Pautes per avaluar projectes de recerca i innovació en salut que utilitzin tecnologies emergents i dades personals

Guidelines for reviewing health research and innovation projects that use emergent technologies and personal data

Pautas para evaluar proyectos de investigación e innovación en salud que utilicen tecnologías emergentes y datos personales

Itziar de Lecuona (Coord.)

Organització de les Nacions Unides per a l'Educació, la Ciència i la Cultura

Càtedra UNESCO de Bioètica de la Universitat de Barcelona

Observatori de Bioètica i Dret

www.bioeticaidret.cat
www.bioeticayderecho.ub.edu
www.bioethicsandlaw.es

Pautes per avaluar projectes de recerca i innovació en salut que utilitzin tecnologies emergents i dades personals

PLANTEJAMENT

L'avaluació dels aspectes metodològics, ètics, legals i socials dels projectes de recerca en salut correspon als comitès d'ètica de la recerca (CER). En el nostre context, l'aprovació de projectes en els quals participen persones, s'utilitzen dades personals i/o mostres biològiques d'origen humà depèn d'aquests òrgans col·legiats interdisciplinaris i establerts per llei. El seu dictamen favorable és obligatori perquè es puguin dur a terme les intervencions proposades, tant en centres públics com privats de recerca. A Europa conviuen diferents fórmules: els CER poden ser de caràcter nacional i regional, però també hi ha la possibilitat que cada centre de recerca compti amb el seu propi CER o s'adscrigui a un ja creat. Tots ells han d'estar acreditats per l'organisme corresponent, previ compliment d'una sèrie de requisits i condicions.

Inicialment els CER es van crear per a avaluar assajos clínics amb medicaments i productes sanitaris, per a després valorar altres tipus de recerques que, per les seves característiques, també plantegen la necessitat de trobar un equilibri entre l'avanç del coneixement científic, l'interès investigador i la protecció de les persones participants. Exemples d'això últim són els projectes que apliquen tecnologies emergents com la intel·ligència artificial, el *Big Data*, la biometria i la realitat virtual, entre d'altres, així com el desenvolupament de dispositius i aplicacions de salut (*Apps*). Recentment, també, es sol·licita als CER que avaluïn projectes purament d'innovació en l'àmbit de la salut.

En aquests processos de creació i transferència de coneixement, els interessos de la ciència, de la tecnologia i de la societat no han de prevaldre sobre els de l'individu. Per a això, els CER han d'analitzar la validesa científica de les propostes, el seu valor social i ponderar els drets i interessos en joc. La recerca és una activitat que sempre comporta uns certs riscos per als participants —com el risc de la fallida de la confidencialitat en els projectes que tractin dades personals—. I aquests riscos s'han de sospesar amb els beneficis, dels quals en moltes ocasions el participant no s'aprofita personal o directament.

Els canvis científics i tecnològics són vertiginosos, en una societat de mercat exacerbada on la salut és objecte d'una creixent mercantilització; i en la qual es monetitzen les dades personals. Si bé és cert que els ritmes de producció normativa i dels processos de creació i aplicació del coneixement no són els mateixos, es produeix una certa paràlisi en l'aplicació de les normes, fonamentalment deguda a la falta de comprensió del fenomen digital al qual ens enfrontem. Per això, es considera que els CER poden i han d'actuar com a garantia que la recerca i la innovació aparellada compleixen amb els principis ètics i amb els requisits legals establerts[1].

La societat digital, guiada per la dada i basada, per tant, en l'explotació intensiva de conjunts de dades, inclosos les dades personals, ha posat de manifest que el model avaluador vigent -i propi de la segona meitat del segle XX- per a analitzar projectes de recerca en els quals participin humans i/o s'utilitzin les seves dades personals està obsolet i és ineficaç, precisament pels reptes que tècnica, ètica, legal i socialment plantegen els tractaments de dades personals en el segle XXI.

En l'actualitat, els CER han de protegir a les persones a través de la salvaguarda de les seves dades personals i assegurar la intimitat i la confidencialitat dels seus titulars. A més, han de promoure i garantir l'exercici de l'autonomia per a prendre decisions de manera lliure i informada, evitar la discriminació (específicament quan és encoberta), així com garantir l'equitat i la transparència. L'equilibri que els CER han d'aconseguir entre maximitzar els beneficis i minimitzar els riscos inclou també tractar adequadament les dades personals. En resum, com els processos de recol·lecció i tractament de dades constitueixen el nínxol on desenvolupar la recerca i innovació, resulta prioritari que els CER prenguin consciència de la rellevància del nou paradigma digital assentat en l'explotació intensiva de dades personals, incloses les dades de salut[2].

La pandèmia per COVID-19 ha posat a prova la capacitat dels CER per a analitzar adequadament els esmentats projectes i prioritzar aquells que beneficiïn l'interès col·lectiu i la salut pública. Actualment, els CER treballen sota pressió i se'ls exigeix una ràpida avaluació dels nombrosos projectes de recerca i innovació que es presenten: assajos clínics per al desenvolupament de vacunes i de medicaments, i altres tipus de recerques; però, també hi ha molts altres projectes que han de ser avaluats i que no requereixen cap intervenció directa sobre les persones, malgrat que impliquen l'accés i el tractament de conjunts de dades personals, entre les quals destaquen les dades de salut. En particular, projectes per al desenvolupament de sistemes de predicció i gestió de la COVID-19 que aguditzen els problemes als quals ja venien enfrontant-se els CER en els últims anys. No són per tant qüestions totalment noves, però sí que és cert que s'han intensificat per raó de l'excepcional situació que estem vivint en la que es fan patents les greus manques del nostre model avaluador.

Davant aquesta situació, el Grup d'Opinió de l'Observatori de Bioètica i Dret- Càtedra UNESCO de Bioètica de la Universitat de Barcelona (OBD), centre de recerca interdisciplinari de la Universitat de Barcelona, ha analitzat els reptes, les qüestions no resoltes i els problemes que es susciten en els projectes de recerca i la innovació en salut. L'objectiu és aportar pautes que contribueixin a homogeneïtzar les qüestions que els CER han d'analitzar i avaluar, així com la informació que sol·licitar als responsables dels projectes, per a impedir que els oportunistes obrin mercats de dades personals disfressades de recerca i innovació i, en particular, amb el pretext de la pandèmia. I també per a evitar que la intimitat dels participants en aquests projectes es vegi exposada públicament sense el seu consentiment[3].

L'adequada avaluació dels tractaments de les dades personals en projectes de recerca i innovació en salut ha de ser una prioritat per als CER, entesos com a mecanismes de protecció de les persones. El principal escull és que no estan aconseguint adaptar-se al paradigma digital i al canvi que suposa assentar els processos de recerca i innovació en salut en l'explotació intensiva de conjunts de dades personals, la qual cosa genera importants disfuncions. L'experiència de membres de l'OBD com a vocals de diferents comitès d'ètica (CER, comitès de bioètica nacionals i autonòmics, assistencials i *ad hoc*), que es reflecteix en aquest treball, permet aportar una perspectiva pràctica a l'anàlisi del marc teòric.

En aquesta ocasió l'autora d'aquest treball és la Dra. Itziar de Lecuona, doctora en dret, professora agregada del Departament de Medicina de la Facultat de Medicina i Ciències de la Salut de la Universitat de Barcelona i subdirectora de l'OBD, que ha coordinat el Grup

d'Opinió i ha rebut les aportacions dels acadèmics, investigadors i professionals que es relacionen al final del Document.

Des de 1996, l'OBD analitza científica i interdisciplinàriament les implicacions ètiques, jurídiques i socials de la biomedicina i la biotecnologia, i incideix en el diàleg entre la universitat i la societat mitjançant la transmissió del coneixement cientificotècnic i els arguments necessaris per a participar en un debat social veritablement informat. A aquest efecte, el Grup d'Opinió ha elaborat ja 31 documents i declaracions[4] concernents a temes d'actualitat, sobre els quals no existeix una opinió unànime, ni en la societat ni en les diverses comunitats científiques implicades; això ha requerit identificar els problemes, contrastar els arguments i proposar recomanacions.

L'anàlisi i les recomanacions que el Grup efectua estan principalment destinats als membres dels CER implicats en l'avaluació dels citats projectes de recerca i innovació en salut, per a que sigui possible la protecció de la intimitat dels titulars de les dades, i orientar el seu tractament de tal forma que s'evitin explotacions innecessàries, així com la comercialització de conjunts de dades personals. La recerca ha de respondre a les necessitats socials i no a interessos espuris. El treball també té com a destinataris a l'ecosistema de recerca i innovació, amb una crida al poder polític i legislatiu perquè prengui en consideració les recomanacions.

ESTAT DE LA QÜESTIÓ

En els centres hospitalaris i de recerca la COVID-19 ha provocat un al·luvió de propostes en recerca i en innovació per a la seva detecció precoç i gestió. Aquestes es basen en l'aplicació d'intel·ligència artificial i tecnologies emergents com el *Big Data* i la biometria i poden comportar el desenvolupament de dispositius de salut, *Apps* incloses. Exemples d'aquests projectes són el desenvolupament de sistemes de predicció de la COVID-19, basats en la programació d'algorismes que es nodreixen de diferents conjunts de dades personals emmagatzemades en històries clíniques i en altres bases de dades, així com d'aquella informació remesa pels titulars de les dades en diferents formats. Així, proliferen les *Hackatons*[5] o reptes per a, per exemple, desenvolupar algorismes com a part de projectes en medicina per a predir el risc de desenvolupar determinades complicacions. L'objectiu és augmentar el coneixement disponible, desenvolupar intervencions personalitzades i millorar la presa de decisions. En suma, en salut es plantegen propostes que poden estar fonamentades en protocols de recerca i altres per a innovar en l'àmbit assistencial, que comparteixen el repte d'assegurar que protegeixen la intimitat dels titulars de les dades personals que necessiten tractar. Aquestes iniciatives haurien de tenir un clar benefici social.

Des de principis dels 2000, Europa aposta per una societat guiada per la dada. És una decisió política i econòmica, que també inclou els processos de creació i de transferència de coneixement. L'objectiu és un mercat digital únic i competitiu, capaç de garantir la protecció dels drets i llibertats de les persones, alhora que promou la recerca i innovació fonamentada en l'explotació intensiva de conjunts de dades, inclosos les dades personals[6]. En l'àmbit de la salut aquesta aposta es tradueix en una medicina més personalitzada, sistemes sanitaris més eficients, predicció dels efectes adversos dels medicaments amb un nombre menor de persones exposades al risc, envelliment actiu i benestar; i sistemes de predicció i gestió de pandèmies, com és el cas de la COVID-19, entre altres prioritats. Tots aquests àmbits en els quals es financen nombrosos i quantiosos consorcis de recerca i innovació públic-privada

basats en les esmentades tecnologies i en el desenvolupament de dispositius de salut[7], tenen com a substrat l'explotació de conjunts de dades, entre les que es troben les dades personals, i per a les quals és necessària la participació de tercers tradicionalment aliens a l'àmbit biomèdic i de salut. Aquests tercers, que poden ser tant empreses privades com fins i tot administracions públiques, tenen interès a accedir a diferents conjunts de dades personals, pel que poden dir dels seus titulars i pel que poden predir. Interès que pot ser diferent i fins i tot contrari al dels investigadors responsables dels projectes.

En pocs anys hem transitat veloçment de l'entusiasme pel *Big Data* a la devoció per la intel·ligència artificial, la realitat virtual i la internet de les coses. Tot just abans de la pandèmia, Europa va presentar la seva Estratègia Digital i d'Intel·ligència Artificial[8] que des de la perspectiva ètica ha de ser "confiable"[9], capaç d'evitar els biaixos per raó de sexe o raça, entre d'altres, i centrada en l'ésser humà. Malgrat aquesta lloable decisió política, és necessari recordar la falta d'infraestructures públiques a Europa que permetin emmagatzemar, usar i compartir dades, la seva interoperabilitat i reutilització. Aquesta situació evidencia l'excessiva dependència europea de les grans tecnològiques, fonamentalment estatunidenques, conegudes com a imperi GAFAM per les seves sigles en anglès (Google, Apple, Facebook, Amazon i Microsoft).

Així, les dades personals són l'or del nostre temps i, entre elles, les dades de salut, les dades biomètriques, i sociodemogràfiques, entre d´altres, són considerades per la legislació com a categories especials de dades[10] que requereixen la més alta protecció perquè ho diuen tot sobre nosaltres; perquè podrien ser utilitzades amb finalitats no desitjades, i donar lloc a discriminacions encobertes, amb profundes implicacions per a la llibertat de les persones i de les generacions futures. La possessió de conjunts de dades personals per part de tercers, bé sigui per iniciativa pública o privada, pot afectar els nostres drets en funció dels usos, conferint-los a aquests tercers un extraordinari poder sobre nosaltres, situació que passa inadvertida per a la gran majoria de les persones. Les decisions que es prenguin en l'àmbit de la recerca i innovació en salut i en contextos altament digitalitzats marcaran els projectes vitals de persones, col·lectius i societats.

En la societat digital hem deixat de ser anònims per a ser reidentificables. El sexe, el codi postal i la data de naixement ens identifiquen amb un percentatge de fiabilitat molt elevat[11]. El Grup d'Opinió de l'OBD ja va alertar sobre aquestes qüestions al 2015, en el "Document sobre bioètica i *Big Data* de salut: explotació i comercialització de les dades dels usuaris de la sanitat pública"[12]. A causa del desenvolupament de la tecnologia i a la ingent quantitat d'informació de caràcter personal acumulada en diferents bases de dades i a la informació que alliberem, és possible realitzar patrons de comportament, predir conductes i, per tant, millorar la presa de decisions. Per a això és necessari programar algorismes que es nodreixen de conjunts de dades, incloses les dades personals. Aquestes dades personals, com a principal matèria primera, són propietat dels seus titulars, que seran al seu torn destinataris finals dels resultats dels processos de recerca i innovació amb l'especial situació de les dades de salut. Com és sabut, la història clínica digitalitzada[13], convenientment estructurada i seguint criteris de qualitat i seguretat, conté dades personals de salut, sociodemogràfiques, i diverses dades personals que són d'interès pel que aquestes diuen de les persones ara i pel que poden predir.

La recerca i la innovació en salut es produeixen en un context altament competitiu i d'ultraliberalisme globalitzat i de domini del mercat [14], en el qual es coalitzen eixos

diferenciats, com els de recerca, innovació, aplicació del coneixement i empresa. En aquest context, s'obre el debat sobre la titularitat de les dades personals, sobre l'altruisme de dades[15] quan el nostre sistema de recerca i d'innovació en salut tradicionalment s'ha basat en la solidaritat, tenint sempre l'opció de no participar en aquests processos de donació de manera lliure i voluntària i sense que això tingui conseqüències negatives. Aquest model altruista i solidari, i que comporta una certa cessió d'informació personal, ha de revertir en tractaments i intervencions per al titular de les dades o per als pacients i les generacions futures. També pot implicar l'augment de coneixement sense un benefici directe. Aquesta cessió no pot suposar que determinats conjunts de dades personals estiguin a l'abast de qualsevol, en particular les dades de salut. Convé recordar aquí que l'accés a dades personals amb finalitats assistencials i de recerca inclou el deure de secret del professional sanitari per a mantenir la confidencialitat de la informació.

Davant el canvi que implica l'explotació intensiva de dades personals i l'elevada probabilitat de reidentificació, el quid de la qüestió radica en quines dades personals se sol·licitaran, com s'obtindran i emmagatzemaran i de quina forma es tractaran -si codificades o seudonimitzades[16]-, qui tindrà accés, durant quant temps i què es farà amb les dades un cop finalitzada la intervenció. Així mateix, l'interès es centra en com es combinaran els conjunts de dades, per exemple, aquells emmagatzemats en històries clíniques digitalitzades en bases de dades altament protegides amb altres dades personals provinents d'altres bases de dades externes al sistema de salut, que poden referir-se al patró de comportament dels seus titulars mitjançant l'anàlisi de la base de dades de telefonia mòbil o altres, com a enquestes de salut.

