Reflexiones sobre las evaluaciones de impacto. Una propuesta para un modelo de Evaluación del Impacto Ético en el ámbito de la salud*

Ricardo Morte Ferrer
Universidad de Granada
LI²FE
ricardo63@autistici.org

ISSN 1989-7022

Reflections on Impact Assessments. A Proposal for a Model for Ethical Impact Assessment in the Field of Health

Resumen: En muchos ámbitos de aplicación de las nuevas tecnologías existe una cierta tradición consistente en realizar evaluaciones de impacto durante el desarrollo y, en el caso ideal, de forma previa a su implementación. Uno de los ejemplos más recientes es la Evaluación del Impacto sobre la Privacidad introducida por el Reglamento General de Protección de Datos (RGPD) en su artículo 35. En este trabajo se revisará el concepto de Evaluación de Impacto y se elaborará una propuesta de modelo de Evaluación del Impacto Ético de nuevas tecnologías en el ámbito de la salud.

Palabras clave: modelo, evaluación, ética, tecnología, vulnerabilidad

Abstract: Since some time exists the tradition of using different types of impact assessment when developing and, ideally, before implementing new technologies. One example is the Data Protection Impact Assessment introduced in article 35 of the General Regulation on Data Protection (GDPR). In this work we will review the concept of Impact Assessment and we will propose a model for the Ethical Impact Assessment of new technologies in the field of Health.

Keywords: model, evaluation, ethics, technology, vulnerability

Ricardo Morte Ferrer: "Reflexiones sobre las evaluaciones de impacto. Una propuesta para un modelo de Evaluación del Impacto Ético en el ámbito de la salud", en Ricardo Morte Ferrer: *Debate: Digitalización y salud*
ILEMATA, Revista Internacional de Éticas Aplicadas, nº 32, 71-82

1. Introducción

El desarrollo tecnológico ha sufrido una aceleración extraordinaria en las últimas décadas, especialmente en lo que afecta a las tecnologías de la información y la comunicación (TIC). Además, ese desarrollo ha tenido un factor diferencial si lo comparamos con anteriores revoluciones tecnológicas, ya que no solo se ha producido la revolución en el campo de las TIC, sino que las TIC han invadido todos los ámbitos de la actividad humana.

Aunque ese sería tema para un trabajo diferente, conviene recordar que la mencionada revolución se ha producido en una época en la que la economía esta dominada por las ideas neoliberales y por la búsqueda permanente e incluso me atrevería a decir incontrolada de la innovación. Por ese motivo el análisis de riesgo de una nueva tecnología sigue más o menos los siguientes pasos:

- ¿Esa tecnología es factible?
- ¿La podemos desarrollar nosotros?
- ¿Va a generar facturación y beneficios a corto o medio plazo?
- ¿Nos puede crear problemas legales a corto plazo?

Si la respuesta a las tres primeras preguntas es afirmativa y la respuesta a la cuarta es negativa, el análisis de riesgo se da por finalizado y el desarrollo e implementación pue-

* Este trabajo se enmarca en los proyectos europeos INBOTS (780073) y EXTEND (779982), del Programa H2020.

Received: 28/04/2020
Accepted: 09/05/2020

ISSN 1989-7022

Dilemata, año 12 (2020), nº 32, 71-82

de arrancar sin ninguna evaluación adicional de las posibles consecuencias (técnicas, de seguridad, sobre la privacidad, éticas…). Reconozco que la exposición aquí realizada está pensada como una provocación, pero quien lea este texto deberá reconocer que, por poner un ejemplo, el desarrollo de lo que se conoce como el Internet de las cosas es un claro ejemplo que ha seguido un proceso de ese tipo. Ese y desarrollos del mismo tipo han llevado al experto en seguridad Bruce Schneier a escribir un libro titulado *„Click here to kill everybody"*.

La mencionada situación, o quizás sería más correcto decir evolución, llama la atención porque desde hace ya bastante tiempo existe una extensa literatura e institutos de investigación sobre la evaluación de la tecnología o de las consecuencias de las tecnologías. Como ya se ha mencionado anteriormente, la evaluación del impacto sobre la privacidad se ha visto reactivada por la entrada en vigor del RGPD. También que hay que reconocer que existen diferentes trabajos sobre la Evaluación del Impacto Ético, aunque no van en la dirección que aquí se quiere proponer. En el siguiente epígrafe revisaremos las metodologías (y terminologías) hasta ahora mencionadas ya que parece necesario hacerlo para poder entender mejor la propuesta que se quiere realizar.

