a bé la pressió social exercida per l'opinió pública. Si un procediment d'avaluació es considera innecessari o no exigible, l'avaluació finalitza amb una declaració raonada del perquè no existeix un impacte significant.

2) *Especificació.* A partir de la descripció inicial aquesta etapa tracta d'identificar:
   a) la preocupació, inquietud o interès social, que pugui veure's afectat per la iniciativa plantejada, com ara la privacitat, la protecció de dades, l'ètica (aplicada), l'entorn natural o humà, i els corresponents requeriments legals o reglamentaris. Aquests interessos socials constitueixen els paràmetres de referència per a l'avaluació d'impacte;
   b) grups d'interès o parts *(stakeholders),* les parts afectades, aquelles parts que podrien veure's afectades, les que estiguin interessades amb la iniciativa plantejada, o que disposin d'un coneixement específic. De totes elles s'haurà d'especificar el grau d'implicació;
   c) les tècniques (mètode *sensu stricto*) per a la valoració dels impactes i per a la implicació de les parts, incloent-hi la participació d'aquestes en el procés de decisió, i que s'haurà d'utilitzar durant tot el procés d'avaluació;
   d) altres tècniques d'avaluació, més enllà del propi procés d'avaluació d'impacte, que puguin ser considerades necessàries o requerides per tal d'assegurar, per exemple, la exhaustivitat de la informació usada en el procés de presa de decisions (e.g. avaluació tecnològica o mediambiental).

   No tots els elements ni persones mencionades hauran o podran ser identificables al principi del procés d'avaluació i, per tant, la identificació requerirà de revisions periòdiques.

3) *Planificació i preparació.* Aquesta etapa defineix els termes de referència per a la realització de l'avaluació. Aquests termes inclouen, entre d'altres:
   a) els objectius de l'avaluació;
   b) el criteri d'acceptabilitat dels impactes negatius;

c) la necessitat de recursos (e.g. diners, força de treball, coneixements, coneixements pràctics, establiments e infraestructura);
d) els procediments i els terminis de l'avaluació;
e) l'assessor o l'equip d'assessors (interns o externs), els seus rols i les seves responsabilitats, la garantia de la seva professionalitat, independència i coneixements;
f) la continuïtat del procés d´avaluació.

Fase II: Avaluació

4) *Descripció*. D'acord amb la descripció inicial (Etapa 1) aquest etapa proporciona una explicació dual de la iniciativa prevista. En primer lloc, una descripció de context, que normalment inclourà:
   a) una descripció de la iniciativa planificada i de l'entitat que la promou;
   b) el context per al desplegament de la iniciativa;
   c) la necessitat de la iniciativa;
   d) les possibles interferències amb interessos socials;
   e) els beneficis i inconvenients de la iniciativa.

   En segon lloc, hi ha una descripció tècnica. En el cas de les avaluacions d'impacte en l'àmbit mediambiental (EIA) això implicaria una descripció, dels components afectats en l'esfera biofísica de l'entorn, i en el cas dels AIPD, descriure les categories de dades personals i els seus fluxos dins l'operació de tractament.

5) *Valoració d'impactes*. En aquesta etapa, els impactes de la iniciativa prevista es valoren d'acord amb les tècniques prèviament seleccionades. Aquests impactes pertanyen al interessos socials dels actors que poden ser afectats per la iniciativa i que són externs als de l'entitat promotora. Normalment, aquesta valoració, consisteix – com a mínim – en una detallada identificació, anàlisi i avaluació dels impactes. Les tècniques de valoració poden comprendre des d'anàlisis de riscs (gestió qualitativa o quantitativa de riscs, o una combinació de les dues), anàlisis de l'escenari (planificació) i previsió tecnològica respecte a la seva compatibilitat amb els marcs legals i reglamentaris, un anàlisi de cost i benefici (CBA) o un anàlisi de fortaleses, debilitats, oportunitats i amenaces (SWOT).

Fase III: Recomanacions

6) *Recomanacions.* En aquesta etapa, es proposen mesures concretes i detallades (controls, garanties, solucions etc.), els destinataris de les mateixes, les prioritats així com els terminis per dur-les a terme de cara a minimitzar els impactes negatius de la iniciativa prevista i, en tant que possible, maximitzar-ne els positius. L'assessor justifica la diferenciació entre impactes negatius i positius, ja que aquesta distinció és contextual i subjectiva. L'assessor també haurà de fer recompte de les mesures ja implementades. A partir d'aquí, i després des la conclusió de l'avaluació, l'entitat promotora prendrà les decisions sobre l'execució de la iniciativa i sobre les condicions de la mateixa. Tanmateix, l'entitat promotora pot voler implementar recomanacions de forma progressiva durant el procés d'avaluació. Generalment una iniciativa es cancel·larà o serà rebutjada si els impactes negatius són considerats inacceptables; dur a terme una iniciativa d'aquestes característiques seria excepcional i requeriria d'una justificació suficient.