Per a la gestió de la COVID-19 hem assistit al desenvolupament d'aplicacions que convidaven a aportar dades personals com la targeta sanitària i la geolocalització per a iniciar una enquesta sobre els símptomes i poder predir si la persona és sospitosa de ser positiva, i com a suport en l'àmbit de la salut pública. Després, s'ha iniciat un debat tardà i gens transparent sobre la seguretat tècnica i la protecció de la intimitat sobre les *Apps* d'identificació de positius i rastreig de contactes[17]. Aquesta informació de caràcter personal, degudament obtinguda i emmagatzemada hauria de poder combinar-se amb altres dades de salut, com s'ha exposat, perquè sigui útil per a la presa de decisions en benefici de les persones i de l'interès públic. Aquests exemples de processos de recerca i innovació han de comptar amb l'aprovació dels corresponents CER.

DECLARACIÓ

Per a orientar la presa de decisions en recerca i innovació en salut, davant l'explotació intensiva de dades personals, convé efectuar les següents consideracions per a una adequada protecció de les persones:

- Que ja no és possible garantir l'anonimat. Hem deixat de ser dades aïllades per a convertir-nos en conjunts de dades, emmagatzemades en diferents bases de dades que es poden combinar amb l'objectiu d'extreure conclusions per a millorar la presa de decisions; pel que hem passat de ser anònims a ser reidentificables.
- Que els protocols d'obtenció del consentiment informat dels participants han quedat clarament desfasats pel fet que es pressuposava no sols que les dades eren anònimes, sinó que sempre ho continuarien sent en el futur.

- Que la pandèmia per COVID-19 ha permès constatar allò que era evident: els greus problemes per a accedir i interpretar les dades que són tan necessàries per a avançar en la presa de decisions polítiques basades en l'evidència científica.
- Que les dades emmagatzemades no estan connectades entre si, no estan adequadament seudonimitzades, ni tampoc hi ha infraestructures públiques per aquests fins, creant una barrera per al coneixement científic, així com per als diferents actors del sistema de recerca, innovació i desenvolupament.
- Que la dependència per part dels Estats i d'Europa de les grans tecnològiques, fonamentalment dels Estats Units és excessiva i ha de ser revertida amb urgència.
- Que el procés de combinació de conjunts de dades personals mitjançant el recurs a les tecnologies emergents i al desenvolupament d'algorismes ha de produir un benefici sobre les persones i no exposar-les a discriminacions manifestes o encobertes ni a usos no desitjats.
- Que el suport que implica la tecnologia no pot conduir a pràctiques de vigilància digital de les persones.
- Que ni els governs ni les grans corporacions tecnològiques han de tenir un control absolut sobre les dades personals i que la gestió d'aquestes ha de sotmetre's a criteris de transparència i retiments de comptes per a evitar l'opacitat que impera en els entorns digitals.
- Que existeix una tendència a la mercantilització de les dades personals també en l'àmbit de la salut i, en particular, a propòsit de la pandèmia per COVID-19.
- Que les decisions han d'estar fonamentades en l'evidència científica i no en propostes proclius a mercats de dades personals disfressades de recerca i innovació en salut.
- Que una persona física identificable és aquella que pot ser identificada, directa o indirectament, en particular per la referència a un identificador com un nom, un número d'identificació, dades d'ubicació, un identificador en línia o a un o més factors específics de l'àmbit físic, fisiològic, genètic, mental, econòmic, identitat cultural o social d'aquesta persona física.
- Que són dades personals: el nom, l'adreça, el número d'identificació, el pseudònim, l'ocupació, el correu electrònic, el CV, les dades d'ubicació, l'adreça de Protocol d'Internet (IP), l'identificador de *cookies*, el número de telèfon, les dades proporcionades per mesuradors intel·ligents, dades en poder d'un hospital o de centres de recerca[18].
- Que són categories especials de dades personals aquelles dades que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, o l'afiliació sindical, i el tractament de dades genètiques, dades biomètriques dirigits a identificar de manera unívoca a una persona física, dades relatives a la salut o dades relatives a la vida sexual o les orientacions sexuals d'una persona física.
- Que juntament amb la legislació vigent, són aplicables els deures ètics i deontològics sobre protecció de la intimitat i la confidencialitat de les dades personals en entorns altament digitalitzats per als professionals sanitaris, però també per als diferents professionals que col·laboren.

- Que els CER no tenen la composició adequada ni les capacitats necessàries per a avaluar els projectes de recerca i innovació que aquí es plantegen. Per això, és urgent aconseguir la seva educació digital, per la responsabilitat que exerceixen aquests òrgans col·legiats sobre la protecció dels drets dels implicats en els processos de recerca i innovació, incloent-hi la llibertat i recerca, al costat d'altres drets fonamentals com la intimitat i la confidencialitat de les dades personals.
- Que els CER han d'identificar els potencials problemes i els conflictes d'interès que puguin sorgir en relació a l'ús de dades personals, així com quina informació sol·licitar als responsables dels projectes, per a garantir la protecció dels drets de les persones.
- Que la recerca i la innovació han d'estar justificades per la seva validesa científica i el seu valor social, i que els drets de les persones es poden restringir de manera proporcionada i justificada per raons de salut pública i interès col·lectiu, però mai arribar a anul·lar-se. En cap cas, i menys en temps de pandèmia, es poden relaxar els estàndards de protecció.

RECOMANACIONS

1. Als comitès d'ètica de la recerca:

1.1. Sobre els projectes de recerca i innovació en salut que utilitzen tecnologies emergents i dades personals:

A) Comprovar i avaluar el compliment dels principis de protecció de dades.

El tractament de dades personals ha de basar-se en els següents principis: "licitud, lleialtat i transparència" en relació a l'interessat; "limitació de la finalitat" que es refereix a que les dades han de ser recollides amb fins determinats, explícits i legítims[19]; "minimització de les dades", que significa que les dades han de ser adequades, pertinents i limitades a allò que és necessari en relació a les finalitats per a les quals es tracten; "exactitud", entenent que les dades seran exactes, i si fos necessari, actualitzades, i que s'adoptaran totes les mesures raonables per a que es suprimeixin o es rectifiquin sense dilació les dades personals que siguin inexactes respecte dels fins per als quals es tracten; "limitació del termini de conservació" i "integritat i confidencialitat", que es refereix a que les dades siguin tractades de manera segura. Així mateix, el responsable del tractament serà el responsable del compliment d'aquests principis i serà capaç de demostrar-lo (responsabilitat proactiva). El responsable del tractament té l'obligació de la protecció de dades "des del disseny" i "per defecte" per a determinar les mesures tècniques i organitzatives necessàries per a assegurar el compliment dels esmentats principis[20].

Per a donar compliment als citats principis, els CER han de comprovar i avaluar:

a) Si la informació i el procés de consentiment informat dels potencials participants en els projectes compleix amb els requisits establerts per la normativa vigent;

b) Si les dades personals es codificaran, seudonimitzaran o anonimitzaran;

c) El format en el qual s'emmagatzemaran les dades personals;

d) Si les dades personals s'enviaran dins i/o fora de la Unió Europea, amb les corresponents garanties i si es compartiran amb tercers; i

e) Si hi ha serveis de núvol i en quines condicions.

B) Assegurar la no identificació de les persones participants que requereix incorporar com a membres o assessors a experts, especialment, en tècniques de seudonimització.

Evitar el recurs al concepte d'"anonimització" amb caràcter general, perquè genera una falsa sensació de seguretat. Les paraules importen i els CER no han de passar per alt aquesta qüestió i han d'incloure en els models de presentació de projectes o en les indicacions corresponents els tipus de tractaments possibles i, així, les diferències entre dades anonimitzades, codificades i seudonimitzades. En aquest sentit, un error comú detectat en les memòries, els protocols i en els fulls d'informació i consentiment informat dels projectes, és indicar que les dades s'anonimitzaran, quan de l'anàlisi dels tractaments de dades es constata que aquestes se seudonimitzaran.

Els CER han de comprovar les tècniques previstes per a assegurar la no atribució de personalitat als conjunts de dades que es tracten, és a dir, la no identificació del titular de les dades. Aquestes qüestions, eminentment tècniques, requereixen comptar amb experts o assessors en el CER que, de manera independent, puguin avaluar i comprovar que les propostes són adequades.

C) En el cas que no es disposi d'un sistema de protecció específic i propi de la institució, s'han de recordar contractualment les condicions que garanteixin la protecció de les dades personals.

Un exemple recurrent i de mala pràctica és el recurs a serveis digitals gratuïts per a efectuar enquestes en xarxa pel tractament de dades personals que no protegeixen la privacitat, tret que es contractin serveis específics per a això. Aquesta situació planteja qüestions ètiques i legals, ja que alliberar dades personals en plataformes que per defecte monetitzen dades personals en entorns no protegits per part de tercers, és també una violació de la integritat científica[21]. Si les institucions participants en aquests projectes no compten amb serveis específics que protegeixin la intimitat, el responsable del tractament ha d'assegurar tal protecció i realitzar els corresponents acords contractuals amb tercers, presentant davant el CER les evidències que siguin necessàries.

D) Exigir i examinar "l'avaluació de l'impacte de les operacions de tractament en la protecció de dades personals" (AIPD) en els supòsits en què així ho exigeix el Reglament General de Protecció de Dades.

Es tracta d'una avaluació de l'impacte de les operacions de tractament en la protecció de dades personals, que han d'efectuar el responsable del tractament amb caràcter previ a l'inici del mateix. En determinats supòsits, com en el cas d´us de noves tecnologies; tractaments de categories especials de dades (dades de salut, genètiques i biomètriques); tractaments que impliquin l'elaboració de perfils de persones; i/o presa de decisions automatitzada, entre altres, els CER han de comprovar que el projecte ha estat sotmès a l'esmentada AIPD. Aquesta pot fer-se seguint unes metodologies que permeten identificar els riscos associats als tractaments[22]. De l'AIPD derivarà un pla d'acció que haurà de dur-se a terme per a mitigar riscos i que haurà de revisar-se periòdicament i actualitzar-se davant possibles canvis en els tractaments de les dades. Aquesta avaluació no pot concebre's com un mer tràmit, sinó com un procés viu que pot ser objecte de modificacions i que permet fer un adequat seguiment del projecte i de les garanties a aplicar per a la protecció de les dades personals. El Delegat de Protecció de Dades, és la figura independent que assessora en aquests processos.

E) Sol·licitar i avaluar el Pla de Gestió de Dades.

Els CER han de sol·licitar a l'investigador principal el Pla de Gestió de Dades, que descriu com s'obtenen, es processen i en el seu cas, es generen noves dades en el marc del projecte; i què ocorrerà amb aquestes una vegada acabat el projecte [23]. Així mateix, el Pla inclou fórmules perquè les dades es puguin trobar, siguin accessibles, interoperables i reutilitzables. La "ciència oberta", en el marc de la societat digital, obliga als CER a comprovar quines metodologies i estàndards s'aplicaran i si les dades es compartiran en accés obert[24]. Convé posar l'accent que el Pla de Gestió de Dades s'insereix en l'anàlisi de riscos i l'adopció de mesures de seguretat que exigeix el Reglament General de Protecció de Dades en tots els casos, es faci o no una avaluació d'impacte relativa a la protecció de dades.

F) Comprovar que els potencials participants dels projectes de recerca i innovació en salut són informats sobre els seus drets i les condicions per al seu exercici.

Dret a ser informat; d'accés; de rectificació; a l'oblit; a restringir el processament de les dades; a la portabilitat de les dades i a no ser objecte d'una decisió automatitzada que ha d'incorporar la intervenció i correcció humana i que inclou l'elaboració de perfils. Així mateix, s'ha d'informar sobre el dret a la revocació que implica assegurar que s'elimina de la base de dades corresponent la informació de la persona que així ho sol·licita.

G) Comprovar que els protocols i els fulls d'informació i de consentiment informat indiquin explícita i detalladament qui és el responsable del tractament i del processament de les dades personals.

Els CER han d'actuar de manera coordinada amb els serveis legals de la institució corresponent per a revisar els acords d'encarregat de tractament i transferència de dades i, quan escaigui, els acords de corresponsabilitat sobre els tractaments[25].

És necessari que els CER estableixin un canal de comunicació fluida amb els responsables de les àrees de tecnologies de la informació i la comunicació de les institucions corresponents.

H) Sol·licitar que la política de privacitat i l'avís legal s'incloguin en la memòria del projecte.

Els CER han de poder avaluar el compliment dels drets i obligacions sobre protecció de dades per part de l'investigador i responsable del tractament. Els CER han de comprovar que la informació no indueix a error, ni genera falses expectatives. És necessari, a més, determinar els usos que es poden fer de la "marca institucional", que servirà com a principal aval dels resultats que es presentin.

1.2. Als comitès d'ètica de la recerca sobre la seva composició i funcions:

A) Integrar perfils experts en tecnologies emergents.

És urgent que els CER integrin perfils de manera permanent o com a assessors a experts en intel·ligència artificial, ciència de les dades i, en particular, en tècniques de seudonimització així com en el desenvolupament de dispositius digitals de salut entre els quals s'inclouen les *Apps*, els *Wearables* i la internet de les coses. Cada tecnologia hauria de comptar amb un expert en la matèria per a avaluar i participar en les deliberacions prèvies a l'emissió de dictamen.

B) Contribuir a generar una cultura de respecte per la intimitat de les persones a través de la protecció de les dades personals.

Es reivindica aquí la funció de sensibilització sobre qüestions bioètiques dels comitès d'ètica que propugna la Declaració Universal sobre Bioètica i Drets Humans de la UNESCO de 2005 (art. 19 d).

2. Als centres de recerca i innovació:

A) Destinar el pressupost suficient per a dotar als CER dels recursos humans i materials per a una adequada avaluació i que permeti seguiment dels projectes de recerca i innovació en salut.

La recerca és el pilar del nostre sistema de salut i si bé l'avaluació amb caràcter previ és condició *sine qua non* per a que aquesta es pugui desenvolupar, també és necessari efectuar el seguiment dels projectes durant la seva execució i fins a la seva la finalització, inclosa la publicació de resultats i la gestió de les dades.

B) Assegurar la independència dels CER per a prendre decisions.

Els CER no responen a interessos institucionals o espuris, tampoc als interessos particulars d'investigadors, promotors o altres tercers implicats en els processos de recerca i innovació. Per a assegurar la seva independència és necessari establir regles i procediments per a la detecció, declaració i corresponent gestió dels conflictes d'interessos que no sols poden ser de naturalesa econòmica, sinó que també poden donar-se per raó de parentiu, amistat, o jerarquia.

C) Garantir la independència del Delegat de Protecció de Dades.

La figura del Delegat de Protecció de Dades establerta en el Reglament General de Protecció de Dades i en la Llei orgànica de Protecció de Dades Personals i garantia dels drets digitals, ha estat incorporada en alguns casos, sense respectar l'esperit independent, afavorint els conflictes d'interessos i la falta de transparència. Tal com estableix el Reglament, el Delegat de Protecció de Dades pot formar part de la plantilla del responsable o de l'encarregat del tractament o bé actuar en el marc d'un contracte de serveis. Els CER en l'àmbit de la salut, biomèdic o del medicament, han d'integrar entre els seus membres un Delegat de Protecció de Dades o, en el seu defecte, un expert amb coneixements suficients del Reglament que s'ocupi d'activitats de recerca que comportin el tractament de dades personals (la Llei orgànica de Protecció de Dades i garantia dels drets digitals, Disposició addicional dissetena).

3. Al legislador:

3.1. Sobre la naturalesa i regulació dels comitès d'ètica de la recerca:

A) Desenvolupar reglamentàriament les competències, funcions, constitució, acreditació, composició i funcionament dels comitès dels CER.

Els CER necessiten un desenvolupament normatiu amb caràcter urgent sobre les competències, funcions, constitució, acreditació, composició i funcionament, que està pendent des de la promulgació de la Llei de Recerca Biomèdica (2007).

B) *Crear comitès d'ètica de la innovació.*

Mentre no es prioritzi cobrir aquesta necessitat, els CER seguiran al límit. A la falta de recursos humans i materials, s'afegeix una sobrecàrrega evident: continuaran avaluant projectes de recerca a l'ús i, a més, les iniciatives provinents de les àrees d'innovació d'hospitals i centres de recerca que utilitzen tecnologies emergents i dades personals, sense la comprensió ni les pautes adequades per a avaluar els tractaments de dades personals. L'aval ètic dels citats projectes ve determinat pel dictamen favorable dels CER d'institucions de reconegut prestigi.