2. Diferentes ejemplos de evaluaciones del impacto de las tecnologías.

2.1. Evaluación de la tecnología y/o de las consecuencias de la tecnología (en alemán **Technik Folgenabschätzung***)*

Aunque hay diferentes definiciones, la siguiente me parece bastante adecuada:

> "En la actualidad se entiende por Evaluación de Tecnologías un conjunto de métodos que analizan los diferentes y diversos impactos o efectos derivados de la aplicación de tecnologías, estudiando los efectos de posibles tecnologías alternativas e identificando los grupos sociales que puedan verse afectados. Su objetivo último estriba en tratar de reducir o anular los efectos negativos de algunos tecnologías imperantes, optimizando sus efectos positivos y contribuyendo así a su aceptación por la sociedad". (Gemma Múñoz-Alonso López).

El motivo por el que esta definición me parece adecuada para el trabajo actual es que se aleja del término inglés *assessment*, que parece implicar un tipo de evaluación aséptica o neutral de una tecnología, y va más en la dirección de una evaluación de las consecuencias, como hace el término alemán *Folgenabschätzung.* En la historia de la evaluación de la tecnología esta diferencia ha existido como una tensión latente y durante mucho tiempo se consideraba que el camino correcto era el que permitía mantener una posición neutral frente a la tecnología que se estaba analizando. Actualmente la tendencia es la contraria y se está reforzando el enfoque normativo en la evaluación de las tecnologías, entre otros motivos por la antes mencionada situación con una economía marcadamente neoliberal, junto con una búsqueda descontrolada de la innovación, que hacen que algunos expertos en la materia muestren una sería preocupación y manifiesten la necesidad de practicar la evaluación de las tecnologías de una forma que permita alcanzar un mayor nivel de información a diferentes niveles (legislativo, ejecutivo, administración pública, empresas…) En la bibliografía incluida al final de este artículo aparece un número de la revista alemana *Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis* (traducción directa del autor: Revista para la Evaluación de las Consecuencias de la Tecnología en la Teoría y en la Práctica) con el título *Normativität in der*

ISSN 1989-7022

Dilemata, año 12 (2020), nº 32, 71-82

Technikfolgenabschätzung (traducción directa del autor: Normatividad en la Evaluación de las Consecuencias de la Tecnología), en el cual aparecen muchos artículos con reflexiones éticas que parecen indicar que el tema del trabajo que aquí se presenta va ganando en actualidad y en importancia.

2.2. Evaluación del Impacto Relativa a la Protección de Datos y/o de las consecuencias sobre la Protección de Datos / Privacidad

Aunque en este artículo nos referiremos a la evaluación regulada en el art. 35 del RGPD, parece conveniente mencionar que en el mundo anglosajón existe una cierta tradición en la utilización de la herramienta del Privacy Impact Assessment (PIA). Sin embargo, pese a existir bastante información al respecto, la verdad es que esa herrramienta ha tenido escasa influencia regulatoria por la falta de una exigencia legal de su uso, ya que básicamente se recomendaba su uso y no se establecían unos criterios claros sobre el procedimiento a seguir[1]

Volviendo a la regulación establecida por el art. 35 RGPD, si bien no es necesario aportar todo el texto[2] en el actual trabajo si que mencionaremos dos puntos que pueden aclarar los objetivos perseguidos por esa norma:

> "1. Cuando sea probable que un tipo de tratamiento, en particular si utilizan nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.
>
> 7. La evaluación deberá incluir como mínimo:
>
> a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
>
> b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
>
> c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el partado 1, y
>
> d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas."

En el primer punto queda claro que la evaluación que nos ocupa no tiene como objetivo la evaluación de las tecnologías utilizadas en un tratamiento de datos personales, pese a que a día de hoy todavía hay especialistas que defienden esta interpretación, sino que tiene como objetivo central defender los derechos y libertades de las personas afectadas y a tal fin evaluar las consecuencias que un tratamiento de datos personales tiene para la Protección de Datos (de nuevo en el término alemán queda más claro: *Datenschutzfolgenabschätzung,* traducción del autor: Evaluación de las Consecuencias para la Protección de Datos).

