Ética y protección de datos de salud en contexto de pandemia: una referencia especial al caso de las aplicaciones de rastreo de contactos

Txetxu Ausín
Instituto de Filosofía. CSIC
txetxu.ausin@cchs.csic.es
M.ª Belén Andreu Martínez
Universidad de Murcia. Centro de Estudios en Bioderecho, Ética y Salud
beland@um.es

Fecha de recepción: 12-6-2020
Fecha de aceptación: 30-6-2020

Resumen

El análisis y el tratamiento masivo (*big data*) de datos de salud mediante algoritmos de inteligencia artificial, así como las plataformas y las aplicaciones para el rastreo de contactos y geolocalización, se han planteado como herramientas necesarias para afrontar con éxito una situación como la actual pandemia de la COVID-19. Ejemplos como los de Corea del Sur, Noruega o Singapur parecen abundar en este sentido, y Europa se ha apuntado con rapidez a secundarlos, aunque sin perder de vista su propio marco normativo, de protección de derechos fundamentales y de respeto a principios éticos básicos. Planteamos algunas cuestiones éticas y jurídicas en torno al tratamiento de datos de salud en un contexto de emergencia de salud pública como el actual: legitimidad, limitaciones para el consentimiento, relaciones entre lo público y lo privado, seguridad, privacidad… Para ello tomaremos como referencia el RGPD de la UE, las recomendaciones de la Comisión Europea, las directrices del EDPB y de la AEPD, los pronunciamientos como el del Comité de Bioética de España o el reciente marco europeo sobre digitalización (febrero-marzo 2020).

Palabras clave: salud; protección de datos; ética; RGPD; apps; COVID-19

Abstract. *Ethics and health data protection in pandemics: A reference to the case of applications for contact tracking*

The analysis and massive treatment (big data) of health data using artificial intelligence algorithms, as well as platforms and applications for contact tracking and geolocation, have been proposed as necessary tools to successfully manage a situation like the current COVID-19 pandemic. Examples such as those from South Korea, Norway or Singapore seem to be having an impact and Europe has been quick to endorse them, although without losing sight of its own regulatory framework, the protection of fundamental

* Este trabajo se realiza en el marco de los proyectos INBOTS CSA network: *Inclusive Robotics for a better Society* (EU H2020 G.A. 780073), y BIODAT: *Datos de salud: Claves ético-jurídicas para la transformación digital en el ámbito sanitario* (Fundación Séneca-Agencia de Ciencia y Tecnología de la Región de Murcia – Ref. 20939/PI/18).

rights, and respect for basic ethical principles. We raise some ethical and legal questions regarding the processing of health data in a context of public health emergency such as the present one: legitimacy, limitations to consent, public/private relations, security, and privacy, among others. To this end, we take as a reference the EU General Data Protection Regulation (GDPR), recommendations of the European Commission, guidelines of the European Data Protection Board (EDPB) and the Spanish Data Protection Agency (AEPD), pronouncements such as that of the Spanish Bioethics Committee or the recent European framework on digitalisation (February–March 2020).

Keywords: health; data protection; ethics; GDPR; apps; COVID-19

Los datos de salud son el conjunto de informaciones obtenidas de registros, muestras y pruebas que recogen la situación y la evolución clínica de un individuo. Dan cuenta del estado físico y mental de una persona, de la atención sanitaria que ha recibido, de la condición de sus funcionamientos básicos, de las enfermedades y cirugías que ha padecido y del riesgo de sufrir otras en el futuro, de los medicamentos consumidos, de los antecedentes familiares y de las vacunas recibidas. También pueden incluir hábitos alimentarios y de ejercicio y metas de salud (como adelgazar o dejar de fumar), siempre que estos revelen información sobre el estado de salud de la persona (RGPD, art. 4.15)[1]. Constituyen, evidentemente, información íntima y personalísima de los individuos y, en consecuencia, son datos sensibles que requieren una protección especial.