Crear comitès específics per a aquesta mena d'estudis, de forma relativament centralitzada, o habilitar aquestes funcions a uns pocs comitès ja existents que puguin assumir aquesta càrrega de treball. La condició seria que en la seva composició en formés part un membre del CER i viceversa per a compartir informació.

C) *Incorporar de manera real i quantificable la Recerca i Innovació Responsable (RRI per les seves sigles en anglès) que Europa propugna mitjançant el desenvolupament de directrius comunes perquè els CER puguin avaluar les agendes que la componen: l'ètica, la igualtat de gènere, l'educació científica i l'accés obert.*

I especialment, *el public engagement* per a que, a partir de la cooperació entre els diferents actors implicats, sigui possible alinear millor el procés de recerca i els seus resultats amb els valors, les necessitats i les expectatives de la societat actual. L'objectiu és reduir la bretxa que existeix entre la comunitat científica i la societat, incentivant que diferents grups d'interès treballin junts en tot el procés de recerca i innovació.

3.2. Sobre la regulació dels usos de dades personals en recerca i innovació en salut:

A) *Desenvolupar la disposició addicional dissetena sobre els tractaments de dades de salut de la Llei orgànica de Protecció de Dades i garantia dels drets digitals* que és insuficient per a tractar els usos de recerca. S'aconsella un desenvolupament normatiu que permeti fer front de manera adequada als reptes actuals en l'àmbit de la recerca i la innovació.

B) *Regular l'àmbit de la telemedicina, la teleassistència i els dispositius digitals i aplicacions de salut, Apps, incloses* en els processos de recerca i assistencials que tractin dades personals. També es fa necessari revisar les mesures establertes per a la protecció de dades en els processos de contractació pública en l'àmbit hospitalari i sociosanitari.

3.3. Sobre les infraestructures per al tractament de dades, incloses les dades personals en recerca i innovació en salut:

A) *Potenciar la creació d'infraestructures europees per a la gestió de dades finançades amb fons públics*, per a que els tractaments de dades personals amb finalitats de recerca i innovació en salut no depenguin de les grans empreses tecnològiques, fonamentalment dels Estats Units.

B) Construir un model de gestió de les dades que permeti el seu accés i la seva combinació en condicions de seguretat, fiabilitat, traçabilitat, qualitat i, especialment, que permeti la seva interoperabilitat i reutilització.

C) Crear estructures de governança de les dades personals que permetin un seguiment des del disseny, durant i una vegada finalitzada la recerca i la innovació en salut.

3.4. Sobre l'educació digital:

A) Desenvolupar reglamentàriament i mitjançant les accions que corresponguin per a aconseguir l'alfabetització i l'educació digital establerta en la Llei orgànica de Protecció de Dades i garantia dels drets digitals (art. 83). Aquesta hauria de ser una prioritat, i des de l'escola, però en particular, per als diferents operadors que prenen decisions en l'àmbit de la recerca i innovació en salut.

B) Potenciar la intel·ligibilitat de l'anàlisi de les dades i de la presa de decisions, evitant la denominada caixa negra de les intel·ligència artificial. L'objectiu final és evitar asimetries entre la informació personal que acumulen tercers -per les dades de què disposen-, i la capacitat de control dels seus titulars.

---

[1] En relació a la normativa aplicable sobre protecció de dades personals en projectes de recerca i innovació en salut vegeu: Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) (Text pertinent a l'efecte del EEE) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679 i Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades i garantia dels drets digitals https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[2] De LECUONA, I. "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (Big Data)" *Gaceta Sanitaria*, Vol. 32. Núm. 6, p. 576-578. 2018. DOI: 10.1016/j.gaceta.2018.02.007 https://www.gacetasanitaria.org/es-evaluacion-los-aspectos-metodologicos-eticos-articulo-S0213911118300864

[3] En aquest sentit vegin-se els resultats de treballs de recerca previs del OBD CASADO, M. (Coord.) *De la solidaridad al mercado: el cuerpo humano ante el comercio biotecnológico*, Editorial Fontamara, México, 2016. ISBN: 978-84-475-4193-5 i editat por Edicions i Publicacions de la UB en 2017 en format electrònic http://www.publicacions.ub.edu/ficha.aspx?cod=08646 i GARCÍA MANRIQUE, R. (Coord.), *El cuerpo diseminado. Estatuto, uso y disposición de los biomateriales humanos*, Editorial Aranzadi, Cizur Menor, 2018. ISBN: 978-84-9177-750-2, disponible també en format electrònic.

[4] Els Documents i Declaracions del Grup d'Opinió del OBD estan disponibles en accés obert, en format pdf i en diversos idiomes en: http://www.bioeticayderecho.ub.edu/es/publicaciones

[5] Un exemple en el context de la pandèmia per COVID-19 és *EUvsVirus Hackathon to develop innovative solutions and overcome coronavirus-related challenges (24-26 de abril de 2020).* https://ec.europa.eu/info/news/euvsvirus-hackathon-develop-innovative-solutions-and-overcome-coronavirus-related-challenges-2020-apr-03_en

[6] Mercat únic digital europeu: https://ec.europa.eu/digital-single-market/en/news/digitalyou-digital-trust

[7] Programa de recerca de la Unió Europea HORIZON 2020: Salut, canvi demogràfic i benestar https://ec.europa.eu/programmes/horizon2020/en/h2020-section/health-demographic-change-and-wellbeing

[8] El 20 de febrer de 2020 la Unió Europea va presentar el seu "paquet digital" que inclou l'estratègia de Dates i Intel·ligència Artificial: https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data. Bruselas, 19.2.2020 COM(2020) 66 final. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf y WHITE PAPER On Artificial Intelligence - A European approach to excellence

and trust Bruselas, 19.2.2020 COM(2020) 65 final. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[9] Grup d'Experts d'Alt Nivell sobre Intel·ligència Artificial de la Unió Europea, "Guies ètiques sobre intel·ligència artificial" https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence Es refereix a evitar els biaixos per raó de raça o de gènere entre altres i a evitar la discriminació algorítmica.

[10] Les dades personals són qualsevol informació relativa a una persona física viva identificada o identificable. Les diferents informacions, que recopilades poden portar a la identificació d'una determinada persona, també constitueixen dades de caràcter personal. Exemples de dades personals: nom i cognoms, domicili, adreça de correu electrònic, del tipus nom.cognom@empresa.com, número de document nacional d'identitat, dades de localització (com la funció de les dades de localització d'un telèfon mòbil) (*), adreça de protocol d'internet (IP), l'identificador d'una cookie (*), l'identificador de la publicitat del telèfon, les dades en poder d'un hospital o metge, que podrien ser un símbol que identifiqués de manera única a una persona. Vegeu Unió Europea: "Què són les dades personals" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es El Reglament general de protecció de dades indica en l'article 9 com a categories especials de dades: origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, o l'afiliació sindical, i el tractament de dades genètiques, dades biomètriques dirigides a identificar de manera unívoca a una persona física, dades relatives a la salut o dades relatives a la vida sexual o les orientacions sexuals d'una persona física.

[11] SWEENEY, L., "Simple Demographics Often Identify People Uniquely". Carnegie Mellon University, Data, Privacy Working Paper 3. Pittsburgh 2000. https://dataprivacylab.org/projects/identifiability/paper1.pdf

[12] LLÀCER, R.M., CASADO, M., BUISÁN, L. *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Ed. UB, Barcelona, 2015 . Disponible a: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf

[13] Vegeu per exemple la Història Clínica Compartida de Catalunya: https://ticsalutsocial.cat/es/projectes/oficina-interoperabilidad/hc3/ i el Sistema d'Informació per al desenvolupament de la Investigació en Atenció Primària (SIDIAP) https://www.sidiap.org/index.php/es

[14] SANTALÓ, J. y CASADO, M. (coords.), "Documento sobre bioética y edición genómica en humanos", Ed. Universitat de Barcelona, 2016, Barcelona. ISBN 978-84-475-4073-0. Disponible a http://hdl.handle.net/2445/105022

[15] "How should we think about clinical data ownership?", *Journal of Medical Ethics*, Ballantyne, Vol. 46, 2020, p. 289–294. Disponible a https://jme.bmj.com/content/medethics/46/5/289.full.pdf

[16] La Reial Acadèmia Espanyola defineix "seudonimización" com a "tractament de dades personals de manera tal que ja no puguin atribuir-se a un interessat sense utilitzar informació addicional, sempre que aquesta informació addicional figuri per separat i estigui subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribueixen a una persona física identificada o identificable. I es refereix específicament a l'article 4.5 del Reglament general de protecció de dades.

[17] Vegeu per exemple la nota d'Agència Espanyola de Protecció de Dades sobre necessitat d'avaluar els tractaments de dades personals de *l'App* Radar COVID (juny de 2020) https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-sobre-la-participacion-de-la-aepd-en-la-app-de i el *Manifiesto en favor de la transparencia en desarrollos de software públicos*, signat per més de 230 acadèmics i investigadors (setembre de 2020) https://transparenciagov2020.github.io/ (última consulta, 5 d'octubre de 2020).

[18] EUROPEAN COMMISSION, *Guidance How to complete your ethics self-assessment European Union*, febrer 2019. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

[19] En aquest sentit vegeu el Reglament General de Protecció de Dades, article 5 Principis relatius al tractament

1. les dades personals seran: b) recollits amb fins determinats, explícits i legítims, i no seran tractats ulteriorment de manera incompatible amb aquests fins; d'acord amb l'article 89, apartat 1, el tractament ulterior de les dades personals amb fins d'arxiu en interès públic, fins d'investigació científica i històrica o fins estadístiques no es considera incompatible amb els fins inicials.

[20] Vegeu la *Guia d'avaluació dels aspectes derivats de la normativa de Protecció de Dades en projectes de recerca*, editada per la Direcció General de Recerca i Innovació en Salut, Direcció General d'Ordenació i Regulació Sanitària i Oficina del Delegat de Protecció de Dades- Fundació TIC SALUT SOCIAL, de 31 de juliol de 2020.

[21] Sobre aquestes qüestions vegin-se les aportacions de la Comissió de Bioètica de la Universitat de Barcelona (CBUB), en particular, els formularis en funció de la mena de recerca a desenvolupar, així com altres requisits a complir per a adaptar-se a la normativa de protecció de dades.

http://www.ub.edu/comissiobioetica/es/formularios La CBUB va ser fundada per la Dra. María Casado en 1996, sent la primera comissió de bioètica d'una universitat pública en el nostre context. Posteriorment, l'any 2002 crea també la Xarxa de comitès d'ètica de les universitats espanyoles i altres organismes públics de recerca (RCEUC). La CBUB i la RCEUE han estat considerades des de 2012 com a referents de bona pràctica per universitats membre de la Lliga Europea de Recerca Intensiva (LERU, per les seves sigles en anglès). Vegeu l'informe "Towards a Research Integrity Culture at Universities: From Recommendations to Implementation", LERU, gener de 2020. https://www.leru.org/files/towards-a-research-integrity-culture-at-universities-full-paper.pdf

[22] Vegeu l'eina *Gestiona EIPD* de l'Agència Espanyola de Protecció de Dades. *Gestiona EIPD* és un "assistent per a l'anàlisi de riscos i avaluacions d'impacte en protecció de dades. Aquesta eina gratuïta guia als responsables i encarregats del tractament en els aspectes que s'han de tenir en compte, proporcionant una base inicial per a una gestió adequada" https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd. També la Guia pràctica i la plantilla avaluació de l'impacte relativa a la protecció de dades del Reglament general de protecció de dades desenvolupada per l'Autoritat Catalana de Protecció de Dades. https://apdcat.gencat.cat/ca/drets_i_obligacions/responsables/obligacions/avaluacio-impacte-relativa-proteccio-dades/. El OBD en col·laboració amb un equip interdisciplinari ha desenvolupat una metodologia específica per a efectuar avaluacions d'impacte relatives als tractaments de dades personals en l'àmbit de la salut i la innovació a proposta de la Fundació TICSalut, Oficina del Delegat de Protecció de Dades.

[23] EUROPEAN COMMISSION, H2020 Programme Guidelines on FAIR Data Management in Horizon 2020 26 de juliol de 2016;

https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf i CSUC, Gestió de dades de recerca, https://www.csuc.cat/es/consorciacion-tic/gestion-de-datos-de-investigacion

[24] LERU, *Open Science and its role in universities: a roadmap for cultural change*, mayo de 2018 i EUROPEAN COMMISSION, https://ec.europa.eu/digital-single-market/en/open-science

[25] Véase EUROPEAN DATA PROTECTION SUPERVISOR, Flowcharts and Checklists on Data Protection , 2020 https://edps.europa.eu/sites/edp/files/publication/flowcharts_and_checklists_on_data_protection_brochure_en_1.pdf

Guidelines for reviewing health research and innovation projects that use emergent technologies and personal data

PRESENTATION

Reviewing the methodological, ethical, legal and social aspects of health research projects is a duty of Research Ethics Committees (RECs). In our context, the approval of projects in which people take part and personal data and/or biological samples of human origin are used, depends on these legally established interdisciplinary collegiate bodies. It is mandatory for the proposed interventions to be conducted in order to obtain a favourable opinion in both public and private research centres. In Europe different formulas coexist: RECs can be national and regional, although there is also the possibility of each research centre having its own REC or adhering to one already created. All of them must be accredited by the relevant body, after meeting a series of requirements and conditions.

RECs were initially created to assess clinical trials of medicinal products for human use and medical devices, before going on to review other types of research that, due to their characteristics, also pose the need to find a balance between progress in scientific knowledge, freedom of research and the protection of participants. Examples of the latter are the projects that use emergent technologies such as artificial intelligence (AI), big data, biometrics and virtual reality, among others, as well as the development of health devices and apps. Recently, moreover, RECs have been asked to review purely innovation projects in the field of health care.

In these knowledge creation and transfer processes, the interests of science, technology and society must not prevail over those of the individual. Therefore, RECs must analyse the scientific soundness of the proposals, their social value, and weigh up the rights and interests at stake. Research is an activity that always entails some risks for those taking part – such as the risk of the breakdown of confidentiality in projects that handle personal data. And these risks must be weighed against the benefits, from which, very often, the participant gains no personal or direct advantage.

Scientific and technological changes are occurring at a dizzying rate, in an exacerbated market society where health is being increasingly commodified, and in which personal data are monetized. Although it is true that lawmaking processes and knowledge creation and transfer rates are not the same, there is a certain paralysis in the application of laws, due basically to a lack of understanding of the digital phenomenon that we are facing. It is therefore considered that RECs are willing and able to act as guarantees that research, and the innovation that goes with it, comply with ethical principles and meet the established legal requirements.[1]

The digital society, data driven, based, therefore, on the intensive exploitation of datasets, including personal data, has clearly shown that the current review model – a child of the second half of the 20th century – for analysing research projects in which humans take part and/or their data personal is used, is outdated and ineffective, due to the technical, ethical and legal challenges posed by personal data processing in the 21st century.

Nowadays, RECs must protect people by safeguarding their personal data and ensuring their owners' privacy and confidentiality. Moreover, they must promote and guarantee the

exercise of autonomy to make free and informed decisions, avoid discrimination (specifically when it is covert), and guarantee fairness and transparency. The balance that RECs must reach between maximizing the benefits and minimizing the risks also includes processing personal data properly. In sum, as the processes of gathering and processing data are the niche in which to conduct research and innovation, it is a priority for RECs to become aware of the importance of the new digital paradigm based on the intensive exploitation of personal data, including health personal data.[2]

The COVID-19 pandemic has put to the test RECs' ability to suitably analyse projects and give priority to those that benefit the collective interest and public health. RECs are currently working under pressure, and they are required to rapidly review a large number of research and innovation projects that are submitted: clinical trials for the development of vaccines and drugs, and other kinds of research. There are also many other projects that have to be reviewed, which do not require any direct intervention on people but which imply access to, and the processing of, personal datasets, including those of health. In particular, projects to develop systems for the prediction and management of COVID-19 are aggravating the problems that RECs have been facing in recent years. These are therefore not new issues, but it is true that they have intensified due to the exceptional situation that we are living through, in which the serious deficiencies of our review model have become obvious.