Fase IV: Etapes permanents

7) *Implicació de les parts, participació pública en el procés de presa de decisions*. Aquesta és una fase de caràcter permanent i transversal, que s'ha de dur a terme al llarg de tot el procés i en la que les parts i grups d´interès, incloent-hi la societat i els seus representats, participen del procés d'avaluació.

   Entès de forma extensiva, serà considerada part, tot aquell qui té una participació (interès) en quelcom, independentment de si n'és conscient o no, o bé si aquest interès està articulat directament o no. En el context de les avaluacions d'impacte, serà considerat part, aquell qui es trobi afectat (present), pugui veure's afectat (en el futur) o qui pugui (o no) veure's afectat per, o estar interessat amb la iniciativa proposada, tant positiva com negativament. Al mateix temps, una part també pot ser algú amb un coneixement específic o pràctic sobre la iniciativa, és a dir, un expert. El concepte de part és, per tant, un concepte obert i comprèn la societat entesa com la població (ciutadà corrent), actors polítics, experts etc. Les parts poden ser tant individus com entitats col·lectives, independentment de si estan formalment reconegudes com a tals (e.g. grups socials, comunitats, nacions, el gran públic, organitzacions de la societat civil etc.). Hi ha multiplicitat de grups d'interès o parts, i per tant aquests poden ser agrupats entre interns (e.g. empleats, comitès d'empresa) i externs (e.g. clients, organitzacions no governamentals) i entre primaris (aquells que tenen un interès directe en la iniciativa (inversors) i secundaris (aquells que influenciats indirectament e.g. els Estats), o classificats pels seus atributs: poder, legitimitat i urgència.

   La implicació de les parts representa un component integral del procés d'avaluació i en general només s'hauria d'ometre en situacions excepcionals. Si no es requereix o no es considera necessària la seva

implicació, aquesta haurà de ser una decisió raonada i documentada. Quan la implicació de les parts sigui obligatòria, i tot i així resulti insuficient o inexistent, s'hauran d'establir les garanties legals corresponents d'acord amb el nivell d'implicació desitjable pel procés d'avaluació. En qualsevol cas, la implicació de les parts no ha de comprometre la legítima confidencialitat (e.g. estatal o comercial), ni tampoc comportar conseqüències negatives per als seus participants (e.g. explotació).

El nivell o grau d'implicació pot comportar des de: a) la mera notificació a les parts de la iniciativa prevista (nivell baix); b) el diàleg i consulta: on es té en consideració les perspectives i opinions de les parts (nivell mig); o fins i tot c) la co-decisió amb les parts sobre l'execució de la iniciativa en qüestió i seva cooperació durant el desplegament (nivell alt).

Existeixen multitud de tècniques per a involucrar les parts, des de notes informatives, entrevistes, qüestionaris, enquestes, grups focals, taules rodones, tallers de ciutadans, i també tècniques estructurades com ara un "cafès globals" o enquestes "Delphy". La tècnica, o combinació de tècniques adequades hauran de ser seleccionades tenint en compte el nivell d'implicació de les parts que es desitja, la iniciativa prevista, el context de desplegament per a la iniciativa i els recursos disponibles per part de l'entitat promotora.

La participació dels grups d'interès pot comportar molts beneficis tant al procés d'avaluació (millorar la seva qualitat, credibilitat i legitimitat) com al resultat (la presa de decisions estarà millor informada). Tanmateix s'hauran de tindre també en compte els seus inconvenients, comprenent qüestions sobre representativitat (e.g. infra o sobre dimensionada), equitat o imparcialitat (e.g. manipulació, astroturfing), reticència a participar, barreres comunicatives, conflicte entre interessos públics i privats, i la naturalesa recurs-intensiva que suposa implicar totes les parts en el procés.

8) *Documentació.* Aquesta etapa té una naturalesa permanent i transversal, que s'estén-a tot el procediment, i que té per objecte la documentació de forma intel·ligible, per mitjà de registres, de forma escrita o en qualsevol forma o format, de totes les activitats que es duen a terme durant el procediment d'avaluació. Aquesta etapa inclou la preparació d'un informe final d'avaluació (o una declaració eximent). L'espectre complet de la documentació relativa a una determinada avaluació d'impacte, es trobarà preferiblement en format electrònic, i podrà arribar a ser accessible amb caràcter públic, registrada centralment, o proporcionada per inspecció sota demanda (amb el degut respecte per a la legítima confidencialitat).