En el siguiente se recoge el contenido mínimo que una evaluación de este tipo debe contener, y refuerza de nuevo lo expresado en el punto anterior.

Conviene recordar que esta evaluación debe realizarse siempre antes de iniciar antes de iniciar el tratamiento a evaluar y que esta evaluación forma parte del fundamento legal del mismo y

ISSN 1989-7022

Dilemata, año 12 (2020), nº 32, 71-82

que en caso de no llevarse a cabo o no ser correcta el tratamiento en cuestión supondrá desde su inicio una infracción de la normativa de Protección de Datos. También se regula que un tratamiento de este tipo deberá ser controlado de forma continuada y que la evaluación deberá repetirse siempre que los riesgos que implica varíen, por ejemplo por cambios en las tecnologías utilizadas, en la organización responsable del tratamiento o en el contexto social afectado.

Aunque no parece adecuado extenderse demasiado en la regulación de la fígura, parece evidente que en el desarrollo de esta figura y de su regulación se ha realizado también una valoración ética en la que (a diferencia de lo que ocurre en otros puntos del RGPD) se ha priorizado de una forma evidente la defensa de los sujetos afectados. Sin embargo parece que algunos expertos en Ética de los Datos [3]no lo entienden así y dudan que el mero cumplimiento de la normativa de Protección de Datos pueda ser suficiente para la valoración ética de muchos tratamientos de datos. Aunque se mencione esta opinión para dejar constancia de la existencia de opiniones contrarias a la aquí presentada, conviene mencionar que curiosamente se hace referencia a un caso sucedido en el 2015 en Dinamarca y por lo tanto en un momento previo a la entrada en vigor del RGPD y de la obligatoriedad del uso de la evaluación que nos ocupa.

Aunque a continuación se mencionarán otros instrumentos o criterios para la realización de Evaluaciones del Impacto Ético de las tecnologías, podemos avanzar que la propuesta que se presentará tendrá bastantes puntos en común con este tipo de evaluación.

2.3. Evaluación del Impacto Ético

Conviene resaltar que existen diferentes propuestas sobre modelos a seguir para realizar una evaluación de ese tipo. En la bibliografía de este artículo aparece el texto "*A framework for the ethical impact assessment of information technology*" (Wright, David), que se estructura en base a los cuatro principios de la Bioética aportados por Beaucham and Childress y adjunta una sección adicional dedicada a la Protección de Datos. Se debe reconocer que este modelo va en una dirección similar a la propuesta que se aportará en este trabajo, si bien ese texto se publicó en el 2010 y carece de las aportaciones llegadas con el RGPD y de otras aportaciones teóricas aparecidas después de su publicación.

Otro documento a resaltar, y que también aparece en la bibliografía del presente trabajo, es el de „*Ethics Guidelines for Trustworthy AI"* de un grupo de expertos en Inteligencia Artificial de la Comisión Europea. En un punto dedicado a principios éticos en el contexto de sistemas de Inteligencia Artificial se hace referencia a cuatro principios éticos:

a) Respeto a la autonomía humana
b) No maleficencia
c) Justicia
d) Explicabilidad

Para un texto aparecido en abril del 2019 parece decepcionante limitarse a escoger tres de los cuatro principios clásicos de la Bioética (cabría preguntarse el motivo de excluir el de beneficiencia) y añadir el de la explicabilidad. Si bien ese principio es perfectamente aplicable, y

ISSN 1989-7022

Dilemata, año 12 (2020), nº 32, 71-82

especialmente importante, parece que después de todos los trabajos sobre Ciberética aparecidos en los últimos tiempos se podría haber avanzado mucho más.

Aparte de iniciativas de tipo más académico como las mencionadas hasta ahora, existen otras a nivel empresarial y económico que llevan a cabo actividades que hasta cierto punto podrían encajar en el tipo de evaluaciones que aquí se estudian. Una de ellas es la de la Economía del Bien Común[4] que ha elaborado una Matriz del Bien Común 5.0[5] en la que se ha desarrollado una metodología para realizar una valoración de diferentes grupos de interés (proveedores, propietarios y proveedores financieros, trabajadores, clientes y otras empresas, entorno social) en base a unos valores preestablecidos (dignidad humana, solidaridad y justicia, sostenibilidad medioambiental, transparencia y democracia).