Faced with this situation, the Opinion Group of Barcelona University's Bioethics and Law Observatory – UNESCO Chair of Bioethics (OBD), an interdisciplinary research centre of the University of Barcelona, has analysed the challenges, the unresolved issues and the problems arising in health research and innovation projects. The goal is to contribute with guidelines to help to homogenize the issues that RECs have to analyse and review as well as the information to be requested from project leaders, in order to prevent opportunists from opening personal data markets disguised as research and innovation and, in particular, under the pretext of the pandemic. And also to avoid the privacy of the participants in these projects from being publicly exposed without their consent.[3]

The proper review of personal data processing in health research and innovation projects must be a priority for RECs, as mechanisms to protect individuals. The main hurdle is that they have not yet adapted to the digital paradigm, and to the changes brought about by health research and innovation processes that depend on the intensive exploitation of personal datasets, and this is causing severe problems. The experience of OBD members on different ethics committees (RECs, national bioethics committees, healthcare and *ad hoc* ethics committees), which is reflected in this paper, allows us to provide a practical perspective together with the analysis of the theoretical framework.

On this occasion the author of this paper is Dr Itziar de Lecuona, doctor of law, assistant professor in the Department of Medicine and the deputy director of the OBD, who has coordinated the Opinion Group and has received contributions from the academics, researchers and professionals who are listed at the end of the document.

Since 1996, the OBD has been making a scientific and interdisciplinary analysis of the ethical, legal and social implications of biomedicine and biotechnology, and it has a bearing on the dialogue between the university and society through the transmission of scientific and technological knowledge and the arguments necessary to take part in a truly informed social debate. For this purpose, the Opinion Group has already drafted 31 documents and declarations[4] concerning topical issues, on which there is no agreed opinion, either in

society or in the scientific communities involved; this has made it necessary to identify the problems, compare the arguments and propose recommendations.

The analysis and the recommendations that the Group makes are addressed mainly to the members of the RECs involved in reviewing the abovementioned health research and innovation projects, to protect the privacy of the data owners, and to guide their processing so that unnecessary exploitation of personal datasets is avoided, and to prevent their commercialization. Research must meet the needs of society and not spurious interests. The paper is also addressed to the research and innovation ecosystem, and calls upon the political and legislative authorities to take the recommendations into consideration.

THE STATE OF THE QUESTION

In hospitals and research centres COVID-19 has produced a flood of research and innovation proposals for its early detection and management. These are based on the application of artificial intelligence and emerging technologies like big data and biometrics, and may entail the development of health devices, applications (apps) included. Examples of these projects are the development of COVID-19 prediction systems, based on the programming of algorithms, which are fed by different personal datasets stored in medical records and in other databases, as well as the information sent by the data owners in different formats. Hackathons[5] also proliferate, or challenges to develop algorithms as part of projects in medicine to predict the risk of developing particular complications. The aim is to increase the available knowledge, develop personalized interventions and improve decision-making. Thus, in healthcare, proposals are considered that may be based on research protocols, and others, for innovation in the field of healthcare, which share the challenge of ensuring that the privacy of the owners of the personal data that they need to process is protected. These initiatives ought to have a clear social benefit.

Since the beginning of this century, Europe has been committed to a data-driven society. It is a political and economic decision, which also includes knowledge creation and transfer processes. The goal is a single, competitive digital market, capable of guaranteeing the protection of people's rights and freedoms and promoting research and innovation based on the intensive exploitation of datasets, including personal data.[6] In the field of healthcare this commitment results in more personalized medicine, more efficient health care systems, the prediction of the adverse effects of drugs with a smaller number of people exposed to risk, active ageing and well-being; and pandemic prediction and management systems, as in the case of COVID-19, among other priorities. All these areas, in which many substantial public and private research and innovation consortia are funded, based on the said technologies and on the development of mHealth, are underlain by the exploitation of datasets, including personal data, and for which the participation of third parties traditionally outside the field of biomedicine and healthcare is necessary.[7] These third parties, who may be either private companies or even public authorities, are interested in accessing different personal datasets, for what they may say about their owners and for what they could predict, an interest that may be different from, and even contrary to, that of the research project leaders.

In a few years we have rapidly gone from enthusiasm over big data to devotion for artificial intelligence, virtual reality and the Internet of Things. Just before the pandemic, Europe presented its Digital and Artificial Intelligence Strategy,[8] which from the ethical perspective

must be "trustworthy",[9] capable of avoiding bias due to race or gender and human-centric. Despite this laudable political decision, it is necessary to remember the lack of public infrastructures in Europe to make it possible to store, use and share data, and to ensure its interoperability and reuse. This situation shows up Europe's excessive dependence on the American tech companies, known as the GAFAM Empire (Google, Apple, Facebook, Amazon and Microsoft).

Thus, personal data are the gold of our time, and health, biometric and socio-demographic data, especially, are considered by law to be special categories of data[10] that require the highest protection because they say everything about us; and because they could be used for unwanted purposes and give rise to covert discrimination, with profound implications for people's freedom and that of future generations. The possession of personal datasets by third parties, whether private or public initiatives, could affect our rights depending on the uses, giving these third parties extraordinary power over us, a situation that goes unnoticed by the great majority of people. The decisions taken in the field of health research and innovation and in highly digitized contexts will mark the lives of people, groups and societies.

In the digital society we have ceased to be anonymous and have become re-identifiable. Our gender, postcode and date of birth identify us with a very high percentage of success.[11] The OBD's Opinion Group drew attention to these issues in 2015, in the "Document on Bioethics and Big Data: Exploitation and Commercialization of User Data in Public Health Care."[12] Due to the development of technology and the huge amount of personal information amassed in different databases, and to the data we disclose, it is possible to create patterns of behaviour, predict conducts and, therefore, improve decision-making. For that it is necessary to programme algorithms that are fed by datasets including personal data. These personal data, as the main raw material, are the property of their owners, who in turn will be the final targets of the results of the research and innovation processes with the special situation of health data. As is well known, electronic medical records,[13] conveniently structured, according to quality and security criteria, contain personal health and socio-demographic data, and personal data that are interesting for what they say about us and what they can predict.

Health research and innovation takes place in a highly competitive environment of globalized ultra-liberalism and market dominance[14] in which separate areas make common cause, for instance those of research, innovation, application of knowledge and business. This situation in which research, innovation, application and business are allied must be emphasized. In this context the debate has begun about the ownership of personal data, about data altruism[15] when our health research and innovation system has traditionally been based on solidarity, always with the option not to take part freely and voluntarily in these donation processes, without it having any negative consequences. This altruistic and solidarity-based model, which entails a certain cession of personal information, must result in treatments and interventions for the data owner, or for patients and the future generations. It may also involve the increase of knowledge with no direct benefit. This cession must not mean that certain personal datasets, especially health personal data, are available to anyone. Here we must remember that access to personal data for healthcare and research purposes implies the healthcare professional's duty of secrecy in order to maintain the confidential nature of the information.

Faced with the change brought about by the intensive exploitation of personal data and the high likelihood of re-identification, the crux of the matter lies in what kind of personal data

are going to be requested, how they are going to be obtained and stored, and how they are going to be processed, whether codified or pseudonymized,[16] who is going to have access, for how long, and what is going to happen with the personal data once the intervention is over. At the same time, the interest is focused on how datasets are going to be combined, for example, those stored in heavily protected electronic medical records with other personal data from other databases outside the health system, which could refer to their owners' patterns of behaviour through the analysis of their mobile telephone database, or others, such as health surveys.

For the management of COVID-19 we have witnessed the development of apps that invite individuals to contribute personal data such as their health card and geo-location for starting a survey on the symptoms, to be able to predict whether the person is possibly positive, and as a support in the field of public health. After that, a belated debate, not at all transparent, has begun on technological security and the protection of privacy with apps to identify positives and trace contacts.[17] It ought to be possible for this personal information, duly obtained and stored, to be combined with other health data, as has been mentioned, so that it may be useful for decision-making for the good of the people and the public interest. These examples of research and innovation processes must have the approval of the relevant RECs.

DECLARATION

To guide decision-making in the contexts of health research and innovation, in the face of the intensive exploitation of personal data, the following considerations to suitably protect people should be made:

- It is no longer possible to guarantee anonymity. We have ceased to be isolated pieces of data and have become datasets, stored in different databases that can be combined with the aim of drawing conclusions to improve decision-making; so we have gone from being anonymous to being re-identifiable.
- The protocols for obtaining participants' consent have clearly become obsolete due to the fact that it was presumed not only that data were anonymous, but that they would remain so in the future.
- The COVID-19 pandemic has been the spur for confirming what was obvious: the serious problems for accessing and interpreting data that are so necessary for making progress in political decision-making based on scientific evidence.
- The data stored are not connected to one another, nor are they suitably pseudonymized, and there is a lack of public infrastructures to make this happen, which is a hindrance for scientific knowledge, and also for the different actors in the research, innovation and development system.
- The dependence of countries and the European Union on the major, fundamentally American, tech companies are excessive and should be urgently reversed.
- The process of combining personal datasets by using emergent technologies and the development of algorithms ought to be beneficial for people and not expose them to clear or covert discrimination, or to unwanted uses.
- The support implied by technology must not lead to the digital surveillance of people.
- Neither governments nor the major tech companies should have absolute control over personal data, and their processing operations should be guided by criteria of transparency and accountability to avoid the opacity that prevails in digital environments.

- There is a tendency to the commodification of personal data in the field of healthcare and to their monetization, particularly on account of the COVID-19 pandemic.
- Decisions must be based on scientific evidence and not on proposals prone to personal data markets disguised as health research and innovation.
- An identifiable individual is someone who can be identified, directly or indirectly, especially by referring to an identifier such as a name, an identity number, geo-location data, an online identifier, or one or more specific factors of that individual's physical, physiological, genetic, mental, economic background, and cultural or social identity.
- Personal data are: name, genetic and biometric data, address, identity number, pseudonym, occupation, email address, CV, geo-location data, Internet Protocol (IP) address, cookie identifier, telephone number, data provided by smart meters, and data in the possession of a hospital or research centres.[18]
- Special categories of data are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- Along with the legislation in force, ethical and deontological duties for the protection of the privacy and the confidentiality of personal data in heavily digitized environments for healthcare professionals, but also for the different professionals involved, are applicable.
- RECs lack the proper composition and the necessary skills to review the research and innovation projects that are considered here. There is thus an urgent need for them to become digitally literate, because of the responsibility these bodies have with regard to the protection of the rights of those involved in processes of research and innovation, including freedom and research, together with other basic rights such as the privacy and the confidentiality of personal data.
- RECs must be able to identify potential problems and conflicts of interest that may arise in relation to the use of personal data, and what information to request from project leaders, in order to guarantee the protection of individuals' rights.
- Research and innovation must be justified due to their scientific soundness and social value; people's rights may be restricted in a proportionate and justified way for reasons of public health and collective interest, but never annulled. Under no circumstances, and even less so during a pandemic, must levels of protection be relaxed.

RECOMMENDATIONS

1. To Research Ethics Committees:

1.1. Concerning health research and innovation projects that use emergent technologies and personal data:

A) Confirm and review compliance with the principles of data protection.

Personal data processing must be based on the following principles:

"Lawfulness, fairness and transparency" in relation to the data subject; "purpose limitation" meaning that data should be collected for specified, explicit and legitimate purposes[19];; "data minimization", which means that the data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; "accuracy" meaning that data should be accurate and, where necessary, kept up to date and that every

reasonable step must be taken to ensure that personal data that are inaccurate, with regard to the purposes for which they are processed, are erased or rectified without delay; "storage limitation" and "integrity and confidentiality", which refers to the fact that the data are processed securely. The data controller will be responsible for compliance with these principles and will be able to demonstrate it (proactive responsibility). The data controller is obliged to protect data "by design", and "by default" to determine the technical and organizational measures necessary to ensure compliance with the above principles.[20]

To comply with these principles, RECs, when assessing research and innovation projects, must confirm and assess:

a) If the process of informing and gaining the informed consent of the potential participants in projects complies with the requirements established by law;

b) If the personal data are going to be codified, pseudonymized or anonymized;

c) The format in which the personal data will be stored;

d) If the personal data are going to be sent within and/or outside the European Union, with the corresponding guarantees, and if they are going to be shared with third parties; and

e) If there are Cloud services, and under what kind of what conditions.

B) Ensure the non-identification of participants, which will require the incorporation of experts in pseudonymization techniques, especially, as members or advisers.

Avoid generally resorting to the concept of "anonymization", as it generates a false sense of security. Words matter and RECs should not overlook this issue and should include possible types of processing in project presentation models or in the corresponding indications and, therefore, the differences between anonymized, codified and pseudonymized data. In this respect, a common mistake detected in project reports, protocols, and in patient information and informed consent leaflets, is to point out that the data will be anonymized when from the analysis of data processing it is confirmed that they will be pseudonymized. RECs must verify the planned techniques to ensure the non-attribution of personality to the datasets processed, that is, the non-identification of the data owner. These are eminently technical issues that require having experts or advisers on RECs who can independently assess and confirm that the proposals are suitable.

C) In the event of the institution not having its own specific protection system, the conditions guaranteeing personal data protection must be agreed contractually.

A recurring example of malpractice is resorting to free digital services to conduct online surveys for personal data processing that do not protect privacy, unless specific services are contracted for this. This situation raises ethical and legal issues, given that disclosing personal data on platforms that by default monetize personal data in environments unprotected by third parties is also a violation of scientific integrity.[21] If the institutions participating in these projects do not have specific privacy protection services, the data controller must ensure this protection by reaching agreements with third parties to provide these services, and demonstrate it by the presentation of the relevant contractual agreements.

D) Demand and review "Data Protection Impact Assessment" in cases in which the General Data Protection Regulation demands it.

RECs must demand and review "data protection impact assessment" (DPIA), an assessment of the impact of processing operations on personal data protection, which should be made by the data controller. In certain cases, as in that of the processing of special categories of data such as health, genetic and biometric; processing that involves profiling; and/or automated decision making, among others, RECs must make sure that the project has been subject to DPIA. This can be done by following methodologies that make it possible to identify the risks associated with processing.[22] From DPIA an action plan will result that must be carried out to mitigate the risks detected and which will have to be reviewed periodically and updated in the event of possible changes in data processing. This review must not be thought of as a mere formality, but as a living process that may be subject to change and which makes it possible to properly monitor the project and the guarantees to be applied for personal data protection. The Data Protection Officer is the independent figure advising on these procedures.

E) Request and review the Data Management Plan.

RECs must request the Data Management Plan from the project leader, which describes how new data are obtained, processed and, where appropriate, new data generated in the context of the project; and what will happen to them when the project is over.[23] At the same time, the Plan includes formulas for the data to be found, accessible, interoperable and reusable. "Open science", in the framework of the digital society, obliges RECs to check what methodologies and standards will be applied and if the data are going to be shared in open access.[24] It must be stressed that the Data Management Plan comes within risk analysis and the adoption of security measures required by the General Data Protection Regulation in all cases, whether or not a data protection impact assessment is made.

F) Check that the potential participants in health research and innovation projects are informed about their rights and the conditions for exercising them.

The right to be informed; of access; of rectification; to be forgotten; to restrict data processing; to data portability and to not be the object of an automated decision that should incorporate human intervention and correction, and which includes profiling. At the same time, information must be given about the right to revoke, ensuring that the personal information of the person who requests it is deleted from the correspondent database.

G) Check that protocols and information and informed consent leaflets state explicitly and in detail who the data controller is.

RECs must act in coordination with the legal services of the entitled institution to review the agreements ordering data processing and transfer and, when appropriate, the agreement for co-responsibility over processing[25].

It is necessary for RECs to establish a fluid channel of communication with the managers of the institutions' departments of information technologies and communication.

H) Request that privacy policies and legal warnings be included in the project report.

RECs can assess compliance by the researcher and data controller with data protection rights and responsibilities. RECs should check that the information is not misleading, nor generates

false expectations. It is further necessary to determine the uses that can be made of the "institutional brand", which will serve as the principal guarantee for the results presented.

1.2. To Research Ethics Committees, concerning their composition and duties:

A) Include experts on emergent technologies.