9) *Control de qualitat.* Etapa permanent i transversal que s'estén a tot el procés d'avaluació i que comprova l'adherència a un estàndard de resultats concret, ja sigui de forma interna (e.g a través d'un monitoratge o revisió per l'entitat promotora) o externa (e.g. per una autoritat reguladora independent, a través d'una auditoria, o pels tribunals de justícia), o ambdues. El control de qualitat pot dur-se a terme durant o després del procediment d'avaluació, o en tots dos.

Fase V: Revisió

10) *Revisió.* En aquesta etapa es decideix si cal realitzar novament el procediment d'avaluació ja sigui total o parcialment. Aquesta etapa es pot repetir tantes vegades com vegades la iniciativa sigui modificada (abans o després del seu desplegament), o quan el context on s'ha de realitzar el tractament canviï. L'etapa de revisió assegura una continuïtat en el procediment d'avaluació, per exemple en el cas en que la iniciativa sigui transferida a una altre entitat.

El mètode d'avaluació d'impacte per a una iniciativa respecte d'aquells interessos socials connexes, té una naturalesa genèrica i cal ser adaptat a les especificitats i necessitats del domini o camp concret, a les parts involucrades així com al seu context d'ús. Per exemple, avaluar els impactes en matèria de protecció de dades a la EU implica un determinat plantejament, com a mínim durant la etapa d'*Exploració o mapatge* (criteri d'anàlisi de llindar), *Descripció* (e.g. llista d'interessos socials), *Valoració del tractament previst* (e.g. tècniques per a l´avaluació i llista de possible d'impactes), *Implicació de les parts, participació pública en el procés de presa de decisions* (e.g. parts i tècniques per a implicar-los) i la etapa de *Recomanacions*.

ARTICLES RELLEVANTS DEL REGLAMENT

Article 35º

1. Quan sigui probable que un tipus tractament, especialment si utilitza noves tecnologies, i tenint en compte la seva naturalesa, abast, context o finalitats, pot comportar un alt risc per als drets i les llibertats de les persones físiques, abans del tractament el responsable ha d'avaluar l'impacte de les operacions de tractament en la protecció de dades personals. Una única avaluació pot abordar una sèrie d'operacions de tractament similars que comportin alts riscos similars. […]

7. L'avaluació ha d'incloure, com a mínim:
   a) Una descripció sistemàtica de les operacions de tractament previstes i de les finalitats del tractament, inclòs, si escau, l'interès legítim perseguit pel responsable del tractament;
   b) Una avaluació de la necessitat i la proporcionalitat de les operacions de tractament, pel que fa a la seva finalitat;
   c) Una avaluació dels riscos per als drets i les llibertats dels interessats a què es refereix l'apartat 1, i
   d) Les mesures previstes per afrontar els riscos, incloses garanties, mesures de seguretat i mecanismes que garanteixen la protecció de dades personals i per demostrar la conformitat amb aquest Reglament, tenint en compte els drets i interessos legítims dels interessats i d'altres persones afectades. […]
9. Si escau, el responsable ha de recollir l'opinió dels interessats o dels seus representants en relació amb el tractament previst, sens perjudici de la protecció d'interessos públics o comercials o de la seguretat de les operacions de tractament.

Article 36º

1. El responsable consultarà a l'autoritat de control abans de procedir al tractament si una avaluació d'impacte relativa a la protecció de les dades, en virtut del que disposa l'article 35, mostra que el tractament comporta un alt risc, si el responsable no pren mesures per mitigar-lo.
2. Quan l'autoritat de control considera que el tractament a què es refereix l'apartat 1 pot infringir aquest Reglament, especialment quan el responsable ha identificat o mitigat suficientment el risc, l'autoritat de control, en un termini de vuit setmanes des de la sol·licitud de la consulta, ha d'assessorar el responsable per escrit, i si escau l'encarregat, i pot utilitzar qualsevol dels poders esmentats a l'article 58 […].

3 UN MÈTODE PER A L'AVALUACIÓ D'IMPACTES EN MATÈRIA DE PROTECCIÓ DE DADES DINS LA UNIÓ EUROPEA

El mètode específic d'AIPD exigit a la EU pel RGPD i descrit a continuació, ha estat interpretat d'acord amb els Articles 35-36, i tenint en compte el mètode genèric. El RGPD obliga al responsable del tractament, a dur a terme una avaluació i al encarregat del tractament, en cas de ser aplicable, a assistir al responsable. És el responsable del tractament qui haurà de retre comptes del procediment d'avaluació.