Otra iniciativa a mencionar es la *Large Company B Corp Certification*[6], un modelo de certificación que valora el impacto delas actividades de una empresa sobre sus empleados, la comunidad, el medio ambiente y sobre sus clientes. Esa iniciativa a creado un modelo de *B Impact Assessment(BIA)*[7] que consta de tres fases: evaluación, comparación y mejora. A continuación se realiza una valoración de los requisitos legales[8] exigidos para poder alcanzar la certificación. Finalmente se valoran los resultados obtenidos para confirmar si se alcanza el baremo establecido de 80 puntos para poder obtener la certificación. Si se alcanza ese baremo se puede pasar a firmar el acuerdo correspondiente y pagar la tarifa de certificación. La certificación debe renovarse cada tres años y para la renovación debe repetirse el BIA.

También parece adecuado mencionar los CEN Workshop Agreements CWA 17145-1 (*Ethics assessment for research and innovation - Part 1:Ethics committee)* y CWA 17145-2 (*Ethics assessment for research and innovation - Part 2: Ethical impact assessment framework).* Los enlaces a los textos están incluidos en la bibliografía de este trabajo, pero no parece necesario profundizar en ellos en este momento.

Conviene resaltar que la lista aquí presentada no pretende ser exhaustiva, sino presentar un abanico de diferentes tipos de evaluaciones de impacto existentes en la actualidad.

3. Propuesta de nuevo modelo de evaluación del impacto ético de las nuevas tecnologías en el ámbito de la salud

A continuación se presentarán los principios que deberían guiar ese nuevo modelo. No se trata necesariamente de principios nuevos, pero se considera que el orden en que se presentan y la inclusión de algunos que no siempre son tenidos en cuenta refuerzan el modelo aquí presentado.

En los principios en lo que se valoran esencialmente aspectos de seguridad informática y de privacidad se hace referencia lo que se conoce como objetivos de protección en esos campos.

Dado que no todo el mundo tiene conocimiento de esos objetivos parece necesario hacer una breve introducción. Los objetivos de protección han jugado un papel básico en la organización de sistemas técnicos cuya seguridad debe ser garantizada desde finales de los años 80. Los objetivos de protección clásicos de la seguridad de los datos son:

ISSN 1989-7022

Dilemata, año 12 (2020), nº 32, 71-82

- **Confidencialidad**, este objetivo de protección recoge como exigencia que nadie pueda acceder a los datos personales sin autorización. En ocasiones el acceso a los datos permite que el sujeto afectado sea identificado porque el contexto en el que los datos son almacenados permite sacar conclusiones sobre ese sujeto. Cuando nos referimos a personas no autorizadas, eso no significa que se trate necesariamente de terceros ajenos a la organización, que pueden actuar con intenciones criminales o de otro tipo, sino que puede tratarse también de empleados de servicios técnicos que para prestar esos servicios no precisan de acceso a los datos personales, o de personas activas en departamentos de la organización que no tienen ninguna relación con un determinado proceso o con el sujeto afectado.

- **Integridad**, en este caso el objetivo de protección resalta como exigencia que los procesos y sistemas informáticos sean capaces de mantener las características que son esenciales para la realización de las funciones imprescindibles para alcanzar la finalidad establecida y, al mismo tiempo, que los datos tratados permanezcan indemnes, completos y actuales. Posibles efectos secundarios deben ser evitados o tenidos en cuenta y tratados. Este objetivo de protección exige que entre las exigencias y la realidad haya una garantía suficiente, tanto en los detalles técnicos como en lo que afecta al tratamiento en general y su ajuste a las finalidades establecidas.

- **Disponibilidad**, este objetivo refleja la exigencia de que los datos personales estén disponibles para ser utilizados de forma adecuada en el proceso para ellos previsto. Para ello deben ser accesibles para las personas previstas y se les deben poder aplicar los métodos previstos para su tratamiento, eso incluye, entre otras cosas, que los metodos sean aplicable al formato en el que los datos están disponibles. La disponibilidad incluye que los datos sean localizables, que los sistemas implicados los puedan presentar de forma adecuada y que esa presentación sea semánticamente comprensible.