RECs must urgently incorporate, permanently or as advisers, experts in artificial intelligence, data science and, especially, pseudonymization techniques, and also in the development of mHealth devices, including apps, wearables and the Internet of Things. Each technology must have an expert on the subject to assess and to take part in the deliberations prior to the issue of a ruling.

B) Contribute to generating a culture of respect for people's privacy through personal data protection.

The role played by ethics committees in raising awareness about bioethical issues, advocated by UNESCO's Universal Declaration on Bioethics and Human Rights, of 2005 (art. 29 d), is stressed here.

2. To research and innovation centres:

A) Allocate enough funds to equip RECs with the human and material resources for a proper assessment that makes the monitoring of health research and innovation projects feasible.

Research is the mainstay of our health system and although prior assessment is a *conditio sine qua non* for it to be carried out, it is also necessary to monitor projects from start to finish, including the publication of results and data management.

B) Ensure RECs' independence for decision-making.

RECs do not respond to institutional or spurious interests, or to the private interests of researchers, promoters or other third parties involved in the processes of research and innovation. To ensure their independence it is necessary to establish rules and procedures for the detection, declaration and corresponding handling of conflicts of interest that may not only be economic, but which may arise due to kinship, friendship or hierarchy.

C) Guarantee the independence of the Data Protection Officer.

The Data Protection Officer, established in the General Data Protection Regulation and in the Organic Law on Personal Data Protection and Guarantee of Digital Rights, has been incorporated in some cases without respecting their independence, fomenting conflicts of interest and the lack of transparency. As established by the Regulation, the Data Protection Officer may be a member of the data controller or data processor´s staff, or act within the framework of a service contract. Furthermore, according to RECs in the field of healthcare, biomedicine or medicinal products must include a data protection officer among their members or, failing that, an expert with sufficient knowledge of the Regulation to oversee research activities involving personal data processing (Organic Law of Data Protection and Guarantee of Digital Rights,17th Additional Provision).

3. To the legislator:

3.1. Concerning the nature and regulation of Research Ethics Committees:

A) *Legally develop the powers, duties, constitution, accreditation, composition and workings of RECs.*

RECs urgently need a normative development of powers, duties, constitution, accreditation, composition and workings, pending since the enactment of the Law of Biomedical Research (2007).

B) *Create innovation ethics committees.*

As long as meeting this need is not given priority, RECs will be stretched to the limit. On top of the lack of human and material resources there is an obvious overload: they will continue to review ordinary research projects and, moreover, initiatives from hospital and research centre innovation departments, based on the abovementioned emergent technologies, without the understanding or the guidelines suitable for assessing personal data processing. The ethical backing of these projects is determined by the favourable ruling of the RECs in institutions of acknowledged prestige.

Create specific committees for these types of studies, in a relatively centralized way, or authorize a few already existing committees to take on the workload and perform these functions. The condition would be that they include a member of the REC, and vice-versa, to share information.

C) *Incorporate the Responsible Research and Innovation (RRI) that Europe is advocating through the development of common guidelines so that RECs can assess the agendas that comprise it: ethics, gender equality, scientific education and open access.*

And especially, *public engagement,* so that, based on cooperation between the different actors involved, it may be possible to better align the process of research and its results with the values, the needs and the expectations of today's society. The aim is to reduce the gap existing between the scientific community and society, incentivizing different interest groups to work together throughout the research and innovation process.

3.2. Concerning the regulation of the uses of personal data in health research and innovation:

A) *Develop the 17th Additional Provision concerning health data processing in the Organic Law of Data Protection and Guarantee of Digital Rights*, which is insufficient to deal with research uses. A normative development is recommended, to make it possible to adequately meet the current challenges in the field of research and innovation.
B) *Regulate the scope of telemedicine, telehealth and mHealth devices and applications, apps included*, in the processes of healthcare research that process personal data. It is also necessary to review the measures established for data protection in the processes of public tendering in the healthcare and socio-sanitary system.

3.3. Concerning the infrastructures for data processing, including personal data in health research and innovation:

A) *Promote the creation of public European data management infrastructures*, so that personal data processing for the purposes of health research and innovation do not depend on American tech companies.

B) *Build a data management model* to allow access to them and their combination in conditions of security, reliability, traceability, quality and, especially, to allow for their interoperability and reuse.

C) *Create data governance structures for data processing* from the design stage, during, and after health research and innovation has ended.

3.4. Concerning digital literacy:

A) *Develop the legislation, and through the relevant actions, to achieve the digital literacy and education established in the Organic Law of Protection and Guarantee of Digital Rights* (art. 83). This should be a priority, in schools, but in particular, for the different operators who make decisions in the field of health research and innovation.

B) *Reinforce the intelligibility of data analysis and decision-making, avoiding so-called Black Box Artificial Intelligence*. The ultimate aim is to avoid asymmetries between the personal information amassed by third parties – from the data they have – and its owners' ability to control it.

---

[1] In relation to the applicable legislation on personal data protection in health research and innovation projects, see: Regulation (UE) 2016/679 of the European Parliament and the Council, of 27 April 2016, relative to the protection of individuals with regard to the processing of personal data and the free circulation of these data, repealing Directive 95/46/EC (General Data Protection Regulation) (Text relevant for the purposes of the EEE) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679 and Organic Law 3/2018, of 5 December, of Data Protection and Guarantee of Digital Rights https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[2] De LECUONA, I. "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (Big Data)" *Gaceta Sanitaria*, Vol. 32. No. 6, p. 576-578. 2018. DOI: 10.1016/j.gaceta.2018.02.007 https://www.gacetasanitaria.org/es-evaluacion-los-aspectos-metodologicos-eticos-articulo-S0213911118300864

[3] In this respect see the results of the OBD's previous research work: CASADO, M. (Coord.) *De la solidaridad al mercado: el cuerpo humano ante el comercio biotecnológico*, Editorial Fontamara, México, 2016. ISBN: 978-84-475-4193-5, and published by Edicions i Publicacions de la UB in 2017 in electronic format http://www.publicacions.ub.edu/ficha.aspx?cod=08646 y GARCÍA MANRIQUE, R. (Coord.), *El cuerpo diseminado. Estatuto, uso y disposición de los biomateriales humanos*, Editorial Aranzadi, Cizur Menor, 2018. ISBN: 978-84-9177-750-2, also available in electronic format.

[4] The Documents and Declarations of the OBD Opinion Group are available in open access, in pdf format, and in several languages at: http://www.bioeticayderecho.ub.edu/es/publicaciones

[5] An example in the context of the COVID-19 pandemic is *EU vs Virus Hackathon to develop innovative solutions and overcome coronavirus-related challenges (24-26 April 2020).* https://ec.europa.eu/info/news/euvsvirus-hackathon-develop-innovative-solutions-and-overcome-coronavirus-related-challenges-2020-apr-03_en

[6] European Digital Single Market: https://ec.europa.eu/digital-single-market/en/news/digitalyou-digital-trust

[7] European Union research programme HORIZONTE 2020: Health, demographic change and well-being https://ec.europa.eu/programmes/horizon2020/en/h2020-section/health-demographic-change-and-wellbeing

[8] On 20 February 2020 the European Union presented its "digital package" which includes the Data and Artificial Intelligence Strategy: https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data. Brussels, 19.2.2020 COM(2020) 66 final. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf and WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust Brussels, 19.2.2020 COM(2020) 65 final. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[9] The European Union's High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines on AI" https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. It refers to avoiding bias for reasons of race or gender, among others, and avoiding algorithmic discrimination.

[10] Personal data are any information relative to a living, identified or identifiable individual. The separate information, which complied could lead to the identification of a particular person, is also classed as personal data. Examples of personal data: name and surname, address, email address of the kind name.surname@company.com, national identity number, location data (such as a mobile telephone's data location function) (*), Internet Protocol (IP) address, a cookie identifier (*), the telephone's advertising identifier, the data in the possession of a hospital or doctor, which could be a symbol to uniquely identify a person. See European Union "What are Personal Data?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

The General Data Protection Regulation indicates, in article 9, as special categories of data: ethnic or racial origins, political opinions, religious or philosophical convictions, or trade union membership, and the processing of genetic data, biometric data addressed to unequivocally identifying an individual, data relative to health or data relative to an individual's sex life or sexual orientations.

[11] SWEENEY, L., "Simple Demographics Often Identify People Uniquely". Carnegie Mellon University, Data, Privacy Working Paper 3. Pittsburgh 2000. https://dataprivacylab.org/projects/identifiability/paper1.pdf

[12] LLÀCER, R.M., CASADO, M., BUISÁN, L. *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Ed. UB, Barcelona, 2015. Available at: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf

[13] See for example the Shared Electronic Medical Record in Catalonia: https://ticsalutsocial.cat/es/projectes/oficina-interoperabilidad/hc3/ and the Information System for Research in Primary Care (SIDIAP) https://www.sidiap.org/index.php/es

[14] SANTALÓ, J. y CASADO, M. (coords.), *Documento sobre bioética y edición genómica en humanos*, Ed. UB, 2016, Barcelona. ISBN 978-84-475-4073-0. Available at: http://hdl.handle.net/2445/105022

[15] "How should we think about clinical data ownership?", *Journal of Medical Ethics*, Ballantyne, Vol. 46, 2020, p. 289–294. https://jme.bmj.com/content/medethics/46/5/289.full.pdf

[16] The Spanish Royal Academy defines pseudonymization as the "processing of personal data in such a way that they can no longer be attributed to an individual without using additional information, provided that this additional information figures separately and is subject to technical and organizational measures aimed at guaranteeing that the personal data are not attributed to an identified or identifiable individual. And it refers specifically to article 4.5 of the General Data Protection Regulation.

[17] See for example the note of the Spanish Data Protection Agency on the need to assess the personal data processing of the COVID Radar App (June 2020) https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-sobre-la-participacion-de-la-aepd-en-la-app-de and *Manifiesto en favor de la transparencia en desarrollos de software públicos,* signed by over 230 academics and researchers (September 2020) https://transparenciagov2020.github.io/ (last consulted, 5 October 2020).

[18] EUROPEAN COMMISSION, *Guidance How to complete your ethics self-assessment. European Union*, February 2019. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

[19] See: General Data Protection Regulation article 5 Personal data shall be: (b) collected for specified, explicit and legitimate purposes and not processed subsequently in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall, in accordance with Article 89(1), not be considered incompatible with the initial purposes.

[20] See the *Guia d'avaluació dels aspectes derivats de la normativa de Protecció de Dades en projectes de recerca*, published by Direcció General de Recerca i Innovació en Salut, Direcció General d'Ordenació i Regulació Sanitària and Oficina del Delegat de Protecció de Dades- Fundació TIC SALUT SOCIAL, 31 July 2020.

[21] On these questions, see the contributions of the University of Barcelona's Bioethics Committee (CBUB), in particular, the forms according to the type of research to be conducted, and other requirements to be met in order to adapt to the law of data protection. http://www.ub.edu/comissiobioetica/es/formularios The CBUB was founded by Dr María Casado in 1996, as the first bioethics committee of a public university in our country. Later, in 2002 she also created the Spanish universities' Ethics Committees' Network and other public research bodies (RCEUC). The CBUB and the RCEUE have since 2012 been considered points of reference for good practices by universities that are members of the League of European Research Universities (LERU). See the report "Towards a Research Integrity Culture at Universities: From Recommendations to Implementation", LERU, January 2020. https://www.leru.org/files/Towards-a-Research-Integrity-Culture-at-Universities-full-paper.pdf

[22] See the *Gestiona* tool of the Spanish Data Protection Agency. *Gestiona* EIPD is an "assistant for data protection risk impact analysis and assessment. This free tool guides processing managers in aspects that must be taken into account, providing an initial basis for proper management." https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd. Also the practical Guide and the template for impact assessment relative to the data protection of the General Data Protection Regulation developed by the Catalan Data Protection Authority. https://apdcat.gencat.cat/ca/drets_i_obligacions/responsables/obligacions/avaluacio-impacte-relativa-proteccio-dades/ The OBD, in collaboration with the interdisciplinary team, is developing a specific methodology for conducting impact assessment relative to personal data processing in the field of health and innovation as proposed by the Fundació TICSalut, Oficina del Delegat de Protecció de Dades.

[23] EUROPEAN COMMISSION, H2020 Programme Guidelines on FAIR Data Management in Horizon 2020 26 July 2016; https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf and CSUC, Research Data Management, https://www.csuc.cat/es/consorciacion-tic/gestion-de-datos-de-investigacion

[24] LERU, *Open Science and its role in universities: a roadmap for cultural change*, May 2018 and EUROPEAN COMMISSION, https://ec.europa.eu/digital-single-market/en/open-science

[25] See EUROPEAN DATA PROTECTION SUPERVISOR, Flowcharts and Checklists on Data Protection , 2020 https://edps.europa.eu/sites/edp/files/publication/flowcharts_and_checklists_on_data_protection_brochure_en_1.pdf

Pautas para evaluar proyectos de investigación e innovación en salud que utilicen tecnologías emergentes y datos personales

PLANTEAMIENTO

La evaluación de los aspectos metodológicos, éticos, legales y sociales de los proyectos de investigación en salud corresponde a los comités de ética de la investigación (CEI). En nuestro contexto, la aprobación de proyectos en los que participan personas, se utilizan datos personales y/o muestras biológicas de origen humano depende de estos órganos colegiados interdisciplinares y establecidos por ley. Su dictamen favorable es obligatorio para que puedan llevarse a cabo las intervenciones propuestas, tanto en centros públicos como privados de investigación. En Europa conviven distintas fórmulas: los CEI pueden ser de carácter nacional y regional, pero también cabe la posibilidad de que cada centro de investigación cuente con su propio CEI o se adscriba a uno ya creado. Todos ellos deben estar acreditados por el organismo correspondiente, previo cumplimiento de una serie de requisitos y condiciones.

Inicialmente los CEI se crearon para evaluar ensayos clínicos con medicamentos y productos sanitarios, para luego valorar otros tipos de investigaciones que, por sus características, también plantean la necesidad de encontrar un equilibrio entre el avance del conocimiento científico, el interés investigador y la protección de las personas participantes. Ejemplos de esto último son los proyectos que aplican tecnologías emergentes como la inteligencia artificial, el *Big Data*, la biometría y la realidad virtual, entre otras, así como el desarrollo de dispositivos y aplicaciones de salud (*Apps*). Recientemente, además, se solicita a los CEI que evalúen proyectos puramente de innovación en el ámbito de la salud.

En estos procesos de creación y transferencia de conocimiento, los intereses de la ciencia, de la tecnología y de la sociedad no deben prevalecer sobre los del individuo. Para ello, los CEI deben analizar la validez científica de las propuestas, su valor social y ponderar los derechos e intereses en juego. La investigación es una actividad que siempre conlleva ciertos riesgos para los participantes —como el riesgo de la quiebra de la confidencialidad en los proyectos que traten datos personales—. Y esos riesgos se deben sopesar con los beneficios, de los que en muchas ocasiones el participante no se aprovecha personal o directamente.

Los cambios científicos y tecnológicos son vertiginosos, en una sociedad de mercado exacerbada donde la salud es objeto de una creciente mercantilización; y en la que se monetizan los datos personales. Si bien es cierto que los ritmos de producción normativa y de los procesos de creación y aplicación del conocimiento no son los mismos, se produce cierta parálisis en la aplicación de las normas, fundamentalmente debida a la falta de comprensión del fenómeno digital al que nos enfrentamos. Por ello, se considera que los CEI pueden y deben actuar como garantía de que la investigación y la innovación aparejada cumplen con los principios éticos y con los requisitos legales establecidos[1].

La sociedad digital, guiada por el dato y basada, por lo tanto, en la explotación intensiva de conjuntos de datos, incluidos los datos personales, ha puesto de manifiesto que el modelo evaluador vigente -y propio de la segunda mitad del siglo XX- para analizar proyectos de investigación en los que participen humanos y/o se utilicen sus datos personales está

obsoleto y es ineficaz, precisamente por los retos que técnica, ética, legal y socialmente plantean los tratamientos de datos personales en el siglo XXI.