El Reglament preveu la realització de set etapes, concretament:

1) *Exploració o mapatge (anàlisi del llindar)*: a fi de determinar la necessitat legal del AIPD, s'haurà d'examinar les operacions de tractament proposades d'acord amb la seva descripció inicial, així com la valoració preliminar dels seus riscs i confrontar-les amb els següents sis criteris:
   - *Criteri 1 – plausibilitat del risc (general)*: d'una forma general, el Reglament exigeix la realització d'un AIPD quan sigui probable que un tipus de tractament, especialment si utilitza noves tecnologies, representi un risc envers els drets i llibertats dels interessats. L'avaluació haurà de tindre en compte quatre criteris qualitatius, en concret, la naturalesa del tractament, el seu abast, context i les seves finalitats (Article 35(1)). Aquests criteris, però no han estat definits més enllà i poden incloure per exemple, el tractament de categories especials de dades personals, dades relatives a antecedents i delictes, mesures de seguretat o dades biomètriques (i.e. la naturalesa de l'operació), la quantitat de dades tractades, l'envergadura geogràfica, el nombre de gent afectada (i.e. abast), l'ús d'una determinada tecnologia o l'àrea d'ús (e.g. data accessible públicament) (i.e. el context), o les dades per a l'elaboració de perfils o la presa de decisions automatitzades (i.e. el propòsit) (cf. Considerant 91). El llavors anomenat Grup de Treball de l'Article 29, va identificar nou criteris a considerar a l'hora de valorar si un tractament "pot comportar un risc elevat" (2017); exemples d'aquests criteris inclouen: si el conjunt de dades estan combinats o relacionats o si el tractament de dades personals té per objecte grups vulnerables. No obstant, recaurà sobre el responsable del tractament el haver de determinar si el risc és elevat.
   - *Criteri 2 – plausibilitat d'alt risc (enumeració)*: el Reglament preveu tres tipus de tractament de dades susceptibles de representar un risc elevat pels drets i llibertats dels interessats i per als quals serà necessari fer un AIPD. En altres paraules, els següents tractaments són, per llei, considerats com altament arriscats, aquest llistat no és exhaustiu:
     - "[a]valuació sistemàtica i exhaustiva d'aspectes personals de persones físiques basada en un tractament automatitzat, com l'elaboració de perfils, sobre la base de la qual es prenen decisions que produeixen efectes jurídics per a les persones físiques o que les afecten significativament de manera similar";

- tractament, a gran escala, de categories especials de dades personals o de dades relacionades amb condemnes i infraccions penals; i
- "[o]bservació sistemàtica a gran escala d'una zona d'accés públic" (Article 35(3)).

- *Criteri 3 – plausibilitat d'alt risc (enumeració positiva per part d'autoritats de protecció de dades)*: l'autoritat de control nacional o regional és competent per establir i publicar, dins la seva jurisdicció, un llistat d'aquelles operacions de tractament de dades per les quals es requerirà la realització d'un AIPD (Article 35(4)).
- *Criteri 4 – plausibilitat de risc elevat (enumeració negativa per part d'autoritats de protecció de dades)*: la mateixa autoritat també podrà establir i publicar un llistat d'altres tipus de tractaments pels quals una AIPD no sigui necessari (Article 35(5)). En tant que aquests llistats impliquin operacions de tractament transfronterers, els mateixos hauran de ser comunicats, aplicant un mecanisme de coherència, al Comitè Europeu de Protecció de dades (CEPD) per sol·licitar-ne la seva opinió (Article 35(4)-(6)). El CEPD emet aquestes opinions des de l'any 2018.
- *Criteri 5 – avaluació d'impactes reguladors previs*: llevat que els Estats Membres ho decideixin altrament, no caldrà la realització d'una AIPD pel tractament de dades personals en compliment d'obligacions legals (Article 6(1)(c)) o tractades en interès públic (Article 6(1)(e)). Tampoc caldrà realitzar una avaluació en aquells casos en que el mateix tractament tingui la base jurídica en el dret de la Unió o en el dret de l'Estat Membre al qual està subjecte el responsable del tractament, o si l'operació específica de tractament ja ha estat objecte d'avaluació en el context de l'adopció de la base legal, en tant que aquesta ja satisfà essencialment les condicions establertes per el RGPD (Article 35(10)).
- *Criteri 6 – exempcions per a determinades professions*: si l'objecte del tractament són dades personals de pacients per part d'un sol metge o un altre professional de la salut o els d'un advocat respecte dels seus clients, aquests tractaments no seran considerats de gran escala (Article 35(3)(b)) i la realització d'una AIPD no serà obligatòria (Considerant 91).

Si es satisfà qualsevol dels primers tres criteris, l'AIPD serà obligatori. Contràriament, si es compleix qualsevol dels tres darrers, el responsable del tractament estarà exempt de dur a terme l'avaluació.

2) *Descripció*: el Reglament requereix l'avaluació s'iniciï amb una descripció sistemàtica del tractament previst (Article 35(7)(a)). Concretament la descripció haurà d'incloure:
   a) *descripció contextual* dels tractaments previstos, particularment respecte la seva naturalesa, objecte, context i finalitat, el interès legítim del responsable del tractament (quan sigui aplicable) i el de les parts implicades (interessats, responsables del tractament, encarregat del tractament, terceres parts i autoritats públiques);
   b) *descripció tècnica* incloent els fluxos de dades personals i – a ser possible – la seva visualització.