Estos tres objetivos de protección han sido aceptados por los responsables por iniciativa propia, ya que los consideraban como necesarios para su propia protección sin que existiera una normativa legal que les obligara a aplicarlos. En un principio fueron formulados para su aplicación en el ámbito de la seguridad informática y describe exigencias para un operativo seguro, especialmente en lo que afecta a procesos en el marco de organizaciones y en relación con su negocio o administración. Esas organizaciones tienen que que proteger sus procesos, independientemente de que los posibles atacantes sean personas ajenas a ellas miembros de las mismas. Es curioso que la abreviatura de estos principios en inglés (*Confidentiality, Integrity, Avaliability) sea* CIA.

Aparte de los ya mencionados objetivos de protección originados en el campo de la seguridad informática, se han desarrollado otros objetivos cuyo interés se centra en la Protección de Datos basados en normativa existente en la materia y a partir de los cuales se pueden derivar medidas técnicas y organizativas. Desde el punto de vista de la normativa de Protección de Datos, las organizaciones deben proteger sus procesos de posibles ataques, siempre que esos procesos afecten a datos de carácter personal. Los objetivos de protección de la Protección de Datos precisan, en comparación con los objetivos de protección de la seguridad informática, de un grado de comprensión más amplio, ya que la Protección de Datos tiene en cuenta una perspectiva de protección adicional, al tener en cuenta los riesgos que las actividades de la organización en sí mismas pueden originar para el sujeto afectado, tanto en el ambito de sus procesos de negocio/administración como fuera de ellos. Desde el punto de vista metodológico eso significa que no sólo una persona debe demostrar ante una organización que es de

ISSN 1989-7022

Dilemata, año 12 (2020), nº 32, 71-82

confianza, sino que la organización debe ser capaz de demostrar frente a una persona que es de confianza. Por ese motivo es preciso establecer objetivos de protección que garanticen la protección de los sujetos afectados frente a diferentes tipos de organizaciones.

Estos objetivos de protección específicos de la Protección de Datos, cuya finalidad es la protección del sujeto afectado, son:

- **No encadenabilidad**, refleja la exigencia de que los datos sólo sean tratados y valorados para la finalidad para la que fueron recogidos.

- **Transparencia**, requiere que, aunque en diferentes niveles, tanto el sujeto afectado, como el responsable de los sistemas y posibles autoridades de control puedan reconocer qué datos y para qué finalidad han sido recogidos y tratados en un proceso, que sistemas y procesos han sido utilizados, en qué dirección y para qué fines fluyen los datos y quien es el responsable legal de los datos y sistemas en las diferentes fases de un tratamiento de datos. La transferencia es imprescindible para el control y dirección de los datos, procesos y sistemas desde su inicio hasta su cancelación, y un requisito previo para que un tratamiento de datos sea legítimo y, en caso de necesidad, los sujetos afectados puedan otorgar su consentimiento.

La transparencia de un tratamiento de datos en su conjunto y de las partes implicadas puede permitir que especialmente los sujetos afectados y las autoridades de control puedan detectar posibles fallos y exigir que se lleven a cabo las modificaciones necesarias para suprimirlos.

- **Capacidad de intervenir**, exige que el sujeto afectado pueda ejercer de forma efectiva sus derechos de acceso, rectificación, cancelación y oposición (ARCO) en cualquier momento, y que el responsable está obligado a tomar las medidas necesarias para hacer efectivos esos derechos. Para alcanzar este objetivo debe ser posible modificar el tratamiento de datos en cualquier momento y en cualquiera de sus fases, desde la recogida de los datos hasta su cancelación.

Después de esta introducción extensa pero necesaria, especialmente porque los principios expuestos a continuación hacen referencia a la evaluación de nuevas tecnologías, se procederá a presentar los principios que guiarán el modelo planteado.

1. Explicabilidad, este principio ya se vió incluido en las *AI Ethics Guidelines* del Grupo de Expertos de la Comisión Europea, como ya se ha mencionado anteriormente en este trabajo. Pero aquí se quiere resaltar la importancia de este principio no solo en lo que afecta a la inteligencia artificial, sino para cualquier nueva tecnología aplicada al ámbito de la salud. El significado de este principio radica en que cualquier organización que pretenda implementar una nueva tecnología en el ámbito que nos ocupa debe alcanzar el máximo grado de transparencia posible sobre el procedimiento a implementar. La regla esencial debería ser que lo que no es explicable no debería ser implementado, si bien se pueden aceptar excepciones debidamente documentadas y que deberían ser revisadas de forma continuada para garantizar el grado de transparencia adecuado.