En la actualidad, los CEI deben proteger a las personas a través de la salvaguarda de sus datos personales y asegurar la intimidad y la confidencialidad de sus titulares. Además, deben promover y garantizar el ejercicio de la autonomía para tomar decisiones de manera libre e informada, evitar la discriminación (específicamente cuando es encubierta), así como garantizar la equidad y la transparencia. El equilibro que los CEI deben alcanzar entre maximizar los beneficios y minimizar los riesgos incluye también tratar adecuadamente los datos personales. En resumen, como los procesos de recolección y tratamiento de datos constituyen el nicho donde desarrollar la investigación e innovación, resulta prioritario que los CEI tomen conciencia de la relevancia del nuevo paradigma digital asentado en la explotación intensiva de datos personales, incluidos los datos de salud[2].

La pandemia por COVID-19 ha puesto a prueba la capacidad de los CEI para analizar adecuadamente los citados proyectos y priorizar aquellos que beneficien el interés colectivo y la salud pública. Actualmente, los CEI trabajan bajo presión y se les exige una rápida evaluación de los numerosos proyectos de investigación e innovación que se presentan: ensayos clínicos para el desarrollo de vacunas y de medicamentos y otros tipos de investigaciones; pero, también hay muchos otros proyectos que deben ser evaluados y que no requieren ninguna intervención directa sobre las personas, pero que implican el acceso y el tratamiento de conjuntos de datos personales, entre los que destacan los datos de salud. En particular, proyectos para el desarrollo de sistemas de predicción y gestión de la COVID-19 que agudizan los problemas a los que ya venían enfrentándose los CEI en los últimos años. No son por lo tanto cuestiones totalmente nuevas, pero sí es cierto que se han intensificado por razón de la excepcional situación que estamos viviendo en la que se hacen patentes las graves carencias de nuestro modelo evaluador.

Ante esta situación, el Grupo de Opinión del Observatorio de Bioética y Derecho- Cátedra UNESCO de Bioética de la Universidad de Barcelona (OBD), centro de investigación interdisciplinar de la Universidad de Barcelona, ha analizado los retos, las cuestiones no resueltas y los problemas que se suscitan en los proyectos de investigación y la innovación en salud. El objetivo es aportar pautas que contribuyan a homogeneizar las cuestiones que los CEI deben analizar y evaluar, así como la información que solicitar a los responsables de los proyectos, para impedir que los oportunistas abran mercados de datos personales disfrazados de investigación e innovación y, en particular, con el pretexto de la pandemia. Y también para evitar que la intimidad de los participantes en esos proyectos se vea expuesta públicamente sin su consentimiento[3].

La adecuada evaluación de los tratamientos de los datos personales en proyectos de investigación e innovación en salud debe ser una prioridad para los CEI, en tanto que mecanismos de protección de las personas. El principal escollo es que no están consiguiendo adaptarse al paradigma digital, y al cambio que supone asentar los procesos de investigación e innovación en salud en la explotación intensiva de conjuntos de datos personales, lo que genera importantes disfunciones. La experiencia de miembros del OBD como vocales de distintos comités de ética (CEI, comités de bioética nacionales y autonómicos, asistenciales y *ad hoc*), que se refleja en este trabajo, permite aportar una perspectiva práctica junto al análisis del marco teórico.

En esta ocasión la autora de este trabajo es la Dra. Itziar de Lecuona, doctora en derecho, profesora agregada del Departamento de Medicina de la Facultad de Medicina y Ciencias de la Salud de la Universidad de Barcelona y subdirectora del OBD; que ha coordinado el Grupo de Opinión y ha recibido las aportaciones de los académicos, investigadores y profesionales que se relacionan al final del Documento.

Desde 1996, el OBD analiza científica e interdisciplinarmente las implicaciones éticas, jurídicas y sociales de la biomedicina y la biotecnología, e incide en el diálogo entre la universidad y la sociedad mediante la transmisión del conocimiento científico-técnico y los argumentos necesarios para participar en un debate social verdaderamente informado. Con este fin, el Grupo de Opinión ha elaborado ya 31 documentos y declaraciones[4] concernientes a temas de actualidad, sobre los que no existe una opinión unánime, ni en la sociedad ni en las diversas comunidades científicas implicadas; ello ha requerido identificar los problemas, contrastar los argumentos y proponer recomendaciones.

El análisis y las recomendaciones que el Grupo efectúa están principalmente destinados a los miembros de los CEI implicados en la evaluación de los citados proyectos de investigación e innovación en salud, para que sea posible la protección de la intimidad de los titulares de los datos, y orientar su tratamiento de tal forma que se eviten explotaciones innecesarias, así como la comercialización de conjuntos de datos personales. La investigación debe responder a las necesidades sociales y no a intereses espurios. El trabajo también tiene como destinatarios al ecosistema de investigación e innovación, con una llamada al poder político y legislativo para que tome en consideración las recomendaciones.

ESTADO DE LA CUESTIÓN

En los centros hospitalarios y de investigación la COVID-19 ha provocado un aluvión de propuestas en investigación y en innovación para su detección temprana y gestión. Estas se basan en la aplicación de inteligencia artificial y tecnologías emergentes como el Big Data y la biometría y pueden conllevar el desarrollo de dispositivos de salud, aplicaciones (*Apps*) incluidas. Ejemplos de estos proyectos son el desarrollo de sistemas de predicción de la COVID-19, basados en la programación de algoritmos, que se nutren de distintos conjuntos datos personales almacenados en historias clínicas y en otras bases de datos, así como de aquella información remitida por los titulares de los datos en distintos formatos. Así proliferan las *Hackatones*[5] o retos para, por ejemplo, desarrollar algoritmos como parte de proyectos en medicina para predecir el riesgo de desarrollar determinadas complicaciones. El objetivo es aumentar el conocimiento disponible, desarrollar intervenciones personalizadas y mejorar la toma de decisiones. En suma, se plantean propuestas que pueden estar fundamentadas en protocolos de investigación, y otras, para innovar en el ámbito asistencial, que comparten el reto de asegurar que protegen la intimidad de los titulares de los datos personales que necesitan tratar. Estas iniciativas deberían tener un claro beneficio social.

Desde principios de los 2000, Europa apuesta por una sociedad guiada por el dato. Es una decisión política y económica, que también incluye los procesos de creación y de transferencia de conocimiento. El objetivo es un mercado digital único y competitivo, capaz de garantizar la protección de los derechos y libertades de las personas, a la vez que promueve la investigación e innovación fundamentada en la explotación intensiva de conjuntos de datos, incluidos los

datos personales[6]. En el ámbito de la salud esta apuesta se traduce en una medicina más personalizada, sistemas sanitarios más eficientes, predicción de los efectos adversos de los medicamentos con un número menor de personas expuestas al riesgo, envejecimiento activo y bienestar; y sistemas de predicción y gestión de pandemias, como es el caso de la COVID-19, entre otras prioridades. Todos estos ámbitos en los que se financian numerosos y cuantiosos consorcios de investigación e innovación público-privada que recurren a las citadas tecnologías y para el desarrollo de dispositivos de salud[7], tienen como sustrato la explotación de conjuntos de datos, entre ellos los datos personales, y para los que es necesaria la participación de terceros tradicionalmente ajenos al ámbito biomédico y de salud. Estos terceros, que pueden ser tanto empresas privadas como incluso administraciones públicas, tienen interés en acceder a distintos conjuntos de datos personales, por lo que éstos pueden decir de sus titulares y por lo que pueden predecir. Interés que puede ser distinto e incluso contrario al de los investigadores responsables de los proyectos.

En pocos años hemos transitado velozmente del entusiasmo por el *Big Data* a la devoción por la inteligencia artificial, la realidad virtual y el internet de las cosas. Justo antes de la pandemia, Europa presentó su Estrategia Digital y de Inteligencia Artificial[8] que desde la perspectiva ética debe ser "confiable"[9], capaz de evitar los sesgos por razón de sexo o raza y centrada en el humano. A pesar de esta loable decisión política, es necesario recordar la falta de infraestructuras públicas en Europa que permitan almacenar, usar y compartir datos, su interoperabilidad y reutilización. Esta situación evidencia la excesiva dependencia europea de las grandes tecnológicas, fundamentalmente estadounidenses, conocidas como imperio GAFAM por sus siglas en inglés (Google, Apple, Facebook, Amazon y Microsoft).

Así, los datos personales son el oro de nuestro tiempo y, entre ellos, los datos de salud, los datos biométricos, sociodemográficos, entre otros, son considerados por la legislación como categorías especiales de datos[10] que requieren la más alta protección porque lo dicen todo sobre nosotros; porque podrían ser utilizados con fines no deseados, y dar lugar a discriminaciones encubiertas, con profundas implicaciones para la libertad de las personas y de las generaciones futuras. La posesión de conjuntos de datos personales por parte de terceros bien sea la iniciativa pública o privada, puede afectar a nuestros derechos en función de los usos, confiriéndoles a estos terceros un extraordinario poder sobre nosotros, situación que pasa inadvertida para la gran mayoría de las personas. Las decisiones que se tomen en el ámbito de la investigación e innovación en salud y en contextos altamente digitalizados marcarán los proyectos vitales de personas, colectivos y sociedades.

En la sociedad digital hemos dejado de ser anónimos para ser reidentificables. El sexo, el código postal y la fecha de nacimiento nos identifican con un porcentaje de fiabilidad muy elevado[11]. El Grupo de Opinión del OBD ya alertó sobre estas cuestiones en 2015, en el "Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública"[12]. Debido al desarrollo de la tecnología y a la ingente cantidad de información de carácter personal acumulada en distintas bases de datos y a la información que liberamos, es posible realizar patrones de comportamiento, predecir conductas y, por lo tanto, mejorar la toma de decisiones. Para ello es necesario programar algoritmos que se nutren de conjuntos de datos incluidos los datos personales. Estos datos personales, como principal materia prima, son propiedad de sus titulares, que serán a su vez destinatarios finales de los resultados de los procesos de investigación e innovación con la especial situación de los datos de salud. Como es sabido, la historia clínica digitalizada[13], convenientemente estructurada y siguiendo criterios de calidad y seguridad, contiene datos

personales de salud, sociodemográficos, y diversos datos personales que son de interés por lo que estos dicen de las personas ahora y por lo que pueden predecir.

La investigación y la innovación en salud se produce en un contexto altamente competitivo, de ultraliberalismo globalizado y de dominio del mercado[14], en el que se coaligan ejes diferenciados, como los de investigación, innovación, aplicación del conocimiento y empresa. En este contexto, se abre el debate sobre la titularidad de los datos personales, sobre el altruismo de datos[15] cuando nuestro sistema de investigación y de innovación en salud tradicionalmente se ha basado en la solidaridad, teniendo siempre la opción de no participar en estos procesos de donación de forma libre y voluntaria y sin que ello tenga consecuencias negativas. Este modelo altruista y solidario, y que conlleva cierta cesión de información personal, debe revertir en tratamientos e intervenciones para el titular de los datos o para los pacientes y las generaciones futuras. También puede implicar el aumento de conocimiento sin un beneficio directo. Esta cesión no puede suponer que determinados conjuntos de datos personales estén al alcance de cualquiera, en particular los datos de salud. Conviene recordar aquí que el acceso a datos personales con fines asistenciales y de investigación lleva aparejado el deber de secreto del profesional sanitario para mantener la confidencialidad de la información.

Ante el cambio que implica la explotación intensiva de datos personales y la elevada probabilidad de reidentificación, el quid de la cuestión radica en qué datos personales se van a solicitar, cómo se van a obtener y almacenar y de qué forma se van a tratar -si codificados o seudonimizados[16]-, quién va a tener acceso, durante cuánto tiempo y qué va a ocurrir con los datos una vez finalizada la intervención. Asimismo, el interés se centra en cómo se van a combinar los conjuntos de datos, por ejemplo, aquellos almacenados en historias clínicas digitalizadas en bases de datos altamente protegidas con otros datos personales provenientes de otras bases de datos externas al sistema de salud, que pueden referirse al patrón de comportamiento de sus titulares mediante el análisis de la base de datos de telefonía móvil u otros, como encuestas de salud.

Para la gestión de la COVID-19 hemos asistido al desarrollo de aplicaciones que invitaban a aportar datos personales como la tarjeta sanitaria y la geolocalización para iniciar una encuesta sobre los síntomas y poder predecir si la persona es sospechosa de ser positiva, y como soporte en el ámbito de la salud pública. Luego, se ha iniciado un debate tardío y nada transparente sobre la seguridad técnica y la protección de la intimidad sobre las *Apps* de identificación de positivos y rastreo de contactos[17]. Esta información de carácter personal, debidamente obtenida y almacenada debería poder combinarse con otros datos de salud, como se ha expuesto, para que sea útil para la toma de decisiones en beneficio de las personas y del interés público. Estos ejemplos de procesos de investigación e innovación deben contar con la aprobación de los correspondientes CEI.

DECLARACIÓN

Para orientar la toma de decisiones en investigación e innovación en salud, ante la explotación intensiva de datos personales, conviene efectuar las siguientes consideraciones para una adecuada protección de las personas:

- Que ya no es posible garantizar el anonimato. Hemos dejado de ser datos aislados para convertirnos en conjuntos de datos, almacenados en distintas bases de datos

que se pueden combinar con el objetivo de extraer conclusiones para mejorar la toma de decisiones; por lo que hemos pasado de ser anónimos a ser reidentificables.

- Que los protocolos de obtención del consentimiento informado de los participantes han quedado claramente desfasados debido a que se presuponía no solo que los datos eran anónimos, sino que siempre lo seguirían siendo en el futuro.
- Que la pandemia por COVID-19 ha permitido constatar aquello que era evidente: los graves problemas para acceder e interpretar los datos que son tan necesarios para avanzar en la toma de decisiones políticas basadas en la evidencia científica.
- Que los datos almacenados no están conectados entre sí, no están adecuadamente seudonimizados, ni tampoco hay infraestructuras públicas para ello, lo que supone una barrera para el conocimiento científico, así como para los distintos actores del sistema de investigación, innovación y desarrollo.
- Que la dependencia por parte de los Estados y de Europa de las grandes tecnológicas, fundamentalmente estadounidenses, es excesiva y debe ser revertida con urgencia.
- Que el proceso de combinación de conjuntos de datos personales mediante el recurso a las tecnologías emergentes y al desarrollo de algoritmos debe producir un beneficio sobre las personas y no exponerlas a discriminaciones manifiestas o encubiertas ni a usos no deseados.
- Que el soporte que implica la tecnología no puede conducir a prácticas de vigilancia digital de las personas
- Que ni los gobiernos ni las grandes corporaciones tecnológicas deben tener un control absoluto sobre los datos personales y que la gestión de éstos debe someterse a criterios de transparencia y rendición de cuentas para evitar la opacidad que impera en los entornos digitales.
- Que existe una tendencia a la mercantilización de los datos personales también en el ámbito de la salud, y en particular, a propósito de la pandemia por COVID-19.
- Que las decisiones deben estar fundamentadas en la evidencia científica y no en propuestas proclives a mercados de datos personales disfrazados de investigación e innovación en salud.
- Que una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por la referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o más factores específicos del ámbito físico, fisiológico, genético, mental, económico, identidad cultural o social de esa persona física.
- Que son datos personales: el nombre, la dirección, el número de identificación, el seudónimo, la ocupación, el correo electrónico, el CV, los datos de ubicación, la dirección de Protocolo de Internet (IP), el identificador de cookie, el número de teléfono, los datos proporcionados por medidores inteligentes, datos en poder de un hospital o de centros de investigación[18].
- Que son categorías especiales de datos personales aquellos datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas,

o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

- Que junto a la legislación vigente son de aplicación los deberes éticos y deontológicos sobre protección de la intimidad y la confidencialidad de los datos personales en entornos altamente digitalizados para los profesionales sanitarios, pero también para los distintos profesionales que colaboran.
- Que los CEI carecen de la composición adecuada y de las capacidades necesarias para evaluar los proyectos de investigación e innovación que aquí se plantean. Por ello, es urgente lograr su educación digital, por la responsabilidad que ejercen estos órganos colegiados en cuanto a la protección de los derechos de los implicados en los procesos de investigación e innovación, incluyendo la libertad e investigación, junto a otros derechos fundamentales como la intimidad y la confidencialidad de los datos personales.
- Que los CEI deben identificar los potenciales problemas y los conflictos de interés que puedan surgir en relación con el uso de datos personales, así como qué información solicitar a los responsables de los proyectos, para garantizar la protección de los derechos de las personas.
- Que la investigación y la innovación deben estar justificadas por su validez científica y su valor social, y que los derechos de las personas se pueden restringir de manera proporcionada y justificada por razones de salud pública e interés colectivo, pero nunca llegar a anularse. En ningún caso, y menos en tiempos de pandemia, se pueden relajar los estándares de protección.