   La descripció del tractament proposat es pot basar en la descripció que feta servir per determinar si el procediment d'avaluació era necessari en primera instancia (cf. Etapa 1).

3) *Valoració del tractament previst o del conjunt de tractaments*: el Reglament requereix l'ús, ja sigui de forma consecutiva o en paral·lel, d'almenys dues tècniques de valoració (mètodes *stricto sensu*): la valoració de la necessitat i proporcionalitat i la valoració de riscs. Ambdues tècniques, són, a grans trets, una novetat dins el dret de protecció de dades. Formulades com un "trincatge jurídic", la seva estipulació al RGPD resulta genèrica i no s'estipula explícitament com s'han d'utilitzar.
   a) L'avaluació de "la necessitat i la proporcionalitat de les operacions de tractament, pel que fa llurs finalitats" (Article 35(7)(b)).

      L'avaluació de la necessitat i proporcionalitat comporta l'observança i respecte dels principis de protecció de dades (Article 5(1)). En particular, s'haurà tenir en compte el principi de limitació de la finalitat, és a dir, qüestionar si la finalitat del tractament no es pot aconseguir raonablement per altres mitjans (Considerant 39) tot assegurant que les dades personals es tractin amb "finalitats determinades, explícites i legítimes" i que posteriorment no se'n faci ús "de manera incompatible amb aquestes finalitats" (Article 5(1)(b)). Aquesta avaluació també s'estén al principi de licitud del tractament (Article 6), així com als principis de minimització de dades, el d'exactitud i el de limitació del termini de conservació. En altres paraules, qüestiona si les dades personals són tractades amb "licitud, lleialtat, i transparència", "de forma adequada, pertinent i limitada al que és necessari en relació amb les finalitats per a les quals es tracten", si les dades són i seran exactes, actualitzades i conservades durant un període no superior al necessari (Article 5(1)(a)-(e)).

L'avaluació s'haurà de fonamentar sobre la base d'un anàlisi empíric, a partir de proves suficients, clarament descrites i verificables. A l'hora de determinar el contingut de l'avaluació de necessitat i proporcionalitat s'haurà de distingir entre els tractaments propis del sector privat i aquells del sector públic. En relació a les operacions de tractament per part del sector públic caldrà distingir els casos d'elaboració de lleis i els d'aplicació de lleis.

b) L'avaluació dels "riscs envers als drets i llibertats dels interessats" (Article 37(5)(c)).

En el context d'un AIPD, l'avaluació de riscs es refereix a la identificació, anàlisi i avaluació de les possibles conseqüències negatives del tractament de dades i, més concretament, dels perjudicis que puguin ser causats per aquelles operacions. L'avaluació de riscs per als drets i llibertats fa referència als "danys i perjudicis físics, materials i immaterials" i comprendrà, per exemple, la discriminació, la usurpació d'identitat, el frau, les pèrdues financeres, els dany per a la reputació, la pèrdua de confidencialitat de dades subjectes al secret professional, la reversió no autoritzada de la seudonimització o qualsevol altre perjudici econòmic o social significatiu, que privi als interessats dels seus drets i llibertats, o que els hi impedeixi exercir el control sobre les seves dades personals, o resulti en un tractament no autoritzat de dades personals de persones vulnerables, en particular nens. (El Considerant 75 proporciona un llarg llistat d'exemples d'aquest tipus perjudicis; la identificació precisa dels riscs es realitzarà durant el procés d'avaluació.) La decisió sobre si un tractament comporta un risc i – subseqüentment – si el nivell d'aquest risc és alt, la prendrà el responsable del tractament en base a una avaluació objectiva (Considerant 76).

Els riscs que hauran d'avaluar-se a través de l'AIPD seran aquells relatius a les persones físiques, enteses com totes les interessades i la societat en sentit ample, no així els responsables del tractament o els encarregats del tractament. Aquests riscs estan relacionats amb el gaudi dels drets i llibertats per les persones i, per tant, no són mers riscs d'adequació normativa. Tenint en compte la finalitat del Reglament, els riscs analitzats tindran un abast més ample que el dret a la protecció de dades, i s'estendran a altres drets i llibertats de forma expansiva (El Considerant 4 indica drets com ara el respecte de la vida privada i familiar, del domicili i de les comunicacions; la llibertat de pensament, de consciència i de religió; la llibertat d'expressió i d'informació; la llibertat d'empresa; el dret a la tutela judicial efectiva i a un judici just; la diversitat cultural, religiosa i lingüística.)