2. Autonomía y libertad del usuario de las nuevas tecnologías. Esto supone que el usuario debe poder conocer las herramientas tecnológicas a fin de poder decidir de forma libre sobre si las quiere usar o no. Este principio tendría como consecuencia que el Software

ISSN 1989-7022

Dilemata, año 12 (2020), nº 32, 71-82

utilizado en el campo de la salud debería ser libre o como mínimo de código abierto para poder controlarlo de forma adecuada. El Software privativo no es controlable.

3. Beneficiencia. Obligación de actuar en beneficio de otros, promoviendo sus legítimos intereses y suprimiendo prejuicios. No parece preciso profundizar en este punto, especialmente cuando estamos estudiando temas de salud.

4. No maleficencia. Abstenerse intencionadamente de realizar actos que puedan causar daño o perjudicar a otros. Se reitera lo expuesto en el punto anterior.

5. Justicia. Tratar a cada uno como corresponda, con la finalidad de disminuir las situaciones de desigualdad. Se debe interpretar como la capacidad de garantizar que la nueva tecnología va a funcionar de forma justa, sin crear desigualdades. De nuevo la utilización del Software Libre parece esencial para el cumplimiento de este principio.

6. Sostenibilidad. Comprobar y analizar el impacto tecnológico sobre la contaminación del suelo, la atmósfera, y el sistema de reciclado de materiales.

7. Precaución: Paralelamente al principio de no maleficencia, respalda la adopción de medidas de ciberseguridad y protección ante sospechas de que ciertas tecnologías puedan crear riesgo en el futuro. En lo que afecta a la ciberseguridad, se debe garantizar la integridad, disponibilidad y confidencialidad de los sistemas a implementar. En lo que afecta a la disponibilidad cabe resaltar que se debe garantizar la redundancia de sistemas, por ejemplo: ¿qué sucede cuando un sistema inteligente falla?. Como ya se ha comentado anteriormente, si en el campo de la radiología se reduce la tarea de los médicos a administrar los resultados emitidos por una inteligencia artificial se hará difícil poder garantizar que esos médicos serán capaces de realizar diagnósticos correctos evaluando ellos mismos las imágenes.

8. Privacidad: El usuario debe conocer los mecanismos de privacidad en red por su seguridad y anonimato, así como los sistemas de privacidad de hardware y software. Aquí se debe garantizar de nuevo la integridad, disponibilidad y confidencialidad de los sistemas, pero poniendo el énfasis en los pacientes. Siempre hay que recordar que la seguridad se centra en las organizaciones, mientras que la privacidad lo hace en las personas, en nuestro caso pacientes. Además hay que garantizar la transparencia, capacidad de intervenir y la no encadenabilidad.

9. Democracia. Paralelamente al principio de autonomía, se debe promover en órganos institucionales una defensa de los Derechos digitales como Derechos Humanos, así como la ciberseguridad en infraestructuras sanitarias. Se debe garantizar que los nuevos sistemas han sido diseñados e implementados garantizando el cumplimiento de esos derechos.

10. Controlabilidad. La organización que plantea la implementación de una nueva tecnología debe poder garanizar que es capaz de controlarla. Por explicarlo de forma gráfica, debe existir un botón rojo que pueda detener el sistema en cualquier momento en caso de necesidad. Este problema se ha planteado en varias ocasiones en los estudios sobre inteligencia artificial, en casos en los que el resultado obtenido es el esperado

ISSN 1989-7022

pero no se puede justificar como se ha obtenido. En el campo de la salud este aspecto es especialmente importante.

11. Auditabilidad. Está estrechamente relacionado con el principio anterior, especialmente en el segundo aspecto comentado. Se deben poder documentar y justificar todas las medidas aplicadas en base a la nueva tecnología implementada.

Los principios 6 a 9 fueron presentados en un trabajo anterior por Javier Romero Múñoz[9] y simplemente han sido adaptados al campo de la salud.

4. Breve ejemplo de evaluación de impacto ético para una COVID App.

Aunque este trabajo no puede asumir el integrar una evaluación como la planteada de forma íntegra, sí que puede resultar de interés es presentar de forma esquemática los aspectos a tener en cuenta para una aplicación como las que se han aplicado hasta ahora y las que todavía se están desarrollando para intentar controlar la extensión de la pandemia que está afectando actualmente al mundo.