RECOMENDACIONES

1. A los comités de ética de la investigación:

1.1. Sobre los proyectos de investigación e innovación en salud que utilizan tecnologías emergentes y datos personales:

A) Comprobar y evaluar el cumplimiento de los principios de protección de datos.

El tratamiento de datos personales deben basarse en los siguientes principios: "licitud, lealtad y transparencia" en relación al interesado; "limitación de la finalidad" que se refiere a que los datos deber ser recogidos con fines determinados, explícitos y legítimos[19]; "minimización de datos", que significa que los datos deben ser adecuados, pertinentes y limitados a aquello que es necesario en relación a las finalidades para las que se tratan; "exactitud", entendiendo que los datos serán exactos y, si fuera necesario, actualizados, y que se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan; "limitación del plazo de conservación" e "integridad y confidencialidad", que se refiere a que los datos sean tratados de forma segura. Asimismo, el responsable del tratamiento será el responsable del cumplimiento de estos principios y será capaz de demostrarlo (responsabilidad proactiva). El responsable del tratamiento tiene la obligación de la protección de datos "desde el diseño" y "por defecto" para determinar las medidas técnicas y organizativas necesarias para asegurar el cumplimiento de los principios señalados[20].

Para dar cumplimiento a los citados principios, los CEI deben comprobar y evaluar:

a) Si la información y el proceso de consentimiento informado de los potenciales participantes en los proyectos cumple con los requisitos establecidos por la normativa vigente;

b) Si los datos personales se van a codificar, seudonimizar o anonimizar;

c) El formato en el que se van a almacenar los datos personales;

d) Si los datos personales se van a enviar dentro y/o fuera de la Unión Europea, con las correspondientes garantías y si se van a compartir con terceros; y

e) Si hay servicios de nube y en qué condiciones.

B) Asegurar la no identificación de las personas participantes, lo que requerirá incorporar como miembros o asesores a expertos, especialmente, en técnicas de seudonimización.

Evitar el recurso al concepto de "anonimización" con carácter general, pues genera una falsa sensación de seguridad. Las palabras importan y los CEI no deben pasar por alto esta cuestión y deben incluir en los modelos de presentación de proyectos o en las indicaciones correspondientes los tipos de tratamientos posibles y, así, las diferencias entre datos anonimizados, codificados y seudonimizados. En este sentido, un error común detectado en las memorias, los protocolos y en las hojas de información y consentimiento informado de los proyectos, es indicar que los datos se anonimizarán cuando del análisis de los tratamientos de datos se constata que estos se seudonimizarán.

Los CEI deben comprobar las técnicas previstas para asegurar la no atribución de personalidad a los conjuntos de datos que se tratan, es decir, la no identificación del titular de los datos. Estas cuestiones, eminentemente técnicas, requieren contar con expertos o asesores en el CEI que, de forma independiente, puedan evaluar y comprobar que las propuestas son adecuadas.

*C) En el caso de que no se disponga de un sistema de protección específico y propio de la institución, se deben acordar contractualmente las condiciones que garanticen la protección de los datos personales***.**

Un ejemplo recurrente y de mala práctica es el recurso a servicios digitales gratuitos para efectuar encuestas en red para el tratamiento de datos personales que no protegen la privacidad, a no ser que se contraten servicios específicos para ello. Esta situación plantea cuestiones éticas y legales, puesto que liberar datos personales en plataformas que por defecto monetizan datos personales en entornos no protegidos por parte de terceros, es también una violación de la integridad científica[21]. Si las instituciones participantes en estos proyectos no cuentan con servicios específicos y que protejan la intimidad, el responsable del tratamiento debe asegurar tal protección y realizar los correspondientes acuerdos contractuales con terceros, presentando ante el CEI las evidencias que sean necesarias.

D) Exigir y examinar la "evaluación del impacto de las operaciones de tratamiento en la protección de datos personales" (EIPD) en los supuestos en los que así lo exige el Reglamento General de Protección de Datos.

Se trata de una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, que debe efectuar el responsable del tratamiento con carácter previo al inicio del mismo. En determinados supuestos, como en el caso de uso de nuevas tecnologías; tratamientos de categorías especiales de datos (datos salud, genéticos y biométricos); tratamientos que impliquen la elaboración de perfiles de personas; y/o toma

de decisiones automatizada, entre otros, los CEI deben comprobar que el proyecto ha sido sometido a la citada EIPD. Esta puede hacerse siguiendo unas metodologías que permiten identificar los riesgos asociados a los tratamientos[22]. De la EIPD derivará un plan de acción que deberá llevarse a cabo para mitigar riesgos detectados y que tendrá que revisarse periódicamente y actualizarse ante posibles cambios en los tratamientos de los datos. Esta evaluación no puede concebirse como un mero trámite, sino como un proceso vivo que puede ser objeto de modificaciones y que permite hacer un adecuado seguimiento del proyecto y de las garantías a aplicar para la protección de los datos personales. El Delegado de Protección de Datos, es la figura independiente que asesora en estos procesos.

E) Solicitar y evaluar el Plan de Gestión de Datos.

Los CEI deben solicitar al investigador principal el Plan de Gestión de Datos, que describe cómo se obtienen, se procesan y en su caso, se generan nuevos datos en el marco del proyecto; y qué ocurrirá con éstos una vez acabado el proyecto[23]. Asimismo, el Plan incluye fórmulas para que los datos se puedan encontrar, sean accesibles, interoperables y reutilizables. La "ciencia abierta", en el marco de la sociedad digital, obliga a los CEI a comprobar qué metodologías y estándares se van a aplicar y si los datos se van a compartir en acceso abierto[24]. Conviene hacer hincapié en que el Plan de Gestión de Datos se inserta en el análisis de riesgos y la adopción de medidas de seguridad que exige el Reglamento General de Protección de Datos en todos los casos, se haga o no una evaluación de impacto relativa a la protección de datos.

F) Comprobar que los potenciales participantes de los proyectos de investigación e innovación en salud son informados sobre sus derechos y las condiciones para su ejercicio.

Derecho a ser informado; de acceso; de rectificación; al olvido; a restringir el procesamiento de los datos; a la portabilidad de los datos y a no ser objeto de una decisión automatizada que debe incorporar la intervención y corrección humana y que incluye la elaboración de perfiles. Asimismo, se debe informar sobre el derecho a la revocación que implica asegurar que se elimina de la base de datos correspondiente la información de la persona que así lo solicita.

G) Comprobar que los protocolos y las hojas de información y de consentimiento informado indiquen explícita y detalladamente quién es el responsable del tratamiento y del procesamiento de los datos personales.

Los CEI deben actuar de forma coordinada con los servicios legales de la institución correspondiente para revisar los acuerdos de encargado de tratamiento y transferencia de datos y, cuando proceda, los acuerdos de corresponsabilidad sobre los tratamientos[25].

Es necesario que los CEI establezcan un canal de comunicación fluido con los responsables de las áreas de tecnologías de la información y la comunicación de las instituciones correspondientes.

H) Solicitar que la política de privacidad y el aviso legal se incluyan en la memoria del proyecto.

Los CEI deben solicitar que la política de privacidad y el aviso legal se incluyan en la memoria del proyecto para evaluar el cumplimiento de los derechos y obligaciones sobre protección de datos por parte del investigador y del responsable del tratamiento.

Los CEI deben comprobar que la información no induce a error, ni genera falsas expectativas. Es necesario además determinar los usos que se pueden hacer de la "marca institucional", que servirá como principal aval de los resultados que se presenten.

1.2. A los comités de ética de la investigación sobre su composición y funciones:

A) Integrar perfiles expertos en tecnologías emergentes.

Es urgente que los CEI integren perfiles de forma permanente o como asesores a expertos en inteligencia artificial, ciencia de los datos y, en particular, en técnicas de seudonimización así como en el desarrollo de dispositivos digitales de salud entre los que se incluyen las *Apps*, los *Wearables* y el internet de las cosas. Cada tecnología debería contar con un experto en la materia para evaluar y participar en las deliberaciones previas a la emisión de dictamen.

B) Contribuir a generar una cultura de respeto por la intimidad de las personas a través de la protección de los datos personales.

Se reivindica aquí la función de sensibilización sobre cuestiones bioéticas de los comités de ética que propugna la Declaración Universal sobre Bioética y Derechos Humanos de la UNESCO de 2005 (art. 19 d).

2. A los centros de investigación e innovación:

A) Destinar el presupuesto suficiente para dotar a los CEI de recursos humanos y materiales para una adecuada evaluación y que permita el seguimiento de los proyectos de investigación e innovación en salud.

La investigación es el pilar de nuestro sistema de salud y si bien la evaluación con carácter previo es condición *sine qua non* para que esta se pueda desarrollar, también es necesario efectuar el seguimiento de los proyectos durante su ejecución y hasta su la finalización, incluida la publicación de resultados y la gestión de los datos.

B) Asegurar la independencia de los CEI para tomar decisiones.

Los CEI no responden a intereses institucionales o espurios, tampoco a los intereses particulares de investigadores, promotores u otros terceros implicados en los procesos de investigación e innovación. Para asegurar su independencia es necesario establecer reglas y procedimientos para la detección, declaración y correspondiente gestión de los conflictos de intereses que no sólo pueden ser de naturaleza económica, sino que también pueden darse por razón de parentesco, amistad, o jerarquía.

C) Garantizar la independencia del Delegado de Protección de Datos.

La figura del Delegado de Protección de Datos establecida en el Reglamento General de Protección de Datos y en la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, ha sido incorporada en algunos casos, sin respetar el espíritu independiente, favoreciendo los conflictos de intereses y la falta de transparencia. Tal como establece el Reglamento, el Delegado de Protección de Datos, puede formar parte de la plantilla del responsable o del encargado del tratamiento o bien actuar en el marco de un contrato de servicios. Además, los CEI en el ámbito de la salud, biomédico o del medicamento,

deben integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales (Ley Orgánica de Protección de Datos y garantía de los derechos digitales, Disposición adicional decimoséptima).

3. Al legislador:

3.1. Sobre la naturaleza y regulación de los comités de ética de la investigación:

A) *Desarrollar reglamentariamente las competencias, funciones, constitución, acreditación, composición y funcionamiento de los comités de los CEI.*

Los CEI necesitan un desarrollo normativo con carácter urgente sobre las competencias, funciones, constitución, acreditación, composición y funcionamiento, que está pendiente desde la promulgación de la Ley de Investigación Biomédica (2007).

B) *Crear comités de ética de la innovación.*

Mientras no se priorice cubrir esta necesidad, los CEI seguirán al límite. A la falta de recursos humanos y materiales, se le suma una sobrecarga evidente: seguirán evaluando proyectos de investigación al uso y, además, las iniciativas provenientes de las áreas de innovación de hospitales y centros de investigación que utilizan tecnologías emergentes y datos personales, sin la comprensión ni las pautas adecuadas para evaluar los tratamientos de datos personales. El aval ético de los citados proyectos viene determinado por el dictamen favorable de los CEI de instituciones de reconocido prestigio.

Crear comités específicos para este tipo de estudios, de un modo relativamente centralizado, o habilitar estas funciones a unos pocos comités ya existentes que puedan asumir esa carga de trabajo. La condición sería que en su composición formara parte un miembro del CEI y viceversa para compartir información.

C) *Incorporar de forma real y cuantificable la Investigación e Innovación Responsable (RRI por sus siglas en inglés) que Europa propugna mediante el desarrollo de directrices comunes para que los CEI puedan evaluar las agendas que la componen: la ética, la igualdad de género, la educación científica y el acceso abierto.*

Y especialmente, *el public engagement* para, a partir de la cooperación entre los distintos actores implicados, sea posible alinear mejor el proceso de investigación y sus resultados con los valores, las necesidades y las expectativas de la sociedad actual. El objetivo es reducir la brecha que existe entre la comunidad científica y la sociedad, incentivando que distintos grupos de interés trabajen juntos en todo el proceso de investigación e innovación.

3.2 Sobre la regulación de los usos de datos personales en investigación e innovación en salud:

A) *Desarrollar la disposición adicional decimoséptima sobre los tratamientos de datos de salud de la Ley Orgánica de Protección de Datos y garantía de los derechos digitales* que es insuficiente para tratar los usos de investigación. Se aconseja un desarrollo normativo que permita hacer frente de forma adecuada a los retos actuales en el ámbito de la investigación y la innovación.

B) Regular el ámbito de la telemedicina, la teleasistencia y los dispositivos digitales y aplicaciones de salud, Apps incluidas en los procesos de investigación y asistenciales que traten datos personales. También se hace necesario revisar las medidas establecidas para la protección de datos en los procesos de contratación pública en el ámbito hospitalario y sociosanitario.

3.3. Sobre las infraestructuras para el tratamiento de datos, incluidos los datos personales en investigación e innovación en salud:

A) Potenciar la creación de infraestructuras europeas para la gestión de datos financiadas con fondos públicos, para que los tratamientos de datos personales con fines de investigación e innovación en salud no dependan de las grandes empresas tecnológicas, fundamentalmente estadounidenses.

B) Construir un modelo de gestión de los datos que permita su acceso y su combinación en condiciones de seguridad, fiabilidad, trazabilidad, calidad y, especialmente, que permita su interoperabilidad y reutilización.

C) Crear estructuras de gobernanza de los datos personales que permitan un seguimiento desde el diseño, durante y una vez finalizada la investigación y la innovación en salud.

3.4. Sobre la educación digital:

A) Desarrollar reglamentariamente y mediante las acciones que correspondan para lograr la alfabetización y la educación digital establecida en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales (art. 83). Esta debería ser una prioridad, y desde la escuela, pero en particular, para los distintos operadores que toman decisiones en el ámbito de la investigación e innovación en salud.

B) Potenciar la inteligibilidad del análisis de los datos y de la toma de decisiones, evitando la denominada caja negra de la inteligencia artificial. El objetivo final es evitar asimetrías entre la información personal que acumulan terceros -por los datos de que disponen-, y la capacidad de control de sus titulares.

---

[1] En relación a la normativa aplicable sobre protección de datos personales en proyectos de investigación e innovación en salud véase: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679 y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[2] De LECUONA, I. "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (Big Data)" *Gaceta Sanitaria*, Vol. 32. Núm. 6, p. 576-578. 2018. DOI: 10.1016/j.gaceta.2018.02.007 https://www.gacetasanitaria.org/es-evaluacion-los-aspectos-metodologicos-eticos-articulo-S0213911118300864

[3] En este sentido véanse los resultados de trabajos de investigación previos del OBD CASADO, M. (Coord.) *De la solidaridad al mercado: el cuerpo humano ante el comercio biotecnológico*, Editorial Fontamara, México, 2016. ISBN: 978-84-475-4193-5 y editado por Edicions i Publicacions de la UB en 2017 en formato electrónico http://www.publicacions.ub.edu/ficha.aspx?cod=08646 y GARCÍA MANRIQUE, R. (Coord.), *El cuerpo*

diseminado. Estatuto, uso y disposición de los biomateriales humanos ,Editorial Aranzadi, Cizur Menor, 2018. ISBN: 978-84-9177-750-2, disponible también en formato electrónico.