Els riscs envers als drets i llibertats són majoritàriament valorats qualitativament, és a dir avaluant-ne la severitat (magnitud del risc) i plausibilitat (certesa d'ocurrència e.g. baixa, mitja o alta) tenint com a referència l'origen, particularitat (Considerant 84) i la naturalesa, abast, el context i les finalitats del tractament de dades (Considerant 75-76). Certs riscs dins la protecció dades, com ara els riscs de seguretat, poden ser valorats quantitativament (e.g. calculant-ne la severitat i probabilitat). La valoració del risc es pot basar en la valoració inicial utilitzada per determinar si l'avaluació és necessària (cf. Etapa 1).

4) *Implicació de les parts (participació publica) en el procés de decisió*: el Reglament contempla que "si escau", es realitzin consultes amb els interessats o els seus representants, sens perjudici de la legítima confidencialitat (e.g. protecció d'interessos públics o comercials o de la seguretat de les operacions de tractament" (Article 35(9)). La "conveniència" de la consulta no ha de ser entesa com a "opcionalitat". De forma excepcional, no es consultarà a les parts quan, per exemple, no es pugui obtenir cap perspectiva o coneixement nou amb la seva implicació o aquesta requereixi d'uns esforços desproporcionats respecte dels seus potencials resultats. La decisió de no implicar a les parts, o de desviar-se dels resultats obtinguts per les consultes, ha de valorar-se de forma raonada i documentada. En paral·lel, el delegat de protecció dades (DPD), quan aquest hagi estat designat, haurà de ser consultat i oferir assessorament (Article 35(2) i 39(1)(c)); sens perjudici d'això últim, el DPD no podrà dirigir el procés d'avaluació.

5) *Les Recomanacions*: el Reglament exigeix que el procés d'avaluació finalitzi amb una llista de mesures recomanades de cara a:

a) afrontar els riscs, incloses les "garanties, mesures de seguretat i mecanismes que garanteixen la protecció de dades personals", i

b) demostrar la conformitat amb el Reglament, "tenint en compte els drets i interessos legítims dels interessats i d'altres persones afectades" (Article 35(7)(d)).

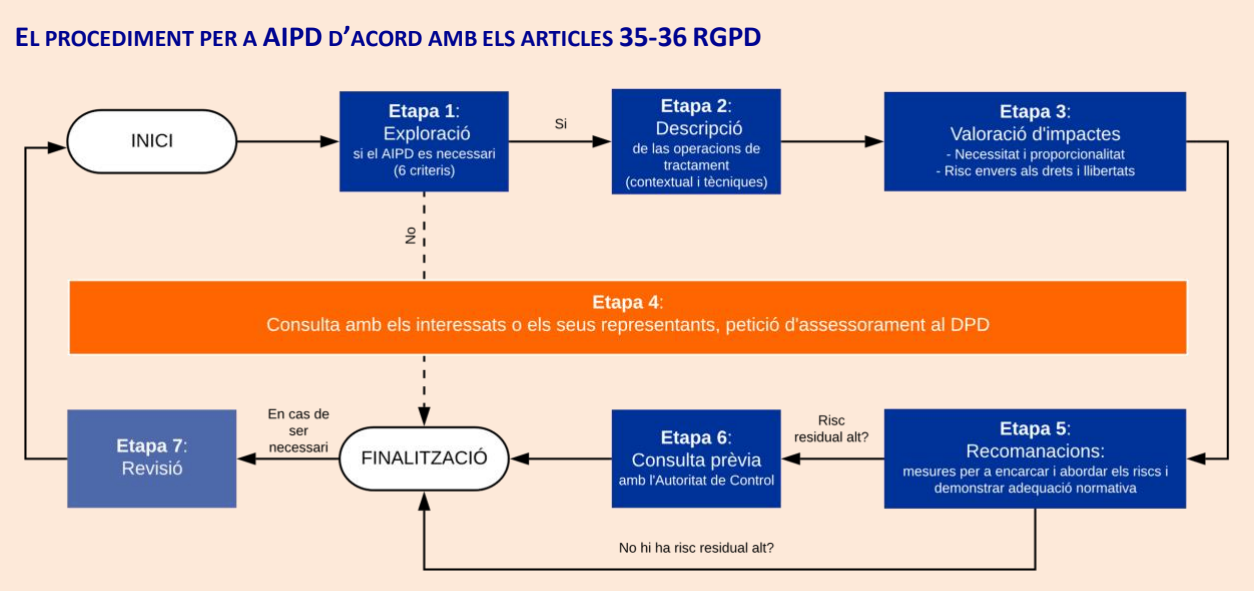
El resultat de l'avaluació d'impacte s'haurà de tenir en compte a "l'hora de decidir les mesures que s'han de prendre amb la finalitat de demostrar que el tractament de les dades personals és conforme a aquest Reglament" (Considerant 84).