1. Explicabilidad. En ninguno de los modelos planteados hasta ahora se puede garanizar la explicabilidad y, desgraciadamente, este no es un problema que afecte únicamente a una COVID App. Las tiendas de aplicaciones de los sistemas preponderantes en la actualidad (Android e iOS) no utilizan el Software Libre, ni siquiera son de código abierto, y por ese motivo ninguna app puede garantizar la explicabilidad de lo que está implementando, ya que no puede controlar los flujos de datos.

2. Autonomía y libertad. De nuevo nos encontramos con el mismo problema, el sistema es cerrado y usuario no puede conocer y decidir libremente.

3. Beneficencia. En este caso parece que sí que se cumple este principio.

4. No maleficencia. A priori no plantea problemas, pero si no se garantizan algunos de los principios ya mencionados, junto con otros que se valorarán a continuación, no se podrá garantizar que no se va a causar daño.

5. Justicia. De nuevo la no utilización del Software Libre supone un problema, ya que no hay forma de garantizar que el Software implementado funciona de forma justa, por tratarse de un sistema cerrado y privativo. El que las empresas que controlan las principales tiendas de aplicaciones estén sometidas a la legislación de los E.E.U.U. de América supone un problema adicional.

6. Sostenibilidad. Por no requerir nuevos dispositivos, este principio no debería plantear grandes problemas, si bien parece necesario mencionar que en la mayoría de casos se requiere tener el Bluetooth permanentemente activo y eso supone un consumo adicional de energía.

7. Precaución. La información disponible para valorar este punto es escasa, pero vale la pena mencionar que con frecuencia se menciona la anonimización de los datos de los usuarios de la app, pero sin especificar como van a ser anonimizados ni qué medidas de

Dilemata, año 12 (2020), nº 32, 71-82

ISSN 1989-7022

Dilemata, año 12 (2020), nº 32, 71-82

seguridad se van a implementar. También parece significativo que los inventores del Bluetooth consideran que esa tecnología no es adecuada para la finalidad a la que se quiere destinar, por ejemplo en lo que afecta a falsos positivos[10]

8. Privacidad. Cabe expresar lo mismo que en el punto anterior, con el agravante añadido que supone el estar tratando grandes volúmenes de datos de salud. Ese hecho hace que exista la obligación legal de presentar una evaluación del impacto sobre la Protección de Datos de acuerdo con lo regulado en el art. 35 RGPD. A día de hoy ninguno de los proyectos existentes ha presentado una evaluación de este tipo y solo existe una disponible elaborada por un grupo de informáticos independientes[11]. Recordando los objetivos de protección, no se dispone de información en lo referente a la transparencia, capacidad de intervenir y no encadenabilidad.

9. Democracia. Los diferentes proyectos para el desarrollo de apps de este tipo no han tenido en cuenta este principio, o al menos no se puede reconocer esa intención en la información disponible.

10. Controlabilidad. De nuevo la información disponible hasta ahora no permite reconocer que se haya tenido en cuenta este principio. Esa sensación se ve reforzada por el hecho que los proyectos existentes dependan de las tiendas de aplicaciones de empresas estadounidenses que no brillan por su transparencia y disposición a permitir controles externos a sus organizaciones.

11. Auditabilidad. Como es fácil deducir de todo lo expuesto hasta ahora, la dependencia de empresas no transparentes y de Software privativo hacen difícil conseguir que las apps en cuestión sean realmente auditables.

Parece conveniente resaltar que los proyectos existentes para el desarrollo de una COVID App están en una fase inicial y cabe esperar que sean capaces de mejorar en los puntos mencionados en este trabajo. Por otra parte, conviene destacar que tanto una evaluación del impacto ético como la que se plantea en este trabajo como una evaluación del impacto sobre la Protección de Datos, tal y como exige el art. 35 RGPD, deben realizarse antes de la implementación de la app, tratamiento de datos, nueva tecnología o sistema que se esté desarrollando.

También cabe comentar que , aunque la solución óptima a nivel ético es el uso de Software Libre o como mínimo de codigo abierto, se puede alcanzar un cierto grado de respeto de los principios aquí presentados recurriendo a una documentación transparente y extensa.