Es claro también que dichos datos son más que un mero recordatorio y registro del estado de salud y del proceso asistencial, porque constituyen una fuente crucial de conocimiento para la investigación médica y biológica. Más allá de que los pacientes comuniquen sus datos para el fin concreto de su cuidado sanitario, estos datos tienen un enorme potencial para la investigación biomédica: mejora de tratamientos, desarrollo de nuevos fármacos, abordaje de enfermedades y creación de nuevos equipos diagnósticos. Estas oportunidades se han multiplicado con las posibilidades que introduce la ciencia de datos masivos (*big data analytics*) y su tratamiento mediante algoritmos de inteligencia artificial, lo que facilitará una mejor comprensión de los procesos de la enfermedad y sus conexiones.

La pandemia de la COVID-19 ha acentuado la urgencia y la necesidad de investigar para encontrar tratamientos y vacunas frente al virus y para alcanzar un mejor conocimiento y control de la enfermedad, a fin de prevenir futuros rebrotes, conjugando la perspectiva clínico-asistencial con el ámbito de la salud pública.

Sin embargo, como expresa el Comité de Bioética de España (en adelante, CBE) en su informe de 28 de abril de 2020 sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de COVID-19, la urgencia para avanzar en el conocimiento no puede

1. Reglamento General de Protección de Datos: Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD).

hacerse a costa del rigor científico imprescindible para conseguir que ese conocimiento alcance suficiente consistencia. Y legitimidad, añadiríamos nosotros.

Precisamente, la UE, dentro del programa Science with and for Society (Ciencia con y para la Sociedad), ha planteado un modelo de investigación e innovación responsables. La RRI (siglas en inglés de Investigación e Innovación Responsables) es una retórica radical sobre la apertura y la socialización de los procesos tecnocientíficos que se concreta en cuatro principios de gobernanza: anticipación, reflexividad, deliberación y responsabilidad (Stilgoe et al., 2013). Esta apertura y socialización comprende como un elemento nuclear la ética para fomentar la integridad científica, con el fin de prevenir y evitar prácticas de investigación inaceptables. Las mejores soluciones éticas sobre cuestiones difíciles facilitan sin duda la aceptabilidad y la confianza en la investigación, cuestiones más determinantes aún a la hora de introducir intervenciones urgentes en un contexto de pandemia (volveremos a hablar de ello más adelante).

Así, el tratamiento de datos personales de salud puede considerarse lícito no solo para proteger los intereses vitales del interesado, sino también por motivos de interés público y fines humanitarios, como es el caso del control de epidemias y su propagación. Especialistas en protección de datos como Ricard Martínez han concluido que los tratamientos de datos vinculados al control y a la lucha contra una epidemia constituyen cláusulas habilitantes al estar en juego los intereses vitales de la comunidad (Martínez, 2020). Como afirmaba el Comité de Bioética de España en su documento antes mencionado, el derecho a la intimidad y la protección de datos, como los demás derechos, se manifiestan en un entorno social de interrelaciones e interdependencia en el que es tan relevante reconocer la autonomía del individuo como la solidaridad del ciudadano. Por ello, lo relevante para el uso secundario de los datos de salud y las muestras biológicas no será tanto que el individuo haya otorgado su consentimiento previo para el nuevo fin al que pretenden destinarse los datos o que el dato esté estrictamente anonimizado, como que el origen de los datos sea legítimo, que su uso secundario revista un interés muy relevante para la salud de la colectividad y que se implementen garantías suficientes que impidan que terceros no legitimados puedan acceder a través del dato a la identidad del individuo, sin exigir necesariamente dicha estricta anonimización (CBE, 2020: 18). Esta visión se encuentra recogida, por otra parte, en el propio RGPD, que establece un marco flexible para la investigación científica con datos personales, con especial referencia a la investigación en salud pública, y se ha reflejado en nuestra Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (disposición adicional 17). En ambos casos, la seudonimización constituye una de las principales garantías para la investigación en salud, y la situación de excepcional relevancia y gravedad para la salud pública es una de las situaciones en que nuestra ley permite a las autoridades encargadas de la vigilancia epidemiológica investigar con datos personales de individuos identificados.