6) *Consulta prèvia amb l'autoritat de control*: El Reglament pot vincular l'inici d'un procediment d'AIPD a la realització d'una consulta prèvia. Serà així quan existeixi un risc residual alt, és a dir, quan l'avaluació

demostri que el risc pot seguir sent elevat, fins i tot després d'haver-se implementat les mesures resultants del procediment d'avaluació. En aquest cas, abans d'iniciar el tractament de dades personals i d'acord amb un procediment preestablert, el responsable del tractament estarà obligat a referir-se i consultar a la ACPD (Article 36).

7) *Revisió*: si escau, el responsable del tractament haurà de revisar que el tractament segueix realitzant-se de conformitat amb l'AIPD, com a mínim quan existeixi un canvi en el riscs de les operacions de tractament. (Article 35(11)). Per tant, aquesta revisió es pot donar tant en un moment determinat, de cara a objectius de monitoratge, o quan hi hagi un canvi que comporti l'obsolescència d'avaluacions prèvies (parcials o totals). Dit això, el Reglament no estipula quines han de ser les conseqüències d'aquesta revisió; així, tenint en compte les possibles variacions en els riscs, l'avaluació pot haver de realitzar-se de nou (en part o completament).

El mètode específic d'AIPD proposat, estableix uns fonaments per a la seva adaptació a contextos d'ús concrets, com ara poden ser les operacions de tractament relatives a les telecomunicacions o les xarxes d'energia intel·ligents, a fi de d'assegurar la "protecció de dades personals" i demostrar la conformitat amb el Reglament (Article 35(7)(d)).



D'acord amb aquesta interpretació, el RGPD no contempla les deu etapes del mètode genèric. Algunes no meriten ser necessàriament regulades per llei, però emergeixen de forma pragmàtica durant el procés d'avaluació. En particular el Reglament no té en compte l'etapa d'*Especificació*. (A nivell pràctic, l'*Especificació*, determinaria per exemple, quins aspectes del dret de protecció de dades personals es troben amb tota seguretat afectats pel tractament de dades proposat, i qui seria el interessat o el representat del interessat respecte aquell tractament.) Altres etapes del mètode genèric poden, amb poques paraules, ser interpretades des d'altres articles del Reglament. En relació a la *Planificació* i preparació, el Reglament estipula només que, per exemple, una sola avaluació pot abastir diversos tractaments similars (Considerant 92) o que l'encarregat ha d'ajudar al responsable a l'hora de dur a terme l'avaluació del tractament (Article 28(3)(f)). En relació a la *Documentació*, el responsable del tractament, està per exemple obligat a demostrar que les operacions de tractament han de ser realitzades d'acord amb la llei (Article 24(1)). Pel que fa al *Control de qualitat*, per exemple, un DPD està encarregat de supervisar l'aplicació del procés d'avaluació (Article 39(c)). El DPD també serà responsable de dur a terme auditories (Article 58(1)(b)). Ara bé, en comparació amb el mètode genèric, el RGPD afegeix l'etapa addicional de la *Consulta prèvia amb l'autoritat de control*.

4 OBSERVACIONS FINALS

En aquesta nota normativa, el d.pia.lab estableix els fonaments de dos mètodes d'avaluació d'impacte: en primer lloc, un mètode genèric, que reflecteix el marc definit en l'anterior nota normativa i que pretén constituir-se en un mètode d'avaluació adaptable a dominis pràctics concrets i contextos d'ús específics. En segon lloc, un mètode per AIPD a la EU, basat en el mètode genèric i interpretat d'acord amb els requeriments del RGPD.

El procediment de AIPD a la EU, es construeix sobre un nombre de conceptes clau, com ara el de risc envers drets i es troba formulat com a un "trincatge jurídic", és a dir, regulat mínimament en els textos legals i requerint per tant, interpretació i orientació. És per això que el d.pia.lab ha procurat interpretar el mètode per a AIPD a través dels Articles 35-36 del RGPD, centrant-se en aquells aspectes contenciosos. En tant que l'obligació de dur a terme el procediment d'AIPD es troba present en altres instruments legals de la EU més enllà del RGPD, les consideracions realitzades també poden resultar aplicables mutatis muntandis a aquelles. Ara bé, certes qüestions com les tècniques d'avaluació de necessitat i proporcionalitat de riscs envers els drets i llibertats de les persones físiques, així com la implicació de les parts, inclosa la societat, reclamen de més atenció acadèmica i professional, i és precisament en elles que el d.pia.lab pretén centrar les seves futures contribucions.