[4] Los Documentos y Declaraciones del Grupo de Opinión del OBD están disponibles en acceso abierto, en formato pdf y en varios idiomas en: http://www.bioeticayderecho.ub.edu/es/publicaciones

[5] Un ejemplo en el contexto de la pandemia por COVID-19 es *EUvsVirus Hackathon to develop innovative solutions and overcome coronavirus-related challenges (24-26 de abril de 2020).* https://ec.europa.eu/info/news/euvsvirus-hackathon-develop-innovative-solutions-and-overcome-coronavirus-related-challenges-2020-apr-03_en

[6] Mercado único digital europeo: https://ec.europa.eu/digital-single-market/en/news/digitalyou-digital-trust

[7] Programa de investigación de la Unión Europea HORIZONTE 2020: Salud, cambio demográfico y bienestar https://ec.europa.eu/programmes/horizon2020/en/h2020-section/health-demographic-change-and-wellbeing

[8] El 20 de febrero de 2020 la Unión Europea presentó su "paquete digital" que incluye la estrategia de Datos e Inteligencia Artificial: https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data. Bruselas, 19.2.2020 COM(2020) 66 final. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf y WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust Bruselas, 19.2.2020 COM(2020) 65 final. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[9] Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial de la Unión Europea, "Guías éticas sobre inteligencia artificial" https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. Se refiere a evitar los sesgos por razón de raza o de género entre otros y a evitar la discriminación algorítmica.

[10] Los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal. Ejemplos de datos personales: nombre y apellidos, domicilio, dirección de correo electrónico, del tipo nombre.apellido@empresa.com, número de documento nacional de identidad, datos de localización (como la función de los datos de localización de un teléfono móvil) (*), dirección de protocolo de internet (IP), el identificador de una cookie (*), el identificador de la publicidad del teléfono, los datos en poder de un hospital o médico, que podrían ser un símbolo que identificara de forma única a una persona. Véase Unión Europea ¿Qué son los datos personales" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es El Reglamento general de protección de datos indica en el artículo 9 como categorías especiales de datos: origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

[11] SWEENEY, L., "Simple Demographics Often Identify People Uniquely". Carnegie Mellon University, Data, Privacy Working Paper 3. Pittsburgh 2000. https://dataprivacylab.org/projects/identifiability/paper1.pdf

[12] LLÀCER,R.M., CASADO, M., BUISÁN, L. *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Ed. UB, Barcelona, 2015 . Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf

[13] Véase por ejemplo la Historia Clínica Compartida de Cataluña: https://ticsalutsocial.cat/es/projectes/oficina-interoperabilidad/hc3/ y el Sistema de Información para el desarrollo de la Investigación en Atención Primaria (SIDIAP) https://www.sidiap.org/index.php/es

[14] SANTALÓ, J. y CASADO, M. (coords.), *Documento sobre bioética y edición genómica en humanos*, Ed. UB, 2016, Barcelona. ISBN 978-84-475-4073-0. Disponible en http://hdl.handle.net/2445/105022

[15] "How should we think about clinical data ownership?", *Journal of Medical Ethics*, Ballantyne, Vol. 46, 2020, p. 289–294. https://jme.bmj.com/content/medethics/46/5/289.full.pdf

[16] La Real Academia Española define seudonimización como "tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona física identificada o identificable. Y se refiere específicamente al artículo 4.5 del Reglamento general de protección de datos.

[17] Véase por ejemplo la nota de Agencia Española de Protección de Datos sobre necesidad de evaluar los tratamientos de datos personales de la App Radar COVID (junio de 2020) https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-sobre-la-participacion-de-la-aepd-en-la-app-de y *Manifiesto en favor de la transparencia en desarrollos de software públicos,* firmado por más de 230 académicos e investigadores (septiembre de 2020) https://transparenciagov2020.github.io/ (última consulta, 5 de octubre de 2020).

[18] EUROPEAN COMMISSION, *Guidance How to complete your ethics self-assessment European Union*, febrero de 2019. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

[19] En este sentido véase el Reglamento General de Protección de Datos, artículo 5 Principios relativos al tratamiento 1. los datos personales serán: b) Recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.

[20] Véase la *Guia d'avaluació dels aspectes derivats de la normativa de Protecció de Dades en projectes de recerca*, editada por Direcció General de Recerca i Innovació en Salut, Direcció General d'Ordenació i Regulació Sanitària y Oficina del Delegat de Protecció de Dades- Fundació TIC SALUT SOCIAL, de 31 de juliol de 2020.

[21] Sobre estas cuestiones véanse las aportaciones de la Comisión de Bioética de la Universitat de Barcelona (CBUB), en particular, los formularios en función del tipo de investigación a desarrollar, así como otros requisitos a cumplir para adaptarse a la normativa de protección de datos. http://www.ub.edu/comissiobioetica/es/formularios La CBUB fue fundada por la Dra. María Casado en 1996, siendo la primera comisión de bioética de una universidad pública en nuestro contexto. Posteriormente, en el año 2002 crea también la Red de comités de ética de las universidades españolas y otros organismos públicos de investigación (RCEUC). La CBUB y la RCEUE han sido consideradas desde 2012 como referentes de buena práctica por universidades miembro de la Liga Europea de Investigación Intensiva (LERU, por sus siglas en inglés). Véase el informe "Towards a Research Integrity Culture at Universities: From Recommendations to Implementation", LERU, enero de 2020. https://www.leru.org/files/Towards-a-Research-Integrity-Culture-at-Universities-full-paper.pdf

[22] Véase la herramienta Gestiona de la Agencia Española de Protección de Datos. Gestiona EIPD que es un "asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos. Esta herramienta gratuita guía a los responsables y encargados del tratamiento en los aspectos que se deben tener en cuenta, proporcionando una base inicial para una gestión adecuada" https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd. También la Guía práctica y la plantilla evaluación del impacto relativa a la protección de datos del Reglamento general de protección de datos desarrollada por la Autoridad Catalana de Protección de Datos.

https://apdcat.gencat.cat/ca/drets_i_obligacions/responsables/obligacions/avaluacio-impacte-relativa-proteccio-dades/ . El OBD en colaboración con un equipo interdisciplinar ha desarrollado una metodología específica para efectuar evaluaciones de impacto relativas a los tratamientos de datos personales en el ámbito de la salud y la innovación a propuesta de la Fundació TICSalut, Oficina del Delegat de Protecció de Dades.

[23] EUROPEAN COMMISSION, H2020 Programme Guidelines on FAIR Data Management in Horizon 2020 26 de julio de 2016; https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf y CSUC, Gestión de datos de investigación, https://www.csuc.cat/es/consorciacion-tic/gestion-de-datos-de-investigacion

[24] LERU, *Open Science and its role in universities: a roadmap for cultural change*, mayo de 2018 y EUROPEAN COMMISSION, https://ec.europa.eu/digital-single-market/en/open-science

[25] Véase EUROPEAN DATA PROTECTION SUPERVISOR, Flowcharts and Checklists on Data Protection , 2020 https://edps.europa.eu/sites/edp/files/publication/flowcharts_and_checklists_on_data_protection_brochure_en_1.pdf

Relación de autores y firmantes del Documento

Itziar de Lecuona
Profesora Agregada del Departamento de Medicina y subdirectora del Observatorio de Bioética y Derecho- Cátedra UNESCO de Bioética de la Universidad de Barcelona. Miembro del Grupo de Trabajo Multidisciplinar Asesor del Ministerio de Ciencia e Innovación sobre los aspectos científicos de la COVID-19; del Comité de Bioética de la Universidad de Barcelona y del Comité de Ética de la Universidad Politécnica de Cataluña. Antigua vocal del Comité de Bioética de Cataluña y del Comité de Ética de Investigación con Medicamentos del Hospital Clínic de Barcelona.

María Jesús Bertrán
Médica, especialista en Medicina Preventiva y Salud Pública. Consultora del Servicio Medicina Preventiva y Epidemiología del Hospital Clínic de Barcelona. Miembro del Comité de Ética de Investigación con Medicamentos del Hospital Clínic de Barcelona y de la Comisión de Bioética de la Universidad de Barcelona.

Blanca Bórquez
Investigadora de la Biblioteca Nacional del Congreso de Chile. Miembro del Observatorio de Bioética y Derecho de la Universidad de Barcelona. Miembro del Comité de Ética del Servicio de Salud Metropolitano Occidente, Ministerio de Salud, Chile.

Lluís Cabré
Médico, especialista en medicina intensiva. Antiguo director de la Unidad de Cuidados Intensivos y Emergencias del Hospital de Barcelona. Miembro del Observatorio de Bioética y Derecho y profesor del Máster en Bioética y Derecho de la Universidad de Barcelona. Miembro de la Comisión Deontológica del Colegio Oficial de Médicos de Barcelona. Antiguo presidente del Comité de Ética Asistencial del Hospital de Barcelona y vocal del Comité de Bioética de Cataluña.

María Casado
Catedrática Acreditada de Filosofía del Derecho Moral y Política de la Universidad de Barcelona. Directora del Observatorio de Bioética y Derecho y Titular de la Cátedra UNESCO de Bioética de la Universidad de Barcelona. Fundadora de la Comisión de Bioética de la Universidad de Barcelona y de la Red de Comités de Ética de las Universidades Españolas y Otros Organismos Públicos de Investigación. Antigua vocal del Comité de Bioética de España y del Comité de Bioética de Cataluña.

Mirentxu Corcoy
Catedrática de Derecho Penal y directora del Departamento de Derecho Penal y Ciencias Penales de la Universidad de Barcelona. Miembro del Observatorio de Bioética y Derecho y Profesora del Máster en Bioética y Derecho de la Universidad de Barcelona.

Mariana Dobernig
Profesora de Derecho Civil y miembro del Observatorio de Bioética y Derecho de la Universidad de Barcelona. Presidenta del Comité de Ética de la Investigación de la Universidad Iberoamericana, Ciudad de México.

Fernando Estévez
Médico, especialista en neurología. Profesor Agregado de la Universidad de Cuenca-Ecuador. Miembro del Observatorio de Bioética y Derecho y profesor del Máster en Bioética y Derecho de la Universidad de Barcelona. Presidente del Comité de Ética del Hospital Santa Inés, Cuenca, Ecuador.

Fernando García López
Médico, especialista en nefrología y epidemiología. Jefe de Unidad del Área Neurodegeneración, Envejecimiento y Salud Mental del Centro Nacional de Epidemiología, Instituto de Salud Carlos III. Miembro del Observatorio de Bioética y Derecho y profesor del Máster en Bioética y Derecho de la Universidad de Barcelona. Presidente del Comité de Ética de la Investigación del Instituto de Salud Carlos III.

Begoña Gómez
Farmacéutica, Consultora 2 del Área de Ensayos Clínicos y Medicamentos en Investigación, Servicio de Farmacia, Área del Medicamento y antigua presidenta del Comité de Ética de Investigación con Medicamentos del Hospital Clínic de Barcelona.

Carlos Humet
Médico. Antiguo director del Hospital de Barcelona. Profesor del Máster en Bioética y Derecho de la Universidad de Barcelona. Miembro del Comité de Ética Asistencial del Hospital de Barcelona.

Lorena Jaume-Palasí
Directora Ejecutiva de la Ethical Tech Society. Cofundadora de la organización AlgorithmWatch. Miembro del Consejo Asesor de Inteligencia Artificial, España.

Eleonora Lamm
Subdirectora de Derechos Humanos de la Suprema Corte de Mendoza, Argentina. Miembro del Observatorio de Bioética y Derecho y Profesora del Máster en Bioética y Derecho de la Universidad de Barcelona. Miembro del Comité Nacional de Ética en las Ciencias y las Tecnologías, Argentina.

Fabiola Leyton
Investigadora posdoctoral del Observatorio de Bioética y Derecho y Profesora Asociada de Filosofía del Derecho de la Universidad de Barcelona. Miembro del Observatorio de Bioética y Derecho y profesora del Máster en Bioética y Derecho de la Universidad de Barcelona. Editora de la Revista de Bioética y Derecho de la Universidad de Barcelona. Miembro de la Comisión de Bioética de la Universidad de Barcelona.

Manuel Jesús López Baroni
Profesor de Filosofía del Derecho de la Universidad Pablo de Olavide. Coordinador y Profesor del Máster en Bioética y Derecho y miembro del Observatorio de Bioética y Derecho de la Universidad de Barcelona.

Ramón López de Mántaras
Profesor de Investigación del Instituto de Investigación en Inteligencia Artificial del CSIC. Premio Nacional de Investigación. Miembro del Consejo Asesor del Observatorio de Ética en Inteligencia Artificial de Cataluña; del Grupo de Trabajo Multidisciplinar Asesor del Ministerio de Ciencia e Innovación sobre los aspectos científicos de la COVID19 y del Comité Asesor del Ministerio de Educación e Investigación del Gobierno Federal Alemán para la implementación de la estrategia alemana de Inteligencia Artificial.

Florencia Luna
Investigadora Independiente del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) de Argentina. Docente de la Universidad de Buenos Aires y coordinadora del Área de Bioética de la Facultad Latinoamericana de Ciencias Sociales (FLACSO). Miembro del Observatorio de Bioética y Derecho y profesora del Máster en Bioética y Derecho de la Universidad de Barcelona. Fundadora de la Revista Perspectivas Bioéticas. Miembro de la Comité de Ética y Derechos Humanos asesor Ministerio de Salud y de la Comisión ad-hoc para realizar recomendaciones sobre la pandemia por COVID-19, Argentina.

Gemma Marfany
Catedrática de Genética y directora del Grupo de Investigación "Genética Molecular Humana"; miembro del Observatorio de Bioética y profesora del Máster en Bioética y Derecho y secretaria de la Comisión de Bioética de la Universidad de Barcelona.

Joaquim Martínez-Montauti
Médico, especialista en medicina interna. Antiguo coordinador del Servicio de Medicina Interna del Hospital de Barcelona. Miembro del Observatorio de Bioética y Derecho y profesor del Máster en Bioética y Derecho de la Universidad de Barcelona. Presidente del Comité de Ética Asistencial del Hospital de Barcelona.

Mariela Mautone
Médica, especialista en nefrología. Miembro del Observatorio de Bioética y Derecho y profesora del Máster de Bioética y Derecho de la Universidad de Barcelona. Co-coordinadora de la Comisión de Derechos Humanos y Bioética del Sindicato Médico, Uruguay.

Irene Melamed
Médica. Profesora e investigadora del Programa de Bioética, FLACSO, Argentina. Miembro del Observatorio de Bioética y Derecho y profesora del Máster en Bioética y Derecho de la Universidad de Barcelona. Miembro del Comité de Bioética Asistencial de Swiss Medical, Ciudad Autónoma de Buenos Aires.

Míriam Méndez
Responsable del área de investigación de la Oficina del Delegado de Protección de Datos de Salud de la Fundació TIC Salut**.** Antigua vocal del Comité de Ética de Investigación con Medicamentos del Hospital Clínic de Barcelona.

Mónica Navarro-Michel
Profesora Agregada de Derecho Privado de la Universidad de Barcelona. Miembro del Observatorio de Bioética y Derecho y profesora del Máster en Bioética y Derecho de la Universidad de Barcelona. Miembro del Comité de Ética de GRAVIDA.

María José Plana
Profesora de la Facultad de Derecho de la Universidad de Wageningen. Miembro del Observatorio de Bioética y Derecho y Codirectora del Máster en Alimentación, Ética y Derecho de la Universidad de Barcelona.

Neus Riba
Farmacóloga Clínica. Secretaria técnica del Comité de Ética de Investigación con Medicamentos de la Fundación de Investigación de Sant Joan de Déu. Antigua secretaria técnica del Comité de Ética de Investigación con Medicamentos del Hospital Clínic de Barcelona.

Germán Rodríguez
Project Manager en la Dirección de Estrategia y Planificación y miembro del Comité de Ética de Investigación con Medicamentos del Hospital Clínic de Barcelona.

Robert Rubió
Director de la Oficina del Delegado de Protección de Datos de Salud de la Fundació TIC Salut y Profesor Asociado de Derecho Internacional Público de la Universidad de Barcelona.

Josep Santaló
Catedrático de Biología Celular de la Universidad Autónoma de Barcelona. Miembro del Observatorio de Bioética y Derecho y Profesor del Máster en Bioética y Derecho de la Universidad de Barcelona. Miembro del Comité de Ética en Experimentación Animal y Humana.

Paula Subías
Matemática especializada en ciencia computacional aplicada al ámbito de la salud. Data Scientist e investigadora de Eurecat, línea Data Analytics in Medicine de eHealth.

Organització
de les Nacions Unides
per a l'Educació,
la Ciència i la Cultura

Càtedra UNESCO de Bioètica
de la Universitat de Barcelona

Observatori de
Bioètica i Dret

www.bioeticaidret.cat
www.bioeticayderecho.ub.edu
www.bioethicsandlaw.es