Uno de los elementos importantes en la lucha contra la pandemia (incluso más que otras medidas, como el confinamiento, para interrumpir la cadena

de transmisión, en palabras de la propia Comisión Europea, 2020/C 124 I/01) son las aplicaciones móviles que alertan del contacto con personas afectadas por COVID-19 —sobre todo en la estrategia de salida en la que nos encontramos y como complemento a otras medidas[2]—. Las alertas tempranas son cruciales, porque permiten adoptar medidas de aislamiento en prevención de la incubación del virus. En una fase de desconfinamiento de la población, el objetivo se está centrando en la rápida detección de los casos positivos para que se pueda detener la cadena de transmisión. La identificación rápida de casos infectados permite un confinamiento selectivo, cortando de raíz los rebrotes que se puedan ir produciendo.

El seguimiento de contactos es una técnica conocida en epidemiología (a través de entrevistas), pero la imposibilidad de hacer un seguimiento «manual» ante el elevado número de contagiados por la COVID-19 ha planteado el uso de medios tecnológicos. Existen al menos 47 aplicaciones de seguimiento de contactos en 28 países (<https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/>), tanto de desarrollo público como privado. Y en Europa un buen número de ellos ya la han puesto en funcionamiento o tienen proyectado hacerlo (European Union Agency for Fundamental Rights, 2020).

Sin embargo, estas intervenciones digitales provocan recelo y desconfianza en la medida en que se contemplan como amenazas a la privacidad y a la equidad, ya que pueden crear perfiles permanentes de las personas sobre su salud, sus movimientos y sus interacciones sociales, de modo que las convierten en más vulnerables.

Ya se han publicado directrices por parte de distintos organismos internacionales con la finalidad de crear un marco mínimo de estándares que debe cumplir la tecnología que se desarrolle para hacer frente a la pandemia. En Europa podemos destacar las de la Comisión Europea (*Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos*, de 17-4-2020, 2020/C 124 I/01), la Junta Europea de Protección de Datos (en adelante la nombraremos EDPB, utilizando sus siglas en inglés: *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, de 21-4-2020) o el Consejo de Europa (*Joint Statement on Digital Contact Tracing*, de 28-4-2020). En todos ellos se pone de relieve la necesidad de generar confianza y aceptación social. Esta aceptabilidad social de la vigilancia y la confianza en la tecnología y las instituciones es determinante para su efectividad, en la medida en que se necesita que en torno a un 60% de la población se instale voluntariamente este tipo de aplicaciones (descartamos aquí la opción autoritaria china que obliga a instalar dichas tecnologías).

2. Nos centraremos principalmente en este tipo de aplicaciones, puesto que son las que mayores problemas éticos y jurídicos están planteando. No analizamos otro tipo de tecnologías relativas al control y seguimiento de la pandemia de COVID-19, como son las cámaras que miden la temperatura corporal, las aplicaciones sobre consejos de salud en el confinamiento, las encuestas de salud o los dispositivos de medición de variables físicas.

Ahora bien, por parte de los gobiernos no se está realizando ningún análisis en profundidad del potencial impacto del uso de la tecnología para frenar la propagación del virus en derechos que no sean la vida privada o la protección de datos personales (European Union Agency for Fundamental Rights, 2020: 45). El desarrollo ético de este tipo de aplicaciones juega un papel fundamental a la hora de generar esa confianza y aceptación de la tecnología en situaciones de crisis como la actual, y es una herramienta que las autoridades deben incorporar en su política de lucha contra la pandemia.