Tanmateix, el mètode per a un AIPD interpretat d'acord amb els requisits del RGPD encara necessita d'una profunda orientació, clarificació i adaptació. Particularment, per part d'aquells organismes més ben posicionats per oferir un major grau de seguretat jurídica, és a dir, el Comitè Europeu de Protecció de Dades, conjuntament amb els DPA nacionals i regionals i la mateixa EU, els quals tenen la capacitat de convertir-se en "centres de referència" per aquest i altres tipus d'avaluacions d'impactes. En aquest sentit meriten especial atenció els formularis per a AIPD ajustats a les circumstancies d'un determinat Estat Membre i context d'ús particular (e.g. una indústria o sector governatiu).

SELECCIÓ DE FONTS CONSULTADES

Arnstein, Sherry R. (1969) "A Ladder of Citizen Participation," *Journal of the American Institute of Planners*, 35(4), pp. 216–224. doi: 10.1080/01944366908977225.

De Hert Paul, Dariusz Kloza and David Wright (2012) "Recommendations for a Privacy Impact Assessment Framework for the European Union," Brussels – London. https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf.

Gellert, Raphaël (2018) "Understanding the notion of risk in the General Data Protection Regulation", *Computer Law & Security Review* 34(2), pp. 279–288. doi: 10.1016/j.clsr.2017.12.003.

Kloza, Dariusz, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn (2017) "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," *d.pia.lab Policy Brief 1/2017*, VUB: Brussels. https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf.

van Dijk Niels, Raphaël Gellert and Kjetil Rommetveit (2016) "A risk to a right? Beyond data protection risk assessments", *Computer Law & Security Review*, 32(2), pp. 286–306. doi: 10.1016/j.clsr.2015.12.017.

Oxford Dictionary of English. https://www.lexico.com/en.

Institut d'Estudis Catalans, *Diccionari Manual de la Llengua Catalana* (2000).

Autoritat Catalana de Protecció de Dades. https://apdcat.gencat.cat/ca/autoritat/normativa/normativa_internacional/unio_europea/.

ALTRES LECTURES RECOMANADES

Article 29 Working Party (2017) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248 rev. 01, Brussels. http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

International Organization for Standardization [ISO] (2018), *Risk management – Guidelines*, ISO 31000:2018, Geneva. https://www.iso.org/iso-31000-risk-management.html.

Jasanoff, Sheila (2012) *Science and Public Reason*. London: Routledge. doi: 10.4324/9780203113820.

European Data Protection Supervisor [EDPS] (2017) *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. Brussels. https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

EDPS (2017) *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* [draft]. Brussels. https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.

EDPS (2019) *Accountability on the ground. Part II: Data Protection Impact Assessments & Prior Consultation*. Brussels. https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf.

Grunwald, Armin (2018) *Technology Assessment in Practice and Theory*. Abingdon: Routledge. doi: 10.4324/9780429442643.

Mays, Claire (2004) *Stakeholder Involvement Techniques. Short Guide and Annotated Bibliography*. Organisation for Economic Co-operation and Development (OECD), Paris. http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf.

Noble, Bram F. (2015) *Introduction to Environmental Impact Assessment. A Guide to Principles and Practice*. Toronto: OUP Canada.

SOBRE EL D.PIA.LAB

El **Brussels Laboratory for Data Protection & Privacy Impact Assessments, o d.pia.lab**, uneix la recerca metodològica i aplicada i proporciona formació i assessorament respecte de polítiques sobre avaluacions d'impacte en àrees d'innovació i desenvolupament tecnològic. Mentre que els aspectes jurídics de la protecció de dades personals, així com aquells vinculats a la privacitat, constitueixen el nucli de la nostra funció i objectius, les activitats del d.pia.lab engloben també disciplines com ara l'ètica, la filosofia, els estudis sobre vigilància i ciència, o les tecnologies de la societat d'informació (TIC). Creat el novembre de 2015, el Laboratori forma part i es construeix sobre l'experiència del Grup de Recerca Law, Science, Technology & Society (LSTS) de la Vrije Universiteit Brussel (VUB), Bèlgica. El Laboratori ha edificat el seu coneixement a través de nombroses avaluacions d'impacte ja concloses i de projectes de recerca encara vigents, com ara PERSONA, HR-RECYCLER, SYSTEM (co-finançats per la Unió Europea) i PARENT (co-finançat per Innoviris).

Les idees expressades en aquesta nota normativa no reflecteixen els punts de vista de cap de les mencionades entitats finançadores. Agraïm – per ordre alfabètic – Alexandra Aslanidou, Jonas Breuer, Alessandra Calvi, Roger Clarke, Katerina Demetzou, Catherine Jasserand-Breeman, Anna Johnston, Gianclaudio Malgieri, Anna Mościbroda, Kjetil Rommetveit, Julien Rossi, Juraj Sajfert, Laurens Vandercruysse, Heidi Waem, Ine van Zeeland i un avaluador anònim per els seu comentaris en les primeres versions d'aquesta nota normativa. Traducció al català a càrrec de Sergi Vazquez Maymir.

dpialab.org | **dpialab@vub.ac.be**