5. Conclusiones

Parece evidente que a nivel general, y en el campo de la salud en especial, la tendencia a la digitalización avanza a una velocidad considerable, por expresarlo de forma suave. Como expresa Bruce Schneier “Internet es una herramienta muy poderosa, pero no es segura. La proliferación de artefactos inteligentes agravará los riesgos si no actuamos ahora”.

El campo de la salud plantea problemas específicos o agravados, ya que no "solo" se ven afectados los derechos fundamentales de los pacientes, sino que errores en los sistemas y las tecnologías utilizadas suponen un riesgo para la salud y la vida de esos pacientes.

Parece evidente que el único camino para conseguir reducir esos riesgos y mejorar los niveles de seguridad y protección de los derechos fundamentales de los pacientes y, conviene no olvidarlo, de todas las personas implicadas (profesionales de la salud en general) está en la aplicación de análisis de riesgos y de evaluaciones de impacto éticas, sobre la seguridad, sobre la Protección de Datos, de consecuencias de las tecnologías,……. Desgraciadamente a día de hoy la tendencia va en otra dirección, uno de los ejemplos más claros/graves se pudo ver en una campaña electoral del partido liberal alemán en 2017 con un slogan difícil de calificar desde el punto de vista de este trabajo "*digital first bedenken second*"[12](traducción del autor: primero digital segundo considerar). Pese a ello parece evidente la dirección a seguir para evitar que la situación empeore.

Referencias:

CEN Workshop Agreement CWA 17145-1 (Ethics assessment for research and innovation - Part 1:Ethics committee)
ftp://ftp.cencenelec.eu/EN/ResearchInnovation/CWA/CWA1714501.pdf

CEN Workshop Agreement CWA 17145-2 (Ethics assessment for research and innovation - Part 2: Ethical impact assessment framework)
ftp://ftp.cencenelec.eu/EN/ResearchInnovation/CWA/CWA17214502.pdf

Ethics guidelines for trustworthy AI
https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Ethical Impact Assessment and Conventional Impact Assessment
https://satoriproject.eu/media/1.a-Ethical-impact-assessmt-CIA.pdf

Morley, Jessica and Cowls, Josh and Taddeo, Mariarosaria and Floridi, Luciano, Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems (April 22, 2020). Available at SSRN: https://ssrn.com/abstract=3582550 or http://dx.doi.org/10.2139/ssrn.3582550

Muñoz-Alonso López, Gemma, LA EVALUACIÓN DE TECNOLOGÍAS (ET): ORIGEN Y DESARROLLO
https://revistas.ucm.es/index.php/RGID/article/download/RGID9797120015A/10963

Romero Muñoz, Javier, CiberÉtica como ética aplicada: una introducción. Dilemata N.º 24 (2017)
https://www.dilemata.net/revista/index.php/dilemata/article/view/412000100/490

TATup Vol 28 No 1 (2019): Normativity in Technology Assessment
https://www.tatup.de/index.php/tatup/issue/view/8

Wright, D. A framework for the ethical impact assessment of information technology. Ethics Inf Technol 13, 199–226 (2011). https://doi.org/10.1007/s10676-010-9242-6

ISSN 1989-7022

ISSN 1989-7022

Dilemata, año 12 (2020), nº 32, 71-82

Notas al final

1. Este texto en castellano aporta algo de información al respecto: Evaluación PIA desde el punto de vista del SDM. Kirsten Bock, Martin Rost y Ricardo Morte Ferrer http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/evaluacion-pia-desde-el-punto-de-vista-del-sdm
2. A efectos informativos se aporta este enlace en el que se puede leer el artículo en su totalidad http://www.privacy-regulation.eu/es/35.htm
3. https://dataethics.eu/time-data-ethics-impact-assessment/
4. https://economiadelbiencomun.org/
5. https://economiadelbiencomun.org/wp-content/uploads/2018/06/Matriz-bien-com%C3%BAn-5-0.pdf
6. https://bcorporation.net/certification
7. https://bimpactassessment.net/
8. https://bcorporation.net/certification/legal-requirements
9. https://www.dilemata.net/revista/index.php/dilemata/article/view/412000100
10. https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing/
11. https://www.fiff.de/dsfa-corona disponible en varios idiomas.
12. https://www.it-zoom.de/mobile-business/e/digital-first-bedenken-second-17640/ aquí se puede leer en alemán un comentario al respecto y una imagen de la mencionada campaña.