¿Y qué elementos éticos han de tomarse en consideración? Básicamente, los siguientes:

1. No maleficencia

La seguridad (*security & safety*) de los sistemas tecnológicos responde al deber de no causar daño, de minimizarlo, protegiendo a los individuos y a los grupos. Y esto implica no solo acciones de anticipación ante posibles riesgos de daño (precaución y prevención). La seguridad es un valor social crucial en la interacción de las personas con la tecnología. En este sentido, se precisan estándares de seguridad que establezcan procedimientos claros para medir, comprobar y certificar la funcionalidad de las aplicaciones.

Igualmente, el tratamiento de datos mediante algoritmos puede producir sesgos injustos que den lugar a un riesgo de discriminación, perfilamiento y estigmatización. En este sentido, la evaluación ética de las aplicaciones ha de extremar el cuidado para detectar sesgos de género, edad, económicos…

2. Proporcionalidad y beneficencia

Significa que la intervención es proporcional y benéfica ante la gravedad de la situación. En este sentido, se trata de aplicaciones suficientemente efectivas, cuya necesidad quede convenientemente demostrada (no existen otras medidas menos invasivas que permitan alcanzar la meta propuesta), y acotadas a un propósito bien definido y determinado (en este caso, el rastreo de contactos de posibles afectados por la COVID-19). Esto significa que no pueden utilizarse este tipo de soluciones tecnológicas para realizar una vigilancia masiva de la población. Señala el EDPB que, conforme al principio de limitación de finalidad, debe estar especificada dicha finalidad y eliminarse otros posibles usos (comerciales, policiales, etc.) que no estén relacionados con la gestión de la COVID-19. Asimismo, implica su carácter temporal: se «desactivará» cuando la pandemia esté controlada y, por tanto, han de establecerse claramente los criterios para determinar dicho momento y qué entidad será la responsable de tomar esta determinación.

3. Autonomía

Significa que no solo la instalación de la aplicación es voluntaria y requiere el consentimiento del afectado (no se impone ni se aplica por defecto), sino

que no conlleva penalización de ningún tipo por su no aceptación. Asimismo, la autonomía implica la capacidad de los usuarios para «desconectarse» de la aplicación en cualquier momento y de borrar sus datos. Esto es, exige la controlabilidad del proceso. En este sentido, su código debería ser abierto (*open source*) para compartir, inspeccionar y, eventualmente, mejorar su desempeño (transparencia).

No obstante, la voluntariedad puede redundar negativamente en la efectividad. Si la instalación es baja (como en Singapur o Noruega, sobre un 20% de la población) podría no compensar el riesgo que se impone sobre la privacidad (análisis de costo-beneficio). Estas aplicaciones están sometidas al trilema entre voluntariedad, privacidad y efectividad. Apostar por la privacidad y la voluntariedad puede reducir la efectividad, en la medida en que no se adopten voluntariamente de forma masiva y no intrusiva.

4. Privacidad

Los datos deben estar seudonimizados (generación de códigos o pseudónimos). En este sentido son preferibles éticamente los sistemas de rastreo de contactos por proximidad (Bluetooth) y no por el seguimiento de los movimientos individualizados de las personas (localización de cada una). Esto último conllevaría una vigilancia o un control permanente del individuo, lo que supone una grave injerencia en su privacidad y, en general, en sus derechos fundamentales. Por ello, su régimen es mucho más estricto (es lícito su uso solo si hay anonimización, libre consentimiento de la persona o en situaciones excepcionales previstas en una ley), y su no utilización se considera un estándar mínimo en las directrices oficiales antes señaladas.

Se impone la privacidad por diseño y por defecto que justificarían también que el funcionamiento de estas aplicaciones se realizara sin identificación directa del usuario (y estableciendo medidas para evitar la reidentificación), la información se almacenara preferentemente en el terminal dispositivo y se recolectara solo cuando fuera necesario (confirmación de contagio), a lo que se podría añadir, como medida de control del usuario, que la persona debe consentir la compartición de los datos que se recabaron en su dispositivo (para generar la alerta) —la autonomía que acabamos de mencionar—.

5. Equidad

Las aplicaciones y otras tecnologías han de estar disponibles y accesibles para todo el mundo, independientemente del nivel económico o tecnológico. Además, también han de ser independientes del grado de alfabetización o destreza digital del usuario. Por tanto, deben ser gratuitas, se deben distribuir a toda la población y su uso ha de ser amigable incluso para legos y para la más amplia gama de dispositivos móviles. Aun así, hay que tener presente el importante número de personas que no dispone ni usa un teléfono inteligente o que el suyo es anticuado (en Australia, por ejemplo, no se contemplaba que su aplicación funcionara en teléfonos con software más antiguo que iOS10 o Android

6.0). (Sobre equidad y eficiencia en contexto de pandemia puede consultarse el trabajo de Teresa López de la Vieja y David Rodríguez-Arias en este mismo número de Enrahonar.)

Para comprobar si las aplicaciones satisfacen estos criterios éticos básicos se puede recurrir a sistemas de evaluación y chequeo ético (Ethical Impact Assessment) y sobre la privacidad (Data Protection Impact Assessment) de las aplicaciones (Morley et al., 2020; Morte, 2020). Se utilice uno u otro sistema de valoración del impacto ético de las aplicaciones, parece claro que esta evaluación habrían de realizarla comités o grupos éticos independientes y no los diseñadores de las mismas o los gobiernos: <https://nhsbsa-socialtracking.powerappsportals.com/EAB%20Letter%20to%20NHSx.pdf>.

Un ejemplo de una aplicación de rastreo de contactos COVID-19 que incorpora los elementos antes mencionados es el protocolo DP-3T, desarrollado por un equipo europeo coordinado por la española Carmela Troncoso, profesora adjunta de la Escuela Politécnica Federal de Lausana (Suiza). Como ejercicio de transparencia, su desarrollo puede consultarse en abierto en la web <https://github.com/DP-3T/documents>. Algunas instituciones, como el Gobierno Vasco (en colaboración con las empresas Tecnalia e Ibermática), están desarrollando un proyecto basado en este protocolo (Optimización del Sistema de Diagnóstico y Contención: OptiDiC). El objetivo final son sistemas que garanticen la minimización de los datos, a fin de evitar su uso abusivo, impedir el seguimiento de los usuarios y que tengan un carácter temporal.

Es un asunto importante definir y delimitar el papel de los diferentes agentes, públicos y privados, en el desarrollo de estas tecnologías. Es evidente que las instituciones públicas necesitan el conocimiento y la experiencia (*how know*) de las empresas tecnológicas para desarrollar este tipo de productos e intervenciones. Pero no hay que olvidar que estas aplicaciones deben estar integradas en una estrategia de salud pública más amplia, donde el responsable del tratamiento de los datos sea la correspondiente autoridad sanitaria, debiendo estar claro el rol y la responsabilidad de los otros actores que puedan intervenir en él. Constituye este un elemento fundamental, en la medida en que la información que se proporcione a través de dichas aplicaciones debe estar contextualizada en el correspondiente escenario de salud pública y, además, la información que se genere debe utilizarse en beneficio del sistema de salud. En este sentido, la confirmación del diagnóstico de infectado (caso) y su notificación a contactos debe ser resultado de una evaluación realizada por la autoridad pública. Igualmente, la determinación, por ejemplo, de qué es un contacto a efectos de estas aplicaciones (cuánto tiempo y a qué distancia han tenido que estar los dispositivos que incorporan la aplicación como para que se genere el código o pseudónimo)[3].

3. La autoridad pública de salud es quien debe confirmar, a través de los tests preceptivos, el diagnóstico y por tanto corroborar el caso, que luego se comunicaría a los contactos. Por otra parte, aunque la notificación a los contactos puede depender de la voluntad del sujeto (en el sentido de que la voluntariedad en el uso de la aplicación implica también que la persona no puede ser obligada a ceder los pseudónimos guardados como contacto en su

Por otra parte, estos sistemas tecnológicos de rastreo de contactos presentan limitaciones importantes: su eficacia depende del número de descargas, como hemos dicho, y podría darse un uso malicioso por parte del usuario. Por ello es crucial que se utilicen como apoyo (que no sustituto) del trabajo que realizan los equipos de «rastreo manual», donde juega un papel determinante la atención primaria.

Existe, además, por parte de las grandes compañías de tecnologías de la información y la comunicación, un uso espurio e interesado de la ética y la autorregulación como coartada para esquivar las regulaciones (Ochigame, 2019). Por ello, los comités éticos independientes monitorizarían la aplicación de estas intervenciones a modo de órganos de garantía para el cumplimiento de estos principios éticos, estableciendo las posibles modificaciones o mejoras necesarias y la propuesta de finalización de su uso en colaboración con las autoridades de salud pública.

Un desarrollo ético de estas intervenciones tecnológicas es indispensable para garantizar su aceptabilidad social, su legitimidad y la confianza pública, indispensables para un abordaje exitoso de la pandemia. Incluso en una crisis como la actual, el enfoque *pruébese-todo* es tremendamente peligroso, no solo porque erosiona los derechos y las libertades fundamentales que organizan la vida social, sino también porque causa una pérdida de recursos por aplicaciones y diseños mal planteados que no se aprovechan efectivamente para enfrentar la crisis.

Referencias bibliográficas

Comisión Europea (2020). *Comunicación de la Comisión «Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos»* (2020/C 124 I/01). DOUE 17.4. 2020.

Comité de Bioética de España (2020). *Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de COVID-19*. Recuperado el 11 de junio de 2020, de <http://assets.comitedebioetica.es/files/documentacion/Informe%20CBE%20investigacion%20COVID-19.pdf>.

dispositivo), ello no significa que dependa de su sola voluntad, pudiendo hacer esta comunicación sin que haya una confirmación oficial de diagnóstico. En este sentido, por ejemplo, en la aplicación francesa StopCovid, la transferencia del histórico de pseudónimos de los contactos de una persona infectada al servidor central (la aplicación francesa se basa en un sistema centralizado) requiere utilizar un código de uso único remitido por un profesional de la salud después de un diagnóstico o una prueba de detección positiva (art. 2 Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé «StopCovid», ELI: <https://www.legifrance.gouv.fr/eli/decret/2020/5/29/SSAZ2012567D/jo/texte>). Con ello se pretende evitar que una persona falsee la base de datos del servidor central de la aplicación declarándose positiva sin haber sido detectada como tal. La norma señalada dispone también, entre otras cosas, que será el Ministerio de Sanidad francés el que determinará los criterios de distancia y duración del contacto, para determinar que dos teléfonos se encuentran a una distancia suficiente como para que pueda existir riesgo de contagio.

European Data Protection Board (2020). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak* (21 de abril). Recuperado el 11 de junio de 2020, de <https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en>.

European Union Agency for Fundamental Rights (2020). *Coronavirus pandemic in the EU - Fundamental Rights Implications: With a focus on contact tracing apps. Bulletin 2*. Recuperado el 11 de junio de 2020, de <https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1>.

Martínez, Ricard (2020). «Los tratamientos de datos personales en la crisis del COVID-19: Un enfoque desde la salud pública». *Diario La Ley*, n.º 9604 (marzo).

Morley, Jessica et al. (2020). «Ethical guidelines for COVID-19 tracing apps». *Nature*, 582, 29-31. <https://doi.org/10.1038/d41586-020-01578-0>

Morte, Ricardo (2020). «Reflexiones sobre las evaluaciones de impacto: Una propuesta para un modelo de Evaluación de Impacto Ético en el ámbito de la salud». *Dilemata*, 32, 71-82. Recuperado el 11 de junio de 2020, de <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000351/671>.

Ochigame, Rodrigo (2019). «The invention of 'Ethical AI': How Big Tech Manipulates Academia to Avoid Regulation». *The Intercept*. Recuperado el 11 de junio de 2020, de <https://theintercept.com/2019/12/20/mit-ethical-ai-artificial-intelligence/>.

Stilgoe, J.; Owen, R. y Macnaghten, P. (2013). «Developing a framework for responsible innovation». *Research Policy*, 42 (9), 1568-1580.

Txetxu Ausín es científico titular en el Instituto de Filosofía del CSIC, donde dirige el Grupo de Ética Aplicada (GEA), además de profesor invitado en varias universidades y colaborador en el Instituto de Gobernanza Democrática - Globernance. Sus áreas de trabajo son la ética pública, la bioética, la lógica jurídica, los derechos humanos y la filosofía de las tecnologías disruptivas. Miembro del Grupo de expertos de la OCDE sobre ética de la investigación y nuevas formas de datos para la investigación económica y social. Editor y autor de varias obras sobre estos temas, en la actualidad forma parte de los equipos de investigación de la Red INBOTS CSA: Robótica Inclusiva para una Sociedad Mejor; EXTEND: Sistema Neuronal Hiperconectado Bidireccional, y BIODAT: Datos en salud. Presidente de la Red Española de Filosofía. Vocal independiente de la Comisión de Ética Pública del Gobierno Vasco y Patrono de la Fundación Clúster de Ética del País Vasco.

Txetxu Ausín is a tenured scientist at the Institute for Philosophy of the Spanish National Research Council (CSIC). He is director of the Applied Ethics Group (GEA) as well as invited professor at several universities and researcher at the Globernance Institute of Democratic Governance. His research areas involve public ethics, bioethics, deontic logic, human rights and philosophy of disruptive technologies. He is member of the OECD Expert Group on research ethics and new forms of data for social and economic research. Editor and author of publications on these issues, he is currently a researcher in the INBOTS CSA network: Inclusive Robotics for a better Society, EXTEND: Bi-directional Hyper-connected Neural System and BIODAT: health data. He is also president of the Spanish Network of Philosophy, an independent member of the Public Ethics Commission of the Basque Government and patron of the Cluster Ethics Foundation of the Basque Country.

M.ª Belén Andreu Martínez es profesora titular de Derecho Civil, coordinadora de investigación del Centro de Estudios en Bioderecho, Ética y Salud (CEBES) y directora del Grupo de Investigación en Bioderecho, Ética, Salud y Tecnología de la Universidad de Murcia. Actualmente es la IP del proyecto *Datos de salud: Claves ético-jurídicas para la transformación digital de la sanidad* (BioDat) (financiado por la Agencia de Ciencia y Tecnología de la Región de Murcia) y participa en otros tres proyectos relacionados con la temática de derecho, tecnología y salud. Cuenta con tres sexenios (de investigación y transferencia). Miembro titular del Consejo Regional de Ética Asistencial (Consejería de Sanidad y Política Social de la Región de Murcia). Coordina la doble titulación de máster en Bioderecho y Nuevas Tecnologías entre las universidades de Murcia y Lille (Francia).

M.ª Belén Andreu Martínez is a professor of private law and research coordinator at the Center for Studies in Biolaw, Ethics and Health (CEBES) and director of the Biolaw, Ethics, Health and Technology Research Group at the University of Murcia. She is currently director of the research project *Health data: Ethical and legal keys for the digital transformation of the health system* (BioDat) of the Science and Technology Agency of the Region of Murcia and is involved in three other projects related to law, technology and health. She has three six-year periods of research and knowledge transfer recognized by the National Commission for the Assessment of Research Activity (CNEAI). She is also member of the Regional Council of Care Ethics of the Department of Health and Social Policy, Region of Murcia. She is coordinator of the dual Master of Bio-law and New Technologies between the University of Murcia and the University of Lille